Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.0.6

March, 2007

Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.0.6

Covers: SCA BB 3.0.6, SCA BB 3.0.5A, SCA BB 3.0.5, SCA BB 3.0.4, SCA BB 3.0.3, SCA BB 3.0.1, SCA BB 3.0.0

OL-8958-09

These release notes for the Cisco SCA BB describe the enhancements provided in Cisco SCA BB Release 3.0.6. These release notes are updated as needed.

For a list of the caveats that apply to Cisco SCA BB Release 3.0.6, 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 3.0.6 of its Service Control Application for Broadband (SCA BB).

This document describes the new functionality, enhancements, and known issues in SCA BB release 3.0.6.

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.

SCA BB Release 3.0.6

Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.0.6. See the *Cisco Service Control Application for Broadband User Guide* for a complete description.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.6.

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
QQ-Live	1032	TV P2P streaming application	Added as a new protocol and to P2P Service
Flash YouTube	1034	Flash video streaming from YouTube site	Added as a new protocol and to HTTP Browsing Service
Flash MySpace	1035	Flash video streaming from MySpace site	Added as a new protocol and to HTTP Browsing Service
Flash Yahoo	1036	Flash video streaming from Yahoo!	Added as a new protocol and to HTTP Browsing Service
Flash	1033	Other Flash traffic	Added as a new protocol and to HTTP Browsing Service

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.

Protocol Updates

The following table lists the protocols that were updated in SCA BB 3.0.6.

Protocol Name	Description	Cisco Number
QQ	Update to support 2006 version	
Thunder	Added support for HTTP download flows	CSCsh16688
Poco	Update to support 2006 version	CSCsg65908
Skype	Added Skype In/Out/Cast services recognition	
Yahoo	Added Yahoo Voice call over TCP recognition	CSCsd53602
PeerEnabler	Updated signatures for GIVE handshake users (eMule, fastTrack, and PeerEnabler)	CSCsg22708 CSCsg74855
Edonkey		
Kazaa		
Ares 1.9.9	Added Download/Upload upon TCP recognition	CSCsf29301 CSCsf29299 CSCsf29178

Resolved Caveats

The following caveats are resolved in this release:

Accomodation with US Daylight policy change

- Cisco Number CSCsh20257

  Previous SCA BB releases did not conform with the US Daylight Saving Time policy change of 2007.

  This issue is resolved in this release.

Compatibility Information

SCA BB 3.0.6 should be used with the following components:

- SCOS 3.0.6
- SCMS-SM 3.0.3, 3.0.5, 3.0.6A

  Note: Use the SCMS-SM 3.0.3 patch for SM-cluster upgrades from SM 3.0.x to SM 3.0.3.
- SCMS-CM 3.0.0, 3.0.3, 3.0.5, 3.0.6

  Note: VoIP reporting capabilities are only supported with CM 3.0.3 and up.

Note about PRPC Authentication Issue

SCA BB 3.0.6 contains a fix for the PRPC authentication issue documented in CSCsh39763.

The recommended combination that implements this fix is using the 3.0.6 version of all components: SCA BB, SCOS, SCMS-CM and SCMS-SM.

For a detailed discussion of the implications of using previous releases with SCA BB 3.0.6 on this issue, please see the SCMS-SM 3.0.6 Release Notes, or Field Notice 62652.

Capacity Information

SCA BB 3.0.6 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

SCA BB Release 3.0.5A

Resolved Caveats

The following caveats are resolved in this release:

Problem in port-based protocol classification

- Cisco Number CSCsg88916

  Problem Description

  When using SCA BB 3.0.5, flows that are initiated from the network toward the subscriber and use port-based protocols are classified using the network-side (source) port number of the flow instead of the server-side (destination) port number. This port number is then used to match against the port-based protocols defined in the service configuration (PQB) file and may cause protocol misclassification followed by a wrong service classification.

  For example, in the default service configuration, SSH is defined as a port-based protocol. Any SSH session initiated from the network side toward a subscriber host will be classified as Generic TCP instead of being classified to the service set for the SSH protocol.

  The same error occurs with many gaming protocols. Traffic initiated toward port-based gaming servers located on the subscriber side of the SCE will be wrongly classified.

  This problem does not affect flows using port-based protocols that are used with servers located in the network.

  This issue is resolved in this release.

Console requires Root level SCE authentication

- Cisco Number CSCsg86093

  The SCA BB Console and the SCA BB **servconf** utility require user authentication in order to perform various management operations on SCE platforms. In release 3.0.5 these operations require Root (level 15) authentication. (Previous releases required Admin (level 10) authentication.)

  The change in required authentication also applies to any application using the SCA-BB Java API.

  This issue is resolved in this release: the required authentication reverts to Admin (level 10).

Compatibility Information

SCA BB 3.0.5A should be used with the following components:

- SCOS 3.0.5
- SCMS-SM 3.0.5, 3.0.3

  Note: Use the SCMS-SM 3.0.3 patch for SM-cluster upgrades from SM 3.0.x to SM 3.0.3.
- SCMS-CM 3.0.5, 3.0.3, 3.0.0

  Note: The new 3.0.3 VoIP reporting capabilities are only supported with CM 3.0.3.

SCA BB Release 3.0.5

Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.0.5. See the *Cisco Service Control Application for Broadband User Guide* for a complete description.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.5.

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
DHT	106	Distributed hash table, used by P2P applications	
EmuleEncrypted	105	eMule 0.47 with protocol obfuscation	
Freenet	107	P2P protocol	
Primus/Lingo	108	VoIP service	
TVAnts	109	TV and video streaming protocol	
Entropy	125	P2P-like protocol (“net inside the net”)	

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.

Protocol Updates

The following table lists the protocols that were updated in SCA BB 3.0.5.

Protocol Name	Description	Cisco Number
Skype	Update signature to support version 2.5	
ARES	Update Wares signature to support ARES 192 version	
MGCP	Bundle problem—related to MGCP transaction-id	CSCse99652
ICQ SIP	Two consecutive calls are not properly bundled	CSCse99641
SMTP	CR-LFs in RDRs where they are not allowed/expected	CSCsd61859
eMule	Classified eMule HTTP based traffic relying on X-Network field in HTTP header instead of user-agent field	CSCsg10743
HTTP 0.9	HTTP 1.0/1.1 packet that starts with 'GET' and not recognized as P2P, will be never reported	CSCsd17487
BitTorrent	Added support for uTorrent 1.6 client	CSCsg10738

Elimination of Traffic Bursts on Quota Refresh

In previous releases, when using periodical quota, a traffic burst could be observed when, at the end of a quota period, a quota refresh would be preformed simultaneously for all affected subscribers. As all of the subscribers who had depleted their quota had a quota replenish at the same time, traffic would rise when they started consuming bandwidth again.

In release 3.0.5, the exact time when the periodical quota refresh happens can be scattered randomly to avoid a traffic burst. Enable this feature by setting the length of scatter time in the package settings window.

Aggregate Global Controller per Link

In release 3.0.5, the GC setting in the service configuration can express an aggregate GC limit per link or on the sum of 2 links. This mode can be enabled in the Console or via the API.

Persistent Long-Term Quota Management

In release 3.0.5, managing subscriber quota using an SM-based external quota manager is supported.

Real-Time Monitoring

SCA BB 3.0.5 has an added feature that, together with third-party tools (MRTG, RRDTool), allows the user to use SNMP data from the SCE to view on-the-fly reports. The available reports and their usage are described in the *Cisco SCA BB SNMP Real-Time Monitoring User Guide*.

Increased Number of Package Counters and Global Controllers

In release 3.0.5, the number of available GCs has been raised to 1024. The number of available package counters has also been raised to 1024.

Resolved Caveats

The following caveats are resolved in this release:

MGCP bundled flows are classified as UDP

- Cisco Number CSCse28478

  When using SCA BB 3.0.3, a small percentage of MGCP bundled flows are classified as UDP.

  This issue is resolved in this release.

BitTorrent misclassification with Metastock application

- Cisco Number CSCse67418

  SCA BB 2.5.10 and 3.0.3 and previous versions classify Metastock traffic as BitTorrent.

  This issue is resolved in this release.

FLYFF game misclassified as P2P

- Cisco Number CSCse79503

  The SSDP utility protocol is assigned to the P2P service. As a result some on-line gaming is filtered when a P2P control is issued. SSDP is a utility protocol and should not be assigned to P2P service.

  This issue is resolved in this release.

Fatal due to memory overrun

- Cisco Number CSCse83771

  Memory overrun (data access event) during MGCP classification can cause a Traverser Guard timeout and in some cases a reboot.

  This issue is resolved in this release.

Protocol Library does not set aging on all flows—as a result aging is set by the OS

- Cisco Number CSCsg14842

  The Protocol Library does not set aging when looking for multiple signatures for the following protocols:

  - STUN/Beat
  - Generic Download

  Instead, the OS sets the aging.

  This issue is resolved in this release.

SNMP traffic misclassified as Skype

- Cisco Number CSCsg29788

  A Service Control Engine 2020 running SCOS / SCA BB 3.0.4 may incorrectly classify SNMP traffic as the Skype protocol resulting in SNMP flows being controlled as if they were Skype.

