Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.1.0

June, 2007

Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.1.0

Covers: SCA BB 3.1.0

OL-8958-11

These release notes for the Cisco SCA BB describe the enhancements provided in Cisco SCA BB Release 3.1.0. These release notes are updated as needed.

For a list of the caveats that apply to Cisco SCA BB Release 3.1.0, see *Open Caveats*.

For further information, please refer to the following related Release Notes:

- Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.0.6
- Release Notes for Cisco Service Control Operating System (SCOS) 3.1.0
- Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 3.1.0
- Release Notes for Cisco Service Control Management Suite Collection Manager (SCMS CM) 3.1.0

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

Contents

Introduction

Cisco is proud to release version 3.1.0 of its Service Control Application for Broadband (SCA BB).

This document describes the new functionality, enhancements, and known issues in SCA BB release 3.1.0.

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

SCA BB Release 3.1.0

New Features

The following sections list the major new features in SCA BB 3.1.0. See the *Cisco Service Control Application for Broadband User Guide* for a complete description of these features.

Asymmetric Routing Classification

Routing protocols allow the creation of different routes for the upstream and downstream traffic of a flow. The result is that in some topologies the two directions of a flow do not pass through the same links and, therefore, not through the same SCE platform, which limits the ability to classify traffic. (This is most likely to occur when the insertion point for service control is at the peering point.) SCA BB 3.1.0 introduces the first step toward supporting classification when only one side of a flow traverses a specific SCE platform.

When the Cisco Service Control solution is deployed in an asymmetric routing environment and unidirectional classification is enabled, SCA BB classifies unidirectional flows more accurately while the classification accuracy of bidirectional flows is preserved. The SCE platform handles unidirectional flows independently, with no synchronization with other SCE platforms that might handle the flows in the opposite direction. Sizing should be performed when planning for deployment in such environments, since the transactions length is expected to be lower, reducing the effective SCE performance envelope.

In release 3.1.0, SCA BB can identify 56 distinct protocols based on only one flow direction, including the network's most common protocols, for example, HTTP, and P2P application protocols including BitTorrent, eDonkey, Encrypted eMule, Gnutella, Warez, POCO, PPStream, and PPLive.

Behavioral P2P

SCA BB release 3.1.0 introduces a new classification mechanism that identifies P2P application traffic according to networking characteristics common to all P2P applications.

The Behavioral P2P mechanism tracks events in subscriber traffic that may indicate the existence of a P2P application. These events are stored in an internal, stateful database and if a flow is not classified using any other protocol signature, the database is consulted. If the flow appears to match the characteristics of P2P traffic, it is classified to the Behavioral P2P protocol signature.

Classification to a specific P2P protocol signature has a higher precedence than Behavioral P2P classification. This allows the service provider to set specific actions to known P2P protocols, if required.

The Behavioral P2P mechanism allows the correct classification of flows from new P2P applications or new version of applications that do not yet have a protocol signature defined in SCA BB.

Virtual Links

Virtual Links is a new global bandwidth control model. In Virtual Links mode, the physical link is divided into a set of smaller “virtual” links, which are separately monitored and controlled. Each Virtual Link has its own set of global controllers, which are initially defined by a Virtual Link “Template”. These global controllers can later be tuned dynamically according to need. The SCA Reporter provides per Virtual Link report capabilities similar to the per package capabilities.

A typical use case of this feature applies to cable modem operators, allowing them to enforce service tier policy per physical cable. Each physical cable can be managed and monitored as a virtual link within the SCE platform’s physical link.

Each physical link (that is, sub-interface representing an aggregation point, such as VLAN, VC, or CableModem) can be managed and monitored as a virtual link within the SCE platform’s physical link.

Protocol Support

The following table lists the protocols that were added in SCA BB 3.1.0. The table includes protocols that are also available in Protocol Pack 08. (See the Cisco Service Control Protocol Pack download page for links to Protocol Pack 08 files and information.)