  This issue is resolved in this release.

Package Hourly Usage Volume per Service report

- Cisco Number CSCse18308

  The report's chart indication of the displayed time span is garbled.

  This issue is resolved in this release.

Package Active Subscriber per Service report: has unnecessary link property

- Cisco Number CSCse18678

  The report contains an irrelevant parameter for choosing the link ID. Setting this parameter yields an error.

  This issue is resolved in this release.

Subscriber Daily Usage Session/Volume per Service

- Cisco Number CSCse19874

  The report contains an invalid parameter for time span indicating a number of hours, instead of a number of days.

  This issue is resolved in this release.

Some reports throw Invalid column name LINK_ID error

- Cisco Number CSCse25655

  Some of the PUR-based reports have a link selection parameter that is not relevant to the report. If this parameter is assigned a value, the Reporter throws an SQL exception when trying to execute the Report (indicating that LINKID is not a valid column)

  This issue is resolved in this release.

GUI gets stuck after left open for many hours

- Cisco Number CSCse41471

  SCA BB Console can hang while working with the Service Configuration Editor for many hours continuously.

  This issue is resolved in this release.

Count sessions for non-classified flows

- Cisco Number CSCse63662

  When viewing BW per Service reports, unclassified flows are shown as BW on the Default Service. However, Sessions per Service reports from the same period show zero sessions on the Default Service.

  This issue is resolved in this release.

TURs interim minimum interval of 30 seconds is not enforced

- Cisco Number CSCse70577

  When TURs (Transaction Usage RDRs) interim interval is set to a value smaller than 30 seconds, the actual interval used is 30 seconds.

  This issue is resolved in this release.

Package Bandwidth per Service report has saw-tooth

- Cisco Number CSCse79517

  The END_TIME field of PUR RDRs may have non-uniform delta between consecutive values. This is most obvious in the Reporter, when producing a PUR-based report—the varying delta displays as saw-tooth peaks in the displayed consumption.

  This issue is resolved in this release.

Unable to disable TURs for Unknown Subscribers

- Cisco Number CSCse80056

  Disabling Transaction Usage RDRs for Unknown Subscribers does not work in SCA BB 3.0.3 because unclassified traffic belonging to Unknown Subscribers is reported on the Default Service of other known subscribers and their packages.

  This issue is resolved in this release.

Error in Top DoS Attacked hosts (Duration[Min])

- Cisco Number CSCse87832

  When producing Top DoS Attacked hosts reports with the following parameters:

  - Metric: Duration[Min]
  - Detected IP side: Subscriber

  The following error appeared: Incorrect syntax near '[Mi'.

  And the report is not generated.

  This issue is resolved in this release.

Flow Interim Signaling RDRs not being generated for the configured interval

- Cisco Number CSCse93210

  Flow Interim Signaling RDRs are not generated for the configured time interval.

  This issue is resolved in this release.

Top Clients report contains redundant WHERE clause

- Cisco Number CSCsf06516

  The SQL code generated by this report contained a redundant "(SOURCE_IP <> 0)" clause, which in some circumstances could hurt the report performance.

  This issue is resolved in this release.

Time display problem in Package Hourly Usage Volume per Service report

- Cisco Number CSCsf25848

  The time-zone offset affects the displayed time in the Package Hourly Usage Volume Per Service.

  For example if the time selected for "Ending before" is 20:00:00 and the time-zone offset is +8 hours, the last indication of time that would be displayed in the report will show 12:00:00 instead of 20:00:00

  This issue is resolved in this release.

Error when executing Daily peak BW for all Packages report

- Cisco Number CSCsg09909

  When executing the Daily peak BW for all Packages report on an Oracle database, the following error massage is generated: ORA 00979 - not a GROUP BY expression

  This issue is resolved in this release.

AGC bandwidth is too low

- Cisco Number CSCse94389

  Symptom: AGC enforcement sometimes gets stuck on a very low value (8 kbps) and bandwidth is not enforced correctly.

  This issue is resolved in this release.

Compatibility Information

SCA BB 3.0.5 should be used with the following components:

- SCOS 3.0.5
- SCMS-SM 3.0.5, 3.0.3

  Note: Use the SCMS-SM 3.0.3 patch for SM-cluster upgrades from SM 3.0.x to SM 3.0.3.
- SCMS-CM 3.0.5, 3.0.3, 3.0.0

  Note: The new 3.0.3 VoIP reporting capabilities are only supported with CM 3.0.3.

Capacity Information

SCA BB 3.0.5 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

SCA BB Release 3.0.4

Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.0.4. See the *Cisco Service Control Application for Broadband User Guide* for a complete description.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.4. Note that some of these protocols are also available in the latest 3.0.3 protocol pack.

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
ICQ	119	Instant Messaging application	Assigned to the default Instant Messaging service.
ICQ VoIP	110	ICQ VoIP is a flavor of SIP, similar to Vonage.	Assigned to the default SIP service.
CU-SeeMe	117	Instant Messaging and video conferencing	Assigned to the default Instant Messaging service.
Rodi	111	P2P file sharing	Assigned to the default P2P service.
GoogleEarth	118	Mapping application	Assigned to the default HTTP service.
Hopster	115	HTTP Tunneling	Assigned to the default HTTP Tunneling service.
Jabber	116	IM application	Assigned to the default Instant Messaging service.
AntsP2P	113	A protocol for free online TV	Assigned to the default P2P service.
Sling	112	TV streaming	Assigned to the default Streaming service.
Share	9	Share NT5 and EX2	

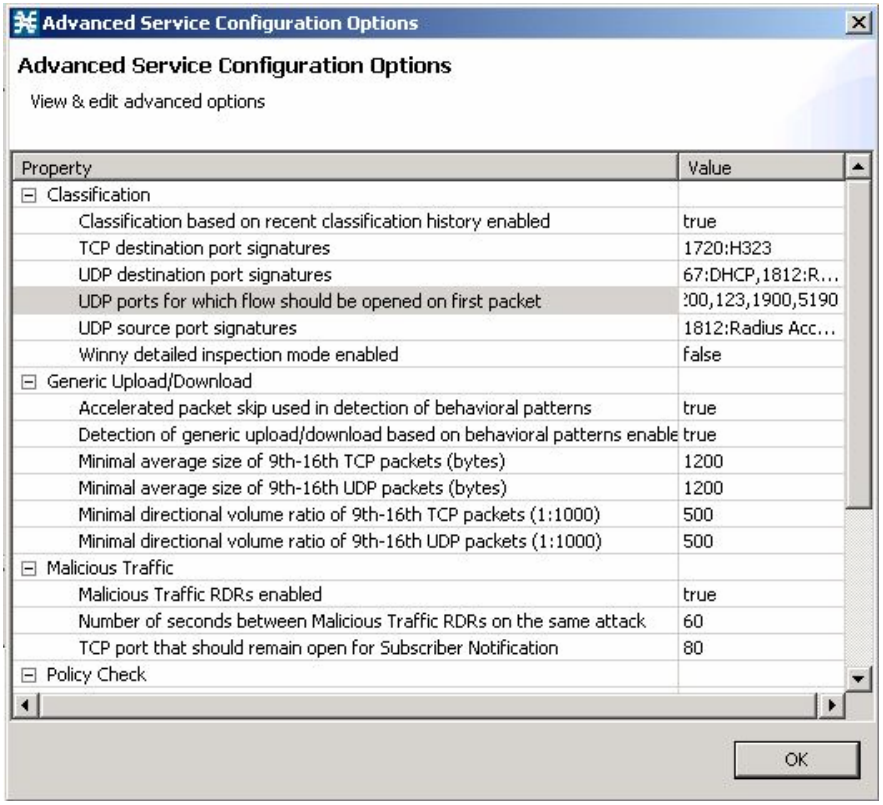
Note When upgrading old PQB files, new signature-based protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as generic TCP. To fix this, manually assign these protocols to a service.

ICQ VoIP Configuration

Although 3.0.4-PP05 correctly classifies 'ICQ VoIP' traffic as SIP, the following additional manual configuration change is required:

Step 1. In the Service Configuration Editor, from the Configuration menu, select **System Settings**.

The Advanced Service Configurations Options dialog box appears.



Step 2. In the Advanced Service Configurations Options dialog box, add port 5190 to the list of "UDP ports for which flows should be opened on first packet."

Protocol Updates

The following table lists the protocols that were updated in SCA BB 3.0.4.

Protocol Name	Description	Cisco Number
Share	New signatures for 2ex added	CSCse06602
Share	New signatures for NT5 UDP added	CSCsc96277
BitTorrent	".torrent" pattern removed	CSCse51968
BitTorrent	Added tunable to enable or disable BitTorrent networking signature to work around misclassification of other protocols (such as Metastock) that use DHT	CSCse67418
Gnutella	Foxy and mxie Gnutella user-agent added	CSCse39295
Warez	Signature updated to fix HTTPS and Telnet traffic misclassification	CSCse25538 CSCse30568
Manolito	Signature updated to fix Mosa VoIP traffic misclassification	CSCsd66745
FTP	Signature updated to fix FTP sessions that are not properly bundled	CSCsd74132
FileCroc	Signature updated to fix HTTPS misclassification as FileCroc	CSCse30568
Skype	Signature updated to fix CounterStrike misclassification as Skype	CSCse10448
Content Filtering Redirect	Fix for a redirect issue in SCA BB 3.0.3	CSCse72875

Resolved Caveats

The following caveats are resolved in this release:

Update SPQI process can throw "out of memory" exception

- Cisco Number CSCse57065

  When installing a protocol pack using SERVCONF, the installation fails due to an out of memory error. When doing the same installation through the Network Navigator GUI, the installation succeeds.

  This issue is resolved in this release.

Non-P2P flows are classified as P2P

- Cisco number CSCsd82777
- Cisco number CSCsd58322

  In SCA BB default service configuration, the default port (or well-known port) for some protocols may be used for classification in addition to the protocol signature. In geographic areas where this default port configuration might be used by other applications, false positive classifications will result.

  This issue is resolved in this release.

Dropped packets in report-only mode when using content filtering

- Cisco Number CSCsd92634

  Web Content Filtering using SurfControl CPA server was added in release 3.0.3. The SCE queries SurfControl's URL database in order to classify HTTP traffic and then waits for the database to return the URL categorization of the traffic. While waiting, the SCE might need to delay the HTTP flow by dropping packets. These HTTP packets can be dropped when the system mode is report-only, even though report-only mode should not affect traffic.

  This issue is resolved in this release.

PQB configuration cannot be applied

- Cisco Number CSCse17066

  Attempting to apply a PQB containing a filtered traffic rule with the transport type set to ‘Any’ and a specific port number will fail.

  Additionally, when the transport type is 'Any', the wizard pages for port numbers should not be shown. However, by pressing the **Back** button on the wizard, it is possible to make the port numbers appear and thus to allow the user to create a configuration that is invalid.

  This issue is resolved in this release.

'Operation Flash Point' & protocol 1009 duplicate port configuration

- Cisco Number CSCse37188

  A number of protocols are defined in SCA BB as having the same port number. ‘Operation Flash Point’ and ‘directplay8’ are both defined as using generic TCP on port 6073 and both will be classified as ‘directplay8’. ‘Diablo’ and ‘fsgs’ are both defined as using generic TCP on port 6112 and both will be classified as ‘Diablo’.

  This issue is resolved in this release.

"Heap Error" exceptions when the GUI is launched by double-clicking a PQB

- Cisco Number CSCse48949

  When the SCA BB console is started by double-clicking a PQB file, some operations can fail and the log will contain "Heap Error" exceptions.

  This issue is resolved in this release.

Global Controller does not allow commas to be used as the decimal point

- Cisco Number CSCse50835

  When the regional setting of the client computer is set to a locale that uses the comma as a decimal point, the Global Controller Settings window on the Service Configuration editor will correctly display a comma in the window if a fractional percentage is entered. I.e. for a value of 0.5% the window will display 0,5%. However, when you close the Global Controller Settings window and save your settings, you will not be able to reopen the window. Clicking on the option on the Configuration Tab will also not open the Global Controller Settings window.

  This issue is resolved in this release.

  Compatibility Issue

  When upgrading to SCABB version 3.0.4 and above, users that have been using comma as a decimal point should be aware to the following issue.

  When loading a PQB file, the comma in the decimal number representing the GC BW is interpreted as a delimiter between BW values for different time frames. As a result the GC configuration will be corrupted; for example, the GC value 20.5, which is written as '20,5' will be interpreted as 20% for the first time frame and 5% for the time frames two to four.

  In such cases, users have two options to handle this problem:

  - Before upgrading to the new SCA-BB solution, modify the GC configuration to use BW values that are whole numbers.
  - After upgrading to the new SCA-BB solution use the SCA-BB console to fix the GC BW values.

Compatibility Information

SCA BB 3.0.4 should be used with the following components:

- SCOS 3.0.3
- SCMS-SM 3.0.0, 3.0.1, 3.0.3
- SCMS-CM 3.0.0, 3.0.3

Capacity Information

SCA BB 3.0.4 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

SCA BB Release 3.0.3

Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.0.3. See the *Cisco Service Control Application for Broadband User Guide* for a complete description.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.3. Note that some of these protocols are also available in the latest 3.0.1 protocol pack.

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
Generic Upload/Download	127	See the following section.	Assigned to a new service, 'Generic Upload/Download' (ID = 39), under the default Generic service
Generic Non-Established TCP	126	TCP flows that are not established properly are mapped to this protocol (syn-ack is missing).	Assigned to the Generic TCP service.
Yahoo Messenger VoIP	45	Yahoo Messenger VoIP is a flavor of SIP, similar to Vonage.	Assigned to a new service, 'Yahoo Messenger VoIP' (ID = 37), under the default VoIP service.
Dijjer	120	P2P	Assigned to the default P2P service.
Exosee	121	P2P	Assigned to the default P2P service.
PeerEnabler	122	P2P application. A signature added to the port-based protocol.	Assigned to the default P2P service.
Furthur	123		Assigned to the default P2P service.
Kontiki	124	P2P	Assigned to the default P2P service.
Google Talk	1030	Port based IM application. Port 5222 TCP.	Assigned to the default Instant Messaging service.
Konspire2b	1031	A port based P2P application. Port 6085 TCP and UDP	Assigned to the default P2P service.

In addition, the following port-based gaming protocols were added to the default service configuration:

Anarchy, Asherons Call, Black And White, Counter Strike, Dark Reign, Diablo, Elite Force, F16, F22 Simulator (lightning 3), Hexen, Kohan Immortal Sovereigns, Motorhead, Myth, Need For Speed, Need For Speed 3, Operation Flash Point, Outlaws, Swat3, Ultima, Warcraft, Znes, Delta Force, Rainbox six, Soldier of fortune, Westwood online, and Yahoo Games.

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.

Generic Upload/Download

This release introduces a new concept of heuristic classification of flows based on their inspected behavior. In previous releases, unidentified traffic is mapped, based on its transport protocol, to the Generic TCP service or to the Generic UDP service. With the introduction of behavioral classification signatures, SCA BB is able to further refine this classification and indicate what type of protocol/application is carried over these unknown flows. Using behavioral classification signatures, the solution is now capable of providing more granular classification even in an environment where new protocols, not previously inspected by the solution, are present in traffic, even before dedicated signatures are implemented for these protocols.

This release implements a Generic Upload/Download signature. The new signature can identify download activity that is taking place over flows of unknown protocols. Note that this feature is disabled by default, and can be disabled through the Advanced Service Configuration Options dialog.

Service Security

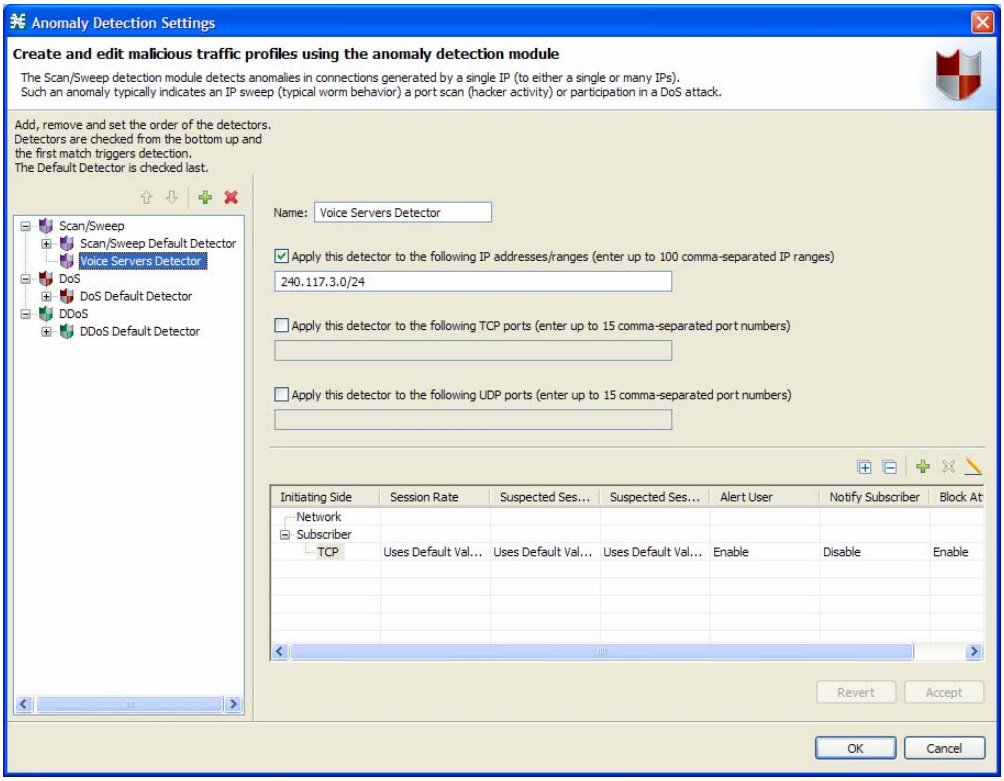
The service security capabilities of Cisco SCA BB are greatly enhanced in this release to provide a robust service control security solution.