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
Google Talk	1030	Instant Messaging	Added as a new protocol and to Instant Messaging Service
Feidian	1037	P2P, TV streaming	Added as a new protocol and to P2P Service
Club Box	1038	Commercial file sharing	Added as a new protocol and to Commercial File Sharing Service
Yahoo VoIP over SIP	1039	Yahoo VoIP service over the SIP protocol	Added as a new protocol and to Yahoo VoIP Service
Video over HTTP	1040	Video files downloaded over HTTP	Added as a new protocol and to HTTP Browsing Service
Audio over HTTP	1041	Audio files downloaded over HTTP	Added as a new protocol and to HTTP Browsing Service
Binary over HTTP	1042	Binary files downloaded over HTTP	Added as a new protocol and to HTTP Browsing Service
Baidu Movie	1043	Commercial file sharing	Added as a new protocol and to Commercial File Sharing Service
Behavioral P2P	1044	Commercial file sharing	Added as a new protocol and to Commercial File Sharing 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 3.1.0.

Protocol Name	Description	Cisco Number
Skype	Support the latest Skype 3.0 version	CSCsh68056
PPLive	Strengthen the TCP based signatures	CSCsi48429
eDonkey	eDonkey traffic is misclassified to Skype	CSCsh9943

Generic Upload/Download Protocol

The protocol Generic Upload/Download was renamed to Behavioral Upload/Download. This protocol is now enabled by default.

Removed Features

Generic Upload/Download Settings

Configuration of the Generic Upload/Download protocol has been removed from the GUI. Any non-default configuration of this protocol is lost.

Reporting of P2P File Extensions

The capability to extract and report file extensions of P2P download was removed. Hence, the Top P2P File Extensions report, which was produced based on this information, is no longer supported.

Backward Compatibility

Layer 7 Filtering

Layer 7 filtering can be used to extend the operating envelope of the SCE platform. It allows the DHT, Gnutella, Gnutella 2 Networking, and Warez protocols to be filtered according to their Layer 7 characteristics. Like all other filtered flows, Layer 7 filtered flows are neither classified, controlled, nor reported. The flows of the filtered protocols are typically short and their overall volume is negligible, which means that filtering these protocols has little effect on network bandwidth and on the accuracy of the SCA BB reports.

The Layer 7 filters are enabled by default. Disable specific filters in the Advanced Options dialog box.

Resolved Caveats

The following caveats are resolved in this release:

Traffic Processing

Traffic ClassificationNTPv2 is misclassified as Skype

- Cisco number: CSCsh90616

  NTP captures taken by customer's NTP server contain UDP traffic sequence that match one of the Skype signature.

  This issue is resolved in this release.

Redirect not working immediately when trying same URL again

- Cisco number: CSCsh74572

  The first time a browser is redirected from a web address, the redirect works as expected. If at this point the subscriber enters the same address at the browser's address bar, the browser will display a blank page for approximately one minute.

  This issue is resolved in this release.

DSS may cause SCE to Reboot

- Cisco number: CSCsi70172

  Dynamically loaded signatures (DSS) that contain a deep inspection clause for substring search may cause SCE vulnerability by triggering the internal protection mechanism (watchdog).

  This issue is resolved in this release.

HTTP URL extraction should be limited in size

- Cisco number: CSCsi73460

  Extraction of extremely long URLs may cause SCE vulnerability by triggering the internal protection mechanism (watchdog) due to timeout for HTTP URL parsing.

  This issue is resolved in this release.

Traffic Accounting and Reporting

Counting problem for protocols with different measurement method

- Cisco Number CSCsi25121

  SCA BB tracks sessions' time duration of VoIP protocols in two modes. The first accounting mode is for VoIP protocols where a single voice session runs over a single flow carrying both media and control data. In this case, SCA BB accounts and reports the flow's time duration. The other accounting mode is for VoIP protocols where a single voice session runs over multiple flows: a control channel and one or more media channels. The SIP protocol is one example of this type of VoIP protocol. For these VoIP protocols, SCA BB accounts and reports the time duration of the media channels only.