Service Security Dashboard

The Service Security Dashboard is a central GUI view inside the Service Configuration Editor, where you can control and monitor network security threats. The dashboard presents the following categories:

- Signature-based detection and mitigation of Internet worms. (Note that currently Cisco does not provide the worm/virus signatures.)
- Anomaly-based detection and mitigation of Internet worms and DoS/DDoS attacks.
- Detection and mitigation of spam zombies and mass-mailing viruses.

For each category, you can configure detection settings, actions to take when an attack is detected, and reports to be generated. Anomaly-based detection categories provide a new GUI for configuring anomaly-based detection and handling parameters. A snapshot of the new screen is shown below.



Note The new GUI for configuring Anomaly based detection replaces the CLI commands for configuring SCE attack filter module, and the CLI for configuring subscriber notification on network attack.

Anomaly Based Worm Detection

A network worm outbreak is reflected by a noticeable increase in the rate of connections (triggered by scans), and in the ratio between unsuccessful and successful connections. The Scan/Sweep mechanism detects IP addresses suspected of propagating worms and the protocol/port in use.

DoS/DDoS Detection

DoS attacks are characterized by a high rate of connections initiated to an IP address. The most common type of attack is characterized by single or multiple sources initiating sessions toward a single destination. The Cisco SCA BB DDoS detection mechanism identifies the attacked IP address, the attacking/attacked IP address pair (in case of a one-to-one attack), and the protocol and port in use.

Note The default values of Suspected Session Rate for Scan/Sweep and DDoS were changed in this release, from 500 to 250 for TCP and UDP, and from 250 to 125 for ICMP and Other.

Spam-Zombie / Mass-Mailing Viruses Detection

This mechanism detects email traffic anomalies caused by spam zombies and mass-mailing viruses. The detection method is based on measuring SMTP rates to off-net SMTP servers. This functionality allows a user to detect spam zombies residing on subscriber machines, as well as hosts that are infected with email-based viruses.

Mitigation Actions

The following mitigation actions are available for threats detected through the above mechanisms:

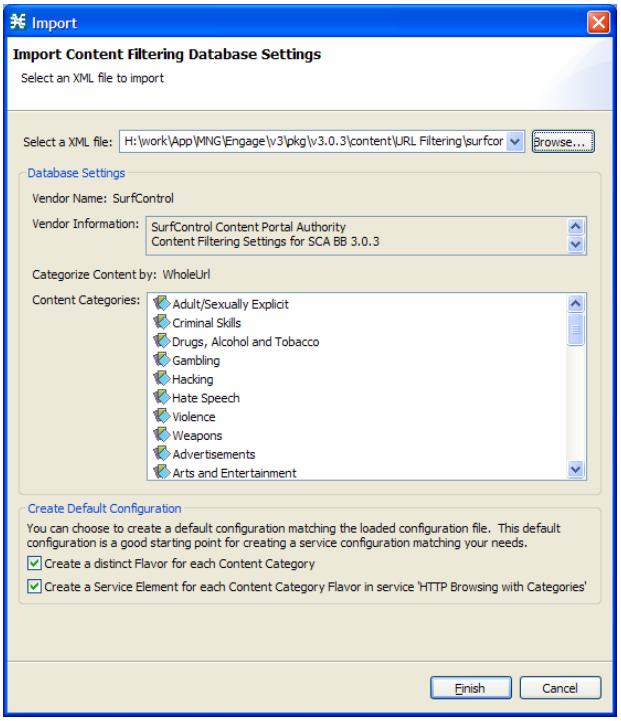
- Provider alarm—Send a notification to the administrator in order to take a manual actions
- Malicious traffic blocking—Block malicious traffic to eliminate the threat
- Subscriber notification—Redirect subscriber traffic to a web portal indication further action

Any combination of the above mitigation actions is configurable.

Content Filtering

Cisco SCA BB provides integration with an external third-party URL database. The external third-party URL database is installed separately on a dedicated machine. This integration is based on the ability to submit a query to the external database, ask for the category the URL belongs to, and act upon the response according to the internal policy. The different categories are defined via a content filtering configuration file, as seen in the screenshot below. SCA BB services can then be defined using these categories.

Note The content filtering solution has not gone through an early field trial (EFT) process prior to the release date.



Media Flow RDR

The MEDIA_FLOW_RDR is generated at the end of every SIP or Skype media flow:

- For SIP, this RDR is generated when a media channel is closed. (SIP includes all SIP based applications, such as Vonage and Yahoo Messenger VoIP.)
- For Skype, this RDR is generated when an end-of-call is detected.

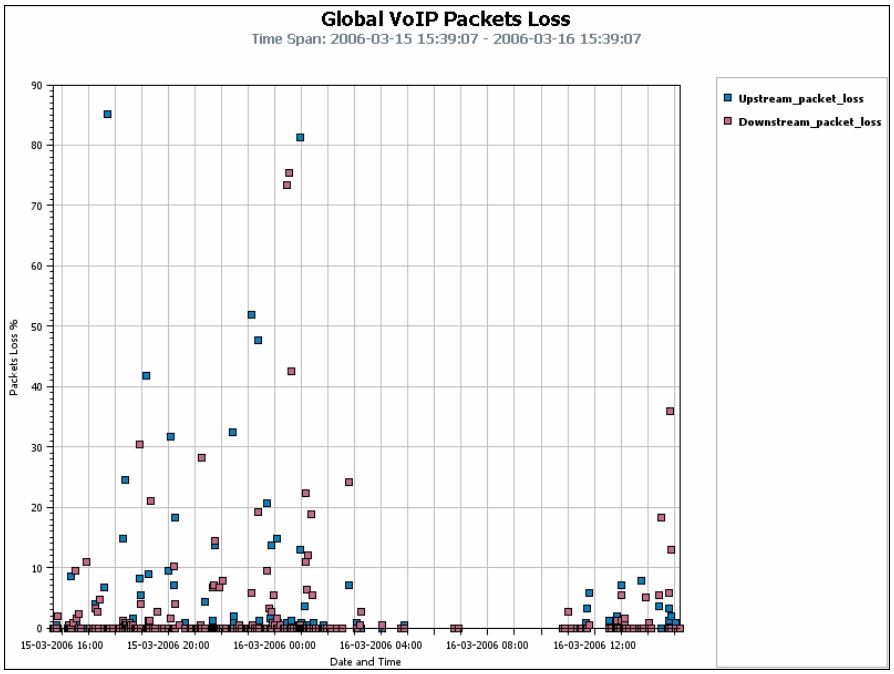
The RDR tag of the MEDIA_FLOW_RDR is 0xF0F0F46C / 4042323052.

For SIP, each RDR contains flow attributes such as SIP domain and user agent, and metrics such as jitter, packet loss, and payload type.

VoIP QoS Reports

The SCA Reporter provides new VoIP QoS reports, which are based on information extracted from RTP/RTCP traffic (SIP Media Flow RDRs). These reports cover the following QoS related metrics:

- Jitter
- Packet Loss (see screenshot below)
- Encoding types
- Calculated MOS (Mean Opinion Score–Listening quality).



Note Voice QoS reports require SCMS CM 3.0.3.

Hitless Upgrade

Prior to this release, protocol upgrade resulted in a period of time in which analysis and control were not performed on traffic. This “service control gap” forced customers to perform application upgrades only during maintenance windows when traffic volume is low and loss of service control is less critical.

This release solves the problem for the frequently released protocol packs by enabling two copies of the application – the old one and the new one – to run simultaneously on the SCE, with all new flows handled by the new application. The two copies of the application share information to prevent any loss in service control. Once the last flow handled by the old copy of the application terminates, the upgrade is complete.

Note Major and minor application releases and SCOS upgrades still require the interruption of analysis and control, and should still be performed at the maintenance window.

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.

  This happened because flows were gradually assigned to a new GC when time frames changed. This controller then restarted the BW convergence process, regardless of the state of the previous GC.

  This issue is resolved in this release as follows:

  Flows are not re-assigned to a new GC on time frame change. 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.

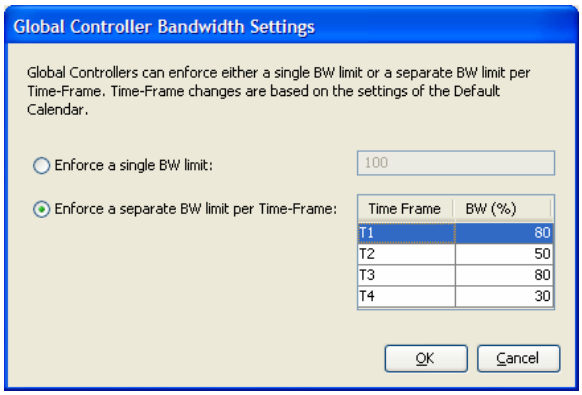
  In the Service Configuration Editor, the Global Controller Settings dialog box was enhanced to allow time-based GC values.

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

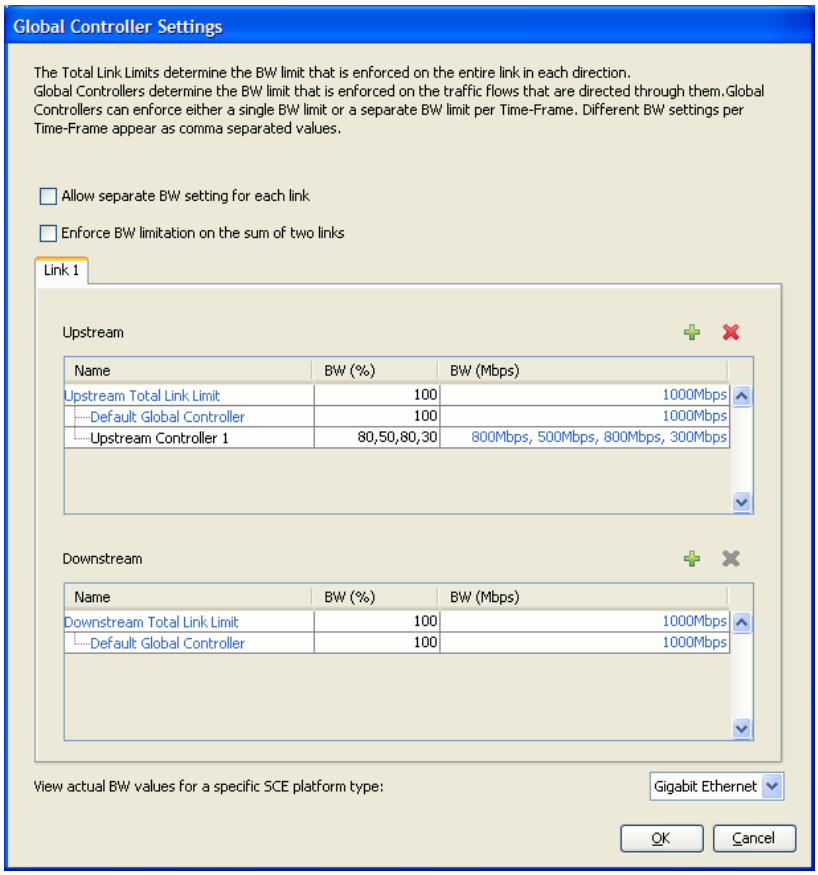
Step 1. In the Global Controller Settings Window, click the "BW (%)" cell to edit the value.

The Global Controller Bandwidth Settings dialog box 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 dialog box 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.

Important Note If you are *upgrading* to this release:
Time-based rules in old PQBs, which use separate GCs per time frame, are not 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.

Network Navigator GUI fails to login to SM and CM

- Cisco number: CSCsd86114

  Attempts to log in to the CM and SM through the SCA BB Console may result in login failures (invalid password) when certain replies from the server are dropped.

  This may result in a scenario where the client login initially succeeds, and subsequently fails, for no apparent reason.

  This can occur when the client is using the SCA BB Console and connecting to the CM or SM through a VPN connection, or if there is an intermediate firewall. After the FTP authentication succeeds, the client sends a QUIT command, but the server either does not reply or the response from the server does not arrive at the client. In this case, the connection may be abruptly closed by the firewall or other intermediate device.

  The abrupt closing of the connection results in a null pointer exception, which leads to authentication failing, despite having initially succeeded.

  This issue is resolved in this release.

Dynamic Signatures with string search might cause SCE platform failure

- Cisco number: CSCsd31562

  Loading a Service Configuration file that includes a Dynamic Signature may cause the SCE platform to reload several times and get into failure mode. This is caused by string-search signatures.

  This issue is resolved in this release.

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 showed an incorrectly low number of active subscribers.

  This issue is resolved in this release.

HTTPS misclassification

- Cisco Number CSCsd13325

  With SCA BB 3.0.0, HTTPS traffic may not be classified as HTTP but as generic TCP.

  As of release 3.0.3, the HTTPS signature is removed and the default protocol configuration is only port-based.

Misclassification of traffic on several known ports

- Cisco Number CSCsd14658

  Traffic on a well-known port that is assigned to an App-Signature protocol in the Service-Configuration file (PQB) will always be classified to the Service based on that App-Signature protocol. This implies that P2P traffic on such port will be misclassified as that App-Signature protocol rather than the correct P2P protocol.

  The impact is that subscribers can set their P2P clients to work with specific ports that will enable them to escape P2P control.

  This issue is resolved in this release.

Skype duration call counter is not functioning

- Cisco Number CSCsd37380

  Voice reports for Skype call minutes show no activity, and the call duration counters in Link and Package RDRs, for the Skype service, are always zero.

  This issue is resolved in this release.

No redirect in subscriber notification

- Cisco Number CSCsd72727

  When activated, subscriber notification is supposed to block and redirect all of the subscriber's HTTP traffic to a designated web page until the notification is dismissed. However, with SCA BB 3.0.0 and 3.0.1 (without the latest protocol pack), HTTP traffic is blocked but not redirected.

  This problem is applicable to SCA BB 3.0.0 and 3.0.1.

  This issue is resolved in the latest 3.0.1 protocol pack, and in release 3.0.3.

Compatibility Information

SCA BB 3.0.3 should be used with the following components:

- SCOS 3.0.3
- SCMS-SM 3.0.0, 3.0.1, 3.0.3
- SCMS-CM 3.0.0, 3.0.3

Capacity Information

SCA BB 3.0.3 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

SCA BB Release 3.0.1

Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.0.1. See the *Cisco Service Control Application for Broadband User Guide* for a complete description

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.1. Note that some of these protocols are also available in the latest 3.0.0 protocol pack.

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
BaiBao	43	A P2P protocol.	Assigned to the default P2P service
PPLive	44	A protocol for free online TV	Assigned to the default P2P service
Mobile MMS	46	Multimedia Messaging Service, for sending text messages on mobile devices	Assigned to the default Instant Messaging 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 applications	Assigned to the default P2P service
NTP	54	Network Time Protocol	Assigned to the default Net-Admin service
HTTP Tunnel	55	Standard HTTP used for tunneling	Added to a new "Tunneling" service.

Mobile MMS Classification

Mobile MMS classification, which was added in release 3.0.1, 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 Zone named "MMS Servers";

Step 2. Add the IP address of the provider's MMS server to the "MMS Servers" zone.

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

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:

BitTorrent is missing from some P2P reports

- Cisco number: CSCsc96183

  BitTorrent protocol was missing from some P2P reports in the Reporter, because it was erroneously left out of the P2P protocol family.

  This issue is fixed in this release.

Duplicate DNS service element after upgrading to 3.0 from 2.5.7 Protocol Pack

- Cisco number: CSCsd00389

  When opening a PQB file from 2.5.7 protocol pack in the SCA BB Console 3.0.0, and trying to add or edit a service element, the GUI displayed an error message. This was caused by a duplicate DNS service element, which was automatically created when the PQB from 2.5.7 was loaded into the 3.0.0 GUI.

  This issue is fixed in this release.

Flavors and zones should be cleared before importing from CSV files

- Cisco number: CSCsc96184

  When importing Zones and Flavors from a CSV file into a Service Configuration, the zone items and flavors items were added on top of existing items.

  In this release, old items are removed before the items from the CSV file are added.

SCE RADIUS Sniffer stopped abnormally

- Cisco number: CSCsd27022

  After a few minutes of sniffing RADIUS traffic, the SCE RADIUS Sniffer stopped generating RADIUS RDRs, due to internal error while extracting RADIUS attributes from traffic.

  This issue is resolved in this release.

P2P protocols are not detected on ports 443, 1720 and 2775

- Cisco number: CSCsd34501

  All P2P protocols are now detected correctly on all TCP and UDP ports.

Multiple "Traverser Guard Watchdog" errors cause SCE platform failure

- Cisco number: CSCsd36114

  SCA BB caused multiple errors in the SCE debug-log, eventually causing the SCE platform to reboot. The errors were:

  - "Traverser Guard Watchdog"
  - "SE Watchdog Module: A problem occurred"

  The root cause was a problem with the MGCP protocol signature, which caused the above errors, and finally caused the SCE reboot.

  This problem in the MGCP signature is resolved in this release.

HTTP 0.9 flows not controlled by the SCE platform

- Cisco number: CSCsd17487

  Flows in which the first payload packet started with 'GET', but didn't match HTTP 1.0/1.1 pattern (such as 'HTTP 0.9' flows), might not have been reported or controlled by the SCE platform.

  This issue is resolved in this release.

Compatibility Information

SCA BB 3.0.1 should be used with the following components:

- SCOS 3.0.1
- SCMS-SM 3.0.0, 3.0.1
- SCMS-CM 3.0.0

Capacity Information

SCA BB 3.0.1 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

SCA BB Release 3.0.0

Release Objectives

Cisco Systems introduces Cisco Service Control Application Release 3.0.0, the first major release of the product since Cisco acquired P-Cube in October 2004. The Cisco Service Control Application product line is a direct continuation of the P-Cube Engage product line and uses the same numbering scheme. Cisco Service Control Application 3.0.0 (SCA 3.0.0) is the Cisco Service Control solution for broadband and mobile service providers. It is used to gain visibility and control over the distribution of network resources and to optimize traffic according to the provider's business strategies. The solution helps service providers reduce network costs, improve network performance and customer experience, and create new revenue-generating service offerings and billing packages.