  Service counters' accounting mode can be one of the two types described above. This means that a service counter can count the time duration of only one type of VoIP protocol. If a service counter is assigned VoIP protocols of different types, it will operate in the mode determined by the majority of protocols. The time duration of protocols not matching the assigned service counter mode is not accounted for.

  In SCA BB 3.1.0, the VoIP services hierarchy and service counters assignment were restructured to obtain accurate VoIP call duration accounting and reporting. This change was applied to the default service configuration only. To correct the accounting of an existing service configuration, amend the service configuration using the service configuration editor.

  The VoIP protocols that have sessions with separate flows for the control channel and media data are: SIP, H323, MGCP, Skinny, Yahoo VoIP over SIP, ICQ VoIP, Primus, and PTT Winphoria SIP. These protocols should not be assigned service counters with other protocols, including other VoIP protocols.

  This issue is resolved in this release.

Malicious Traffic RDR timestamps have mismatch

- Cisco Number CSCsg80079

  The END_TIME field in MALUR RDRs is skewed by an amount of time equal to the offset from GMT configured in the SCE.

  This issue is resolved in this release.

Discrepancy in reported call minutes between Link and Media Reports

- Cisco Number CSCsh79386

  The call minutes reported in RDRs for SIP and Skype calls differ between RPT_MEDIA and RPT_LUR. The RPT_LUR field will, in some cases, be consistently higher (by up to 10%) than the corresponding RPT_MEDIA field.

  This issue is resolved in this release.

Missing PUR RDRs

- Cisco number: CSCsg28867 (Handlers should get more CPU time)

  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.

  This issue is resolved in this release.

Traffic Control

QP session limit allows Number of Sessions + 1 before applying breach action

- Cisco Number CSCsh24604

  When working with External or Internal Quota Provisioning and limiting the number of sessions, subscriber is allowed for one extra session than his quota allows him.

  This issue is resolved in this release.

QP redirected (due to quote depletion) sessions are counted as used

- Cisco Number CSCsh24612

  When subscriber reaches depletion he will be redirected to the notification destination URL. The sessions for which the subscriber was redirected upon are also being counted as used sessions so if the next quota event will be Add Quota, those redirected sessions will be reduced from the amount of sessions this subscriber is now allowed to have.

  This issue is resolved in this release.

Internal quota with SM pull mode not working properly

- Cisco Number CSCsi02186

  When using SM in pull mode, with internal quota, a subscriber will not get the configured quota upon login. When traffic is consumed, this subscriber will enter a breach state.

  This issue is resolved in this release.

Quota Replenish Scatter - does not work as expected

- Cisco Number CSCsi46479

  Quota management is configured to work in periodical mode, i.e. subscriber quota is replenished every hour or day, and quota replenish is scattered around the due time, which is the top of the hour or midnight.

Subscribers which their quota should be replenished before the top of the hour (1/2 of the subscribers) constantly get new quota during the time between their scheduled quota replenish and the top of the hour. For instance, subscriber that is scheduled for new quota at 11:55 receives new quota between 11:55 and 12:00.

This issue is resolved in this release.

Concurrent session limitation is not working

- Cisco Number CSCsi33779

  Concurrent session limitation might not be enforced properly after applying a new limitation and in particular in transition between unlimited policy and a limited one, and vice versa. The incorrect limitations enforcement applies only to subscribers that have open sessions at the time of the policy change. A concurrent session limit change can be due to applying of a service configuration or a change in the subscriber's package.

  This issue is resolved in this release.

Miscellaneous

Services are sometimes shown by number in reports

- Cisco Number CSCsg84258 (Value.INI not properly updated upon apply from some PCs)

  In extremely rare cases, the Reporter will show certain services by their numbers instead of by their symbolic names. The problem occurs in the second apply when a policy has been applied via the console, then modified by renaming, adding, or deleting services and reapplied.

  This issue is resolved in this release.

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.