Cisco SCA 3.0.0 delivers the next maturity level of service control, supporting the rapidly growing installed base of the Cisco Service Control solution with a superior infrastructure that provides a robust foundation for upcoming releases.

- Triple-play delivery
- New business models
- Service creation
- Service security
- Scaling
- Usability
- Solutions and architectures

Customers deploying Cisco SCA 3.0.0 can now, more than ever, feel the power of service control for analyzing and controlling their networks. By using Cisco Service Control, they become intimately familiar with their network traffic and can control their most important asset—their network—for increased revenue generation from their subscriber base.

Triple-Play Delivery

Service providers delivering the triple-play solution of data, voice, and video realize significant savings in infrastructure expenses by running all three technologies simultaneously over the same inexpensive IP transport. Cost savings increase profits and allow service providers to become more competitive. However, these savings cannot come at the expense of the subscriber's quality of experience.

Cisco SCA 3.0.0 offers service providers the ability to monitor the quality of their data, voice, and video services, and allows them to deliver the required predictable behavior of these services through its new FastPath™ solution that provides bounds on jitter and delay for mission-critical applications.

New Business Models

Service control technology was initially made available to broadband and mobile service providers. As the technology matured, the Cisco Service Control solution began to be deployed in the networks of other providers delivering services, such as managed enterprises, data centers, and Metro Ethernet. At the same time, the Cisco Service Control solution also became popular among enterprise and higher-education customers.

As an integral component of the Cisco product offering, Cisco SCA 3.0.0 builds on Cisco experience, knowledge, and proven technology in each of these markets. Deployment in these new markets requires the Cisco Service Control solution to accommodate new business models.

One example is the management of services in MPLS-VPN environments. Cisco SCA 3.0.0 incorporates the solid, field-proven Cisco IOS® Software, which helps service providers fully analyze and control the VPN traffic in an MPLS-VPN environment.

Service Creation

Innovative developments and infrastructure investment in the classification model of Cisco SCA 3.0.0 allow prompt support for many new protocols, and strengthen the policy model. As with every Cisco Service Control release, Release 3.0.0 delivers support for new services offered over network traffic. One of the new services introduced with release 3.0.0 delivers content filtering to protect subscribers from content they wish to avoid.

Realizing that a service control solution cannot always address and support all new and existing services, Cisco SCA 3.0.0 introduces a new service control concept that helps enable the support of any value-added service (VAS). With this capability, Cisco SCA 3.0.0 can work in tandem with expert systems dedicated to addressing and controlling such services. Cisco Service Control Engines running Cisco SCA 3.0.0 identify traffic belonging to a VAS and redirect it to one or more expert systems, which handle the traffic and return it for further processing. This ability to deliver service control capabilities for services that are not part of a specific release makes the Cisco SCA 3.0.0 solution an integral part of any service delivery that must scale rapidly, independent of product delivery schedules.

Service Security

Cisco SCA 3.0.0 places special emphasis on eliminating security threats from traffic. Based on Cisco security experience and expertise, Cisco SCA 3.0.0 is dedicated to securing valuable network resources against malicious attacks both by mitigating them as they occur and by taking preventive measures before they occur. These protective and preventive measures address known as well as new attacks.

Scaling

As service control becomes a mainstream network technology, major providers need to scale into any network size, capacity, and topology. The new Cisco SCA 3.0.0 infrastructure helps customers meet required scalability levels for current and future growth.

Subscriber integration has been enhanced to accommodate any RADIUS, Dynamic Host Configuration Protocol (DHCP), or other authentication, authorization, and accounting (AAA) environment. Direct and indirect integrations are enabled to fit any integration philosophy.

Usability

This release places special emphasis on improving the usability and serviceability of the solution across all its aspects.

One of the major usability enhancements implemented in Cisco SCA 3.0.0 is the consolidation of all graphical clients and tools under one unified framework. The new framework provides an ideal environment for interoperability, which integrates all tools used for managing and monitoring the product components. It automates the most common user activities, and it delivers an open and extensible platform for accommodating new tools in the future.

Solutions and Architectures

The ability to understand and control network content is critical to the evolution of network technology. As a strategic and innovative network technology leader, Cisco has realized the important evolutionary role of service control and constantly strives to transparently integrate service control technology into all its network architectures and solutions. Cisco SCA 3.0.0 is taking the first significant steps toward this goal by integrating with multiple new and existing Cisco architectures and solutions.

For example, Cisco SCA 3.0.0 is the intercept application manager (IAM) component in the CableLabs® PacketCable™ Multimedia (PCMM) architecture, it integrates into the Cisco Mobile Exchange framework, and it provides an application control point for IP Multimedia Subsystem (IMS) and non-IMS applications in Cisco IMS architectures. The service control solution also plays a central role in the Cisco Service Exchange Framework (SEF), and it supports the required interfaces for integration into the Cisco IP Next-Generation Network management framework.

Many more physical and logical integrations into Cisco solutions and architectures are planned for follow-up releases of Cisco Service Control.

Summary

Cisco SCA 3.0.0 was designed and built to facilitate evolutionary progress toward making service control solutions a mainstream network technology. The abilities to support any service required by new and existing markets, accommodate any network scale and architecture, and integrate into the large variety of solutions offered by Cisco make Cisco SCA 3.0.0 the ideal deployment choice.

New Features

The following sections list the major new features in SCA BB 3.0.0. See the *Cisco Service Control Application for Broadband User Guide* for a complete description.

Enhanced Classification Model

The classification model of release SCA BB 3.0.0 is extensively enhanced to improve the accuracy, efficiency, and robustness of this core solution capability. Although most of the technical details are outside the scope of this document, some of its benefits and their impact on the solution's robustness are provided.

Signature Detection on All Ports

Before network elements were capable of performing stateful deep packet inspection, network devices detected applications based on the applications' TCP/UDP port numbers. Today, when many standard protocols dynamically negotiate the ports they use, and the majority of network traffic uses nonstandard protocols, port classification is quite useless. With previous SCA BB releases, HTTP, FTP, and all P2P protocols were identified on all ports. Starting with release 3.0.0, SCA BB no longer relies on TCP and UDP ports for any protocol classification; it identifies all protocols based on traffic signatures. Each traffic flow, regardless of its port number, is compared against all protocol signatures. The patented SW/HW architecture of the SCE platforms enables this important classification improvement without performance penalty.

Enhanced Dynamic Signature Script (DSS)

The DSS enhancements in SCA BB 3.0.0 allow a much more flexible signature definition using dynamic configuration. This allows support for additional protocol signatures without the need for a software upgrade. In addition, a Signature Editor allows users to define their own signatures.

The enhanced expression powers of the Signature Editor include:

- Search for single or multiple strings anywhere in the payload
- Length-bounded search
- Search within payload and across packets

Protocol Flavors

Protocol flavors provide an additional level of granularity in defining services in the SCA BB solution. A protocol flavor uses an additional protocol attribute in classifying a service, making this service a "flavor" of the service based on the protocol only. As an example, the User-agent attribute of the HTTP protocol could be added as a protocol flavor, allowing the definition of all HTTP traffic generated by the same browser type (indicated in the user-agent field) as one service. Note that all existing parameters that add granularity to service definitions, such as the destination address, are still applicable for flavors.

The following table lists the flavors defined in SCA BB 3.0.0:

Flavor Type	Applicable for protocol	Valid Values
User Agent	HTTP RTSP	Prefix string
URL	HTTP	<host suffix, path prefix, path suffix, URL params prefix> o Host—From the beginning of the URL till the first '/' o Path—The section from the first '/' to the '?' o URL params—Any string following the '?' (It is not required to start the params prefix with '?')
Host Name	RTSP SMTP	Host suffix
SIP Source Domain	SIP	Host suffix
SIP Destination Domain	SIP	Host suffix
Composite Flavor (Composite Flavors are pairs of two defined flavors)	HTTP	<user agent flavor, URL flavor>
	RTSP	<user agent flavor, host name flavor>
	SIP	<SIP source domain, SIP destination domain>

The default configuration contains the following predefined flavors: HTTP Streaming Agents, Vonage as Source, and Vonage as Destination. When loading old PQB files, the HTTP Streaming and Vonage protocols are automatically replaced by these predefined flavors. The HTTP Streaming and Vonage services remain unchanged.

The Host/URL Lists feature of 2.5.x is replaced in SCA BB 3.0.0 by the HTTP URL flavor. When loading old PQB files, Host/URL lists are automatically converted into HTTP URL flavors.

The term IP List used in 2.5.x is replaced by the term Zone.

Classification Configuration Flexibility

The configuration of the enhanced classification model of SCA BB 3.0.0 is more flexible. For example, services and protocols can be defined using wildcards and port ranges.

Another example of this flexibility is the separation between ports and signatures, which gives the user more power when partitioning the network traffic, such as the following service partitioning:

- Service A—All FTP traffic on port 21
- Service B—All FTP traffic on ports other than 21
- Service C—All non-FTP traffic on port 21

SCA BB Console GUI Framework

One of the major usability enhancements implemented in SCA BB 3.0.0 is the consolidation of all graphical clients and tools in one unified framework.

The new framework achieves the following main goals:

- Provides a unified environment for client interoperability that integrates all tools used for managing and monitoring the product's components
- Automates the most common user activities
- Delivers an open and extensible platform for accommodating future new tools

The framework delivered as part of SCA BB 3.0.0 supports the following clients and tools:

The Network Navigator (new)

The Network Navigator is a new tool introduced with the SCA BB 3.0.0, which provides the ability to group devices together and apply the same configuration on them.

Specifically, the Network Navigator helps the user in performing the following activities on one or more devices:

- Install or upgrade software, including signature updates
- Apply or retrieve configurations, assuring consistent policy across devices
- Monitor operational state for maintenance and troubleshooting
- Start and stop devices
- Extract logs and support info

The list of network devices in the Network Navigator can be shared between users by exporting it to a file.

The Network Navigator uses a Password Manager, so that users do not have to provide passwords for multiple devices more than once.

The Service Configuration Editor

The Service Configuration Editor provides a service configuration editing view; it existed in previous releases of SCA BB.

The Reporter (improved)

The Reporter generates useful graphs, charts, and reports for traffic usage analysis based on the information collected by the CM. The Reporter existed in previous releases of SCA BB. The Reporter is greatly enhanced as part of SCA BB 3.0.0 (see the *Release Notes for Cisco SCA Reporter* for more information).

The SCA BB Subscriber Manager Client

The SCA BB Subscriber Manager Client provides an interface for controlling the subscribers DB in the SM; it existed in previous releases of SCA BB.

The Signature Editor (new)

The Signature Editor tool is a new addition in SCA BB 3.0.0. It provides an interface for defining new traffic signatures that can be uploaded to SCA BB to enable the recognition of new protocols.

Detailed VoIP Transaction RDRs

This release includes the support for detailed Transaction Usage RDRs for MGCP and SIP sessions using the same SCA BB VoIP RDR template used for the H.323 protocol.

Below is the description of some of the VoIP RDR fields (for complete details see the *Cisco Service Control Application for Broadband Reference Guide*):

RDR Field Name	Type	Description
APPLICATION_ID	UINT32	The ITU-U vendor ID of the application
UPSTREAM_PACKET_LOSS	UINT16	The average fractional upstream packet loss for the session, taken from the RTCP flow
DOWNSTREAM_PACKET_LOSS	UINT16	The average fractional downstream packet loss for the session, taken from the RTCP flow
UPSTREAM_AVERAGE_JITTER	UINT32	The average upstream jitter for the session in units of 1/65 millisecond, taken from the RTCP flow
DOWNSTREAM_AVERAGE_JITTER	UINT32	The average downstream jitter for the session in units of 1/65 millisecond, taken from the RTCP flow
UPSTREAM_PAYLOAD_TYPE	UINT8	The upstream RTP payload type for the session
DOWNSTREAM_PAYLOAD_TYPE	UINT8	The downstream RTP payload type for the session
MEDIA_CHANNELS	UINT8	The number of data flows that were opened during the session

Dual Link BW Control

This feature allows the enforcement of Global Controllers (GCs) over traffic that spans over two links. Using an SCE 2000 4xGBE platform for controlling these two links, the administrator can define the GC limit on the total throughput of both links. Enforcing BW limitation on the sum of two links can be activated in the Global Controller Settings dialog box of the Service Configuration Editor.

Value Added Services (VAS) Integration

The VAS integration capability allows classification and control of services not currently supported by SCA BB. The concept behind this capability is that the solution should use an external expert system for classification and control of the service traffic.

With this new capability, traffic of such a new service is forwarded by the SCE to the preconfigured destination of the expert system (VAS server). After appropriate processing, the traffic is sent back to the SCE, which then sends it to its original destination. The decision to forward traffic is based on the policy applied for the subscriber using the service and on characteristics of the traffic. These settings are configured in the Service Configuration Editor.

More information about VAS configuration can be found in the *Cisco Service Control Engine Software Configuration Guide*.

Enhancements for Billing

The SCA BB solution provides a prepaid and postpaid, comprehensive, charging-interface for charging and quota systems.

The following enhancements to the interface are added to SCA BB 3.0.0:

Transaction Usage RDR Volume Threshold

Transaction Usage RDRs (TURs) provide very granular reporting information, and are useful for billing purposes. This high granularity is often translated into a large volume of TURs, which may require more powerful and expensive collection systems. In order to reduce the volume of TURs, a global volume threshold is defined with SCA BB 3.0.0, so that each TUR describing a transaction whose total volume is lower than this threshold is not reported.

The global volume threshold is configured in the Service Configuration Editor.

The global volume of all TURs not generated due to this threshold is recorded, and can be obtained using a root CLI command.

Periodic TUR Generation

For very long transactions, it may not be enough to wait until the end of the transaction to generate a TUR. SCA BB 3.0.0 allows the generation of interim TURs for such transactions. Whether to generate the interim TURs and the generation time interval are configured in the Service Configuration Editor.

HTTP and RTSP Application Layer Attributes

The following application layer attributes are added to Transaction Usage RDRs:

- RTSP URI
- HTTP user-agent

Real-Time Signaling

When performing stateful deep packet inspection at the application layer (layer 7) on all traffic flows, the SCE identifies many network events that are used by SCA BB for policy resolution. In many solution architectures it is useful to share these network events with external systems. The real-time signaling mechanism externalizes events such as session establishment and termination, and malicious traffic start and stop.

One use case that is specifically targeted by SCA BB 3.0.0, is acting as a Packet Cable Multimedia (PCMM) Intercept Application Manager.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.0.0. Note that some of these protocols are also available in the latest 2.5.7 and 2.5.8 protocol packs.

Protocol Name	Protocol ID
DNS	933
PTT Winphoria	61
RTP	57
https	358
imap	59
tftp	60
IRC	62

Removed Features

SM Quota API

The SM Quota API is obsolete; the SCE Subscriber API replaces it. This allows direct connection from the policy server to the SCE for subscriber quota provisioning. See the *Cisco SCMS SCE Subscriber API Programmer's Guide* for more information.

Subscriber quota across log-ins

Subscriber quota is no longer maintained by SCA BB across subscriber log-ins. Upon subscriber log-out, the remaining quota buckets associated with this subscriber are reported, and it is assumed that the external quota provisioning system will maintain them until the subscriber logs in again.

Weekly and monthly quotas

As part of the internal quota management configured through the SCA BB console, weekly and monthly quotas are deprecated from SCA BB 3.0.0 and only daily and hourly quotas are supported.

Resolved Caveats

The following caveats from 2.5.x have been resolved for this release:

Transactions not properly mapped for Generic TCP/UDP

- Cisco number: CSCpu08391

Editing service transaction mapping can clear list selection

- Cisco number: CSCpu10609

RPC server error during GUI installation

- Cisco number: CSCpu10637

Dropped packets/bytes counters unavailable in Cisco-SCAS-BB MIB

- Cisco number: N/A

Quota reset when subscriber becomes introduced (pull mode)