  This issue is resolved in this release.

Enable/disable of Anomaly Detection does not enable/disable the attack filter

- Cisco Number CSCsh41269

  Enabling or disabling of the Anomaly Detection in the SCA BB Console does not enable/disable the attack filter.

  This issue is resolved in this release.

PQI install is not saving all the application configuration

- Cisco Number CSCsi01743

  A PQI install (by CLI) does not save the configuration of RDR tag mapping to categories and the packageId per template index.

  If the SCE is then rebooted without a prior apply, this configuration is cleared.

  This issue is resolved in this release.

Compatibility Information

SCA BB 3.1.0 should be used with the following components:

- HW Platform SCE-1010-2XGBE 2U

  SCE-2020-4XGBE

  SCE-2020-4/8XFE
- SCOS 3.1.0
- SCMS-SM 3.1.0
- SCMS-CM 3.1.0, 3.0.6, 3.0.5, 3.0.3

  Virtual Links reporting capabilities are only supported with CM 3.1.0.
- SCA Reporter 3.1.0

  The Reporter is also packaged with the SCA BB Console.

For more information regarding compatibility between Service Control components, refer to the *Cisco Service Control Application for Broadband Download Guide*.

Capacity Information

SCA BB 3.1.0 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

Content Filtering-CPA client hangs when losing connection to the server

- Cisco Number CSCsi67423

  Given an HTTP URL, the CPA client queries the Surf Control Server for a category that is used to map the HTTP flow to a service. If the connection to the Surf Control Server becomes unavailable, the CPA client hangs and no succeeding queries are made. Due to this defect, the CPA client and the HTTP Content Filtering classification are disabled in this software release.

L7 functionality is not supported for HTTP traffic that is not browsing

- Cisco Number CSCsi31670

  L7 functionality is not supported for HTTP traffic that is not classified by the protocol library as HTTP browsing (for example, Flash and HTTP download protocols). The features that are not supported for these protocols are: flavors classification (including contents filtering), redirection, subscriber notification, HTTP RDRs, and reporting of URLs. This also means that flows mapped to these protocols are not included in the Top Web Hosts report.

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

Radius/DHCP sniffer in SCE might stop functioning for certain flows

- Cisco number: CSCsi82268

  In some cases, the interception of RADIUS and DHCP events stops functioning and notifications on these events are not sent. As a result, subscriber information is not provisioned to the SCE.

  Workaround:

  - Make sure that the SCE is working within its capacity envelope.
    - The most popular mitigation for capacity issues is to filter *all* UDP traffic other than RADIUS
  - Contact the BU for chirurgical recovery of these specific flows
  - As a last resort, perform shutdown and then no-shutdown for the SCE.

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 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: CSCsd74145

  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.

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: N/A

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

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

Incorrect Values in Session ID field in RTSP TUR

- Cisco Number CSCsb60539

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

Traffic Control

Virtual links is not supported for the SCE1010 platform

- Cisco Number CSCsi86983 (apply policy failed on SCE1010)

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

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

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

Installing OS Fails with an Error

- Cisco number: CSCsi80412

  Sometimes when installing SCOS on an SCE platform using the Network Navigator, the operation appears to fail after a number of minutes and the following error message appears on the screen: “Failed to update OS: the connection is not active.” The Network Navigator prompts the error message when the installation takes longer than expected even though the installation is proceeding. When this error message is displayed, do not take any action; wait for the SCE platform to load with the new SCOS installation.

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

Signature Editor does not limit searchable range

- Cisco Number CSCsi92754

  The Signature Editor must not allow users to configure substring search that searches a string in a range that exceeds 100 bytes. Searching a specific string within a wide range delays packet processing significantly which may trigger a traversal watchdog.

Merging a custom DSS with a protocol pack

- Cisco number: N/A

  If you have created a DSS in the Signature Editor, and would also like to install a protocol pack, you need to merge the DSS with the signatures in the protocol pack. To do this, 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

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.

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

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 26) 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 26), 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.