- Cisco number: CSCsb78012

Default service rule refers to an invalid BW controller

- Cisco number: CSCsc44706

In releases earlier than 2.5.8, the Default Service Rule in each package contained an invalid mapping of traffic to the default 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 this release. Old PQB files are automatically repaired when used in this release. 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.
```

Compatibility Information

SCA BB 3.0.0 should be used with the following components:

- SCOS 3.0.0
- SCMS-SM 3.0.0
- SCMS-CM 3.0.0

Upgrade Information

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

- SCA BB 3.0.0 does not use the same Default DSS that was installed for older 2.5.x releases.
- If a protocol pack for SCA BB 3.0.0 is available, it should be installed on top of a SCA BB 3.0.0 installation. Do not install a 2.5.x protocol pack on top of SCA BB 3.0.0.

For complete upgrade information, see the *Cisco Service Control Application for Broadband – Guide to Upgrading to SCA BB 3.0*.

Capacity Information

SCA BB 3.0.0 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000)	80,000	1.7M [850K bidirectional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bidirectional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	1.7M [850K bidirectional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bidirectional]
SCE1000_1.5U (EngageDefaultSCE1000)	40,000	620K [310K bidirectional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	800K [400K bidirectional]

Open Caveats

Traffic Processing

Traffic Classification

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

- Cisco number: CSCsd81077

  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.

Flow capacity deteriorates when HTTP URL table is full

- Cisco number: N/A

  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 Capacity Information.

Traffic Accounting and Reporting

Handlers should get more CPU time

- Cisco number: CSCsg28867

  When using a large number of package counters, if the PUR generation interval is set below 5 minutes PURs will sometimes be generated for only some packages and services.

  Workaround: Always set the PUR generation interval to 5 minutes or more. If a shorter interval is needed, do not use more than 64 package counters.

  This issue is due to a limitation of the CPU time allocated to certain operations by the SCE OS.

Inaccurate report for number of active subscribers

- Cisco number: CSCsg50079

  Under certain conditions, PUR and LUR reports has a value of ACTIVE_SUBSCRIBERS that is greater then TOTAL_ACTIVE_SUBSCRIBERS.

  Currently this issue is believed to exist only when working in subscriberless mode. (In this mode, the value of these 2 fields should be 1 at most)

Subscribers are counted and reported in subscriberless mode

- Cisco number: CSCsg50099

  In some cases, when working in subscriberless mode, the number of subscribers reported in PUR or LUR is greater than 1 (the maximum expected).

  Workaround: These values can be ignored.

Reported volume lower than that reported by other network devices

- Cisco number: CSCsa94382

  Reported volume of network traffic might be lower than the volume reported by other network devices monitoring the same link. This can happen for the following reasons:

  - The SCE bypasses non-IP traffic and some types of encapsulated traffic

- The SCE bypasses traffic that it identifies as being part of a network attack
- The SCE application counts L3 volume, while other network devices might be counting L1/2 volume
- Traffic filtered by filter rules is not counted by the SCE application
- The SCE application does not count TCP retransmitted packets and packets with checksum errors

To get a more accurate counter of the amount of traffic that passed through the SCE, including the attack volume and the traffic that was mapped to a filtered traffic rule, you can configure a traffic counter that will count packets/bytes of all this traffic. This counter can be monitored via CLI or SNMP. For more information about traffic counters and how to configure them, see the *Cisco Service Control Engine Software Configuration Guide*.

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

- Cisco number: N/A

The number of concurrent sessions reported by the SCE application can sometimes be lower than the number of open flows in the SCE platform counters. In certain services, such as VoIP and FTP, a single session 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.

Inaccurate numbers of active subscribers and concurrent sessions

- Cisco number: CSCsa77598

The number of concurrent sessions is not decreased immediately when a session ends. This is because some sessions are closed only after a certain period of inactivity since the last packet. Only then is the concurrent session counter is updated. This is most common in UDP sessions, such as VoIP calls, and may cause both the concurrent sessions counter and the active subscribers counter for these services to show inaccurate values.

Also, in rare cases, sessions that cause internal errors in the SCE are not tracked properly. The concurrent sessions and active subscribers counters will reflect that these sessions ended only when the subscriber logs out. Such error incidents are usually logged in the SCE debug log.

Skype reporting limitations

- Cisco number: CSCsb05427, CSCsb05425, CSCsb05422

  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.

Reporting volume of bundled flows on multiple links

- Cisco number: CSCpu13647

  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 will 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 SCA Reporter, although the total volume and bandwidth reports will remain accurate.

BW reports may contain spikes after DoS attacks

- Cisco number: CSCpu10822

  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.

Clarification regarding VoIP accounting

- Cisco number: CSCsb67206

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

Incorrect Values in Session ID field in RTSP TUR

- Cisco Number CSCsb60539

  When enabling TURS 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.

Traffic Control

Quota Threshold RDRs are not supported for Number of Sessions bucket

- Cisco Number CSCsg08507

  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.

Flow redirection and blocking might not work in cascade mode

- Cisco Number CSCse23591

  Flow redirection and blocking may not work in cascade setups, since the injected packets are sent on the wrong links. (Note that regarding blocking on a TCP connection, packets will be blocked even if the RST packet is not sent correctly.)

  In cascade setups, one SCE platform is configured to handle "link-0" and the other is configured to handle "link-1". The problem occurs only on the box configured as "link-1", regardless of the priority configuration.

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 because additional uncontrolled traffic, such as traffic filtered by traffic filter rules, is also assigned to this GC.

  Although the amount of uncontrolled traffic is very small, it is nevertheless recommended not to use this GC for BW control, and to keep its BW limit set to 100%.

Resolution limitation on quota breach detection

- Cisco number: CSCpu10470

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

SCA BB Console

General

A duplicate DNS service element is created after upgrading to 3.0.0 from 2.5.7 protocol pack

- Cisco number: CSCsd00389

  When opening a PQB file from the 2.5.7 protocol pack in the SCA BB Console 3.0.0 and trying to add or edit a service element, the following error appears: "*Item uniqueness violation error: duplicate Service Element*". This is caused by a duplicate DNS service element, which was automatically created when the PQB from 2.5.7 was loaded into the 3.0.0 GUI.

  Workaround: Delete the DNS duplicate service element. This service element is usually found under the "Net Admin" service.

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

- Cisco number: CSCsa91254

  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.

Limitations in navigating from the Reporter to the Service Configuration Editor

- Cisco number: N/A

  SCA BB allows the user 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.

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

- Cisco number: N/A

  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

Network Navigator configuration not removed when SCA BB Console uninstalled

- Cisco number: CSCsc32003

  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

Internet Explorer 5.5 (or up) required

- Cisco number: CSCsb20234

  SCA BB Console 3.0.0 requires that Internet Explorer 5.5 (or up) be installed on the workstation.

Uninstalling while GUI is open

- Cisco number: CSCsa94964

  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.

Must uninstall SCA BB Console before reinstalling it

- Cisco number: CSCsa94964

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

Network Navigator

Changing the port of the RPC server cause failure

- Cisco number: CSCsg29991

  After changing the RPC server port in a device (SM/CM/SCE), any subsequent invocation of this device from the Console will fail

  Workaround: Do not change the port number for RPC on devices that you intend to manage using the Network Navigator.

Two identical devices can be created

- Cisco number: CSCsa95657

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

Incorrect error message for failure to connect

- Cisco number: CSCsc49774

  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.

Running an FTP server on the workstation might cause Network Navigator operations to fail

- Cisco number: CSCsc27156

  For some operations, such as OS installation and support file extraction, the Network Navigator launches a local FTP server. If another FTP server is already running on the workstation, the operation might fail. See the *Cisco Service Control Application for Broadband User Guide* for Network Navigator networking requirements.

Concurrent operations on the same SCE platform are not supported

- Cisco number: N/A

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

Updating CM with service configuration values in a NAT environment

- Cisco number: N/A

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

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

  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

New protocols not assigned automatically to services in old PQB files

- Cisco number: N/A

  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.

Calendar window displayed incorrectly

- Cisco number: CSCsa98116

  When Windows is running a non-Western language, the hour table header on the calendar window is displayed incorrectly.

Signature Editor

Merging a custom DSS with a protocol pack

- Cisco number: N/A

  Users who have created a DSS in the Signature Editor, and would also like to install a protocol pack, need to merge their DSS with the signatures in the protocol pack. To do this, users should follow these steps:

Step 1. Extract the DSS from the protocol pack, by unzipping the protocol pack's SPQI file.

Step 2. Open your DSS and then import the protocol pack's DSS into the signature editor. Make sure there are no overlapping signatures IDs.

Step 3. Save the merged DSS.

Reporter

Reporter sometimes shows service number instead of service name

- Cisco number: N/A

  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

General

Apply failed with error when using flavor with illegal host suffix

- Cisco number: CSCsg48506

  When using a flavor with host suffix/prefix containing a colon the apply operation will fail.

  Workaround: Do not use a colon as part of the host suffix/prefix.

Reboot after apply causes the SCE to come up with no application

- Cisco number: CSCsg21233

  Symptom

  After applying a service configuration, there is a short period of time (~20 seconds) where rebooting the SCE causes it to come up with no application.

  Workaround: Do not reboot the SCE during the 20 seconds after applying a service configuration.

Applying service configuration might fail if the SCE platform is configured with a large lookup tables

- Cisco Number CSCse28465

  When configuring a very large number of entries (~10K) in more than one lookup table (such as services, HTTP URLs, Flavors), although a first apply operation will be successful, a second apply operation may fail due to RPC function failure. This is a result of exhaustion of the RPC resources, caused by the large number of RPC operations.

Subscriber notification on DoS attacks removed on PQI installation

- Cisco number: CSCpu11773

  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 installation.

Installing the PQI on the SCE with a non-default capacity option

- Cisco number: N/A

  SCA BB flow and subscriber capacity numbers can be tuned during the installation by selecting the appropriate capacity option. See Capacity Information for available capacity options for each SCE platform type.

  To install the PQI on the SCE with a non-default capacity option, you should install the PQI using CLI, and specify the name of the capacity option on the 'options' modifier of the PQI install CLI command.

  For example, to install the PQI with 'SubscriberLessSCE2000' capacity, use the following CLI commands:

```
#>configure
(config)#>interface LineCard 0
(config if)#>pqi install file eng30037.pqi options
capacityOption=SubscriberLessSCE2000
```

Persistent storage of service configuration might fail

- Cisco number: CSCpu10609

  In rare circumstances, the persistent storage of a service configuration on the SCE platform fails, although the new configuration is applied. This means that after the SCE platform 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: Reapply the service configuration if you receive the following error message:

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

Microsoft Excel may invalidate the format of SCA BB CSV file

- Cisco number: CSCpu10658

  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 in a vanilla text editor before importing the CSV file.

SCE log and SNMP traps when a service configuration is applied

- Cisco number: N/A

  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

Subscriber import exception for site with SCE having no service configuration applied

- Cisco number: CSCsg39206

  Importing subscribers into the SM may produce an error message when one or more SCEs in the domain are not reachable or do not have a service configuration applied.

  (There is no impact on functionality.)

Backward compatibility with SCA BB 2.5 Service Configuration API

- Cisco number: N/A

  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.

Unneeded connections should be closed

- Cisco number: CSCpu10580

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

Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page 65) 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* (on page 65), 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.