Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.1.5

Covers: SCA BB 3.1.5, SCA BB 3.1.1, SCA BB 3.1.0

Part no.: OL-14439-03

These release notes for Cisco SCA BB describe the enhancements provided in Cisco SCA BB Release 3.1.5. These release notes are updated as needed.

For a list of the caveats that apply to Cisco SCA BB Release 3.1.5, see Open Caveats, page 22.

For further information about SCA BB, please refer to:

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

For further information about related products, please refer to the latest versions of the following Release Notes:

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

Contents

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

Introduction

This document describes the new functionality, enhancements, and known issues in SCA BB release 3.1.5.

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.

For a list of the caveats that apply to Cisco Service Control Application for Broadband (SCA BB) 3.1.5, see Open Caveats, page 22

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

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

SCA BB Release 3.1.5

This module describes functional enhancements, backward compatibility, resolved issues, and capacity of SCA BB release 3.1.5.

Information About Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.1.5. See the *Cisco Service Control Application for Broadband User Guide* for a complete description of these features.

Protocol Support

Refer to the Protocol Pack Notes for information regarding protocol support for Protocol Pack #11 (included in SCA BB 3.1.5).

DSCP Marking Enhancements

SCA BB release 3.1.5 decouples DSCP marking from the SCE platform queuing mechanism and provides a simplified GUI configuration for DSCP marking based on seven possible DSCP values. After an application is classified by the SCE, the DSCP-marking functionality can mark the relevant packets per package, service, and traffic direction.

Managing MPLS-VPN Branches

SCA BB release 3.1.5 extends the functionality of managing an MPLS-VPN encapsulation as a managed subscriber by supporting the ability to define a branch or site as the managed subscriber. The solution provides DPI usage analysis and control per branch of an enterprise in an MPLS-VPN encapsulation.

Identifying Subscribers per VLAN ID and IP

SCA BB release 3.1.5 adds the ability to define a subscriber through a combination of VLAN ID and IP address range (subnet).

Flexible Subscriber Introduction

With the introduction of SCA BB release 3.1.5, the Radius Listener LEG component of the Subscriber Manager infrastructure can now leverage a Regular Expressions infrastructure for extracting and manipulating VSA attributes.

Configuration Wizards

SCA BB release 3.1.5 includes several configuration wizards for the SCA-BB policy client that enable the configuration of predefined use cases while hiding the configuration complexity of these use cases. This is achieved by walking the end user through the configuration steps and simplifying the configuration process, while making sure that all system elements are properly configured. At the end of the process, the device (SCE, CM, and so on) is configured and ready to go.

Report Coloring

SCA BB release 3.1.5 enhances the SCA BB Reporter by providing a coloring scheme that is persistent between different sessions of the Reporter. The release also provides the capability for a user to define colors for the datasets of the entities.

Information About Backward Compatibility

This section describes backward compatibility between SCA BB release 3.1.5 and earlier releases of SCA BB.

MPLSL3-VPN Encapsulation

SCOS 3.1.5 has improved the definition and context of a subscriber in an MPLSL3-VPN domain. While in previous releases a *subscriber* referred to all the traffic of a specific VPN mapped to a specific PE, in release 3.1.5 the MPLSL3-VPN subscriber can be defined as all the traffic from a specific CE. This is achieved by using the detailed subnet information of each CE and integrating it with the subscriber definition.

This change imposes backward compatibility issues and the definition of new interfaces for the specification of the CE as a subscriber in the MPLSL3-VPN domain. This new concept and mode of operation is the only one that is supported in release 3.1.5.

DSCP Marking

The concept of mapping traffic portions to a specific DSCP value has changed in release 3.1.5.

In previous versions of the SCA BB solution, the mapping was only possible based on the CoS (Diffserv Class of Service) to which the service was mapped. Starting with 3.1.5, it is possible to map each service to one of seven configurable DSCP values independently.

The old DSCP marking mode is no longer supported.

Information About Resolved Caveats

This section describes caveats that are resolved in SCA BB release 3.1.5.

Quota State Restore RDR should be issued at package change

- Cisco number: CSCsk09831

  The previous product behavior was to issue a Quota State Restore RDR only at login. The Quota State Restore RDR should be issued also when there is a package change (when the quota is managed externally).

  This issue is resolved in this release.

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.

  This issue is resolved in this release.

Protocol pack installation process is not intuitive

- Cisco number: CSCsk55440

  After installing a protocol pack, the user must perform immediately a retrieve policy operation. The protocol pack installation process should prevent the user from applying a policy before the retrieve policy operation, as doing this results in unpredictable damage to the classification process.

  This issue is resolved in this release.

Remove 'lately used' setting from the Advanced settings dialog

- Cisco number: CSCsk04251

  The "Classification based on recent classification history enabled" option in the SCA-BB GUI 'Advanced settings' dialog is now obsolete and should be removed.

  This issue is resolved in this release.

Remove 'SW Filter tunables' from the Advanced settings dialog

- Cisco number: CSCsk53535

  The SW Filter tunables should not appear in the SCA-BB GUI 'Advanced settings' dialog.

  This issue is resolved in this release.

Quota State Restore RDRs should not be sent for internal quota

- Cisco number: CSCsj95411

  Quota State Restore RDRs are being generated for all subscribers who are logged in, irrespective of whether those subscribers have external quota management or internal quota management enabled. The expected behavior is that Quota State Restore RDRs should only be generated for subscribers who have external quota management enabled.

  This issue is resolved in this release.

Number of active subscribers reported to be more than total subscribers

- Cisco number: CSCsk57446

  The "Package usage RDRs" may sometimes report the number of active subscribers on a service to be more than the total number of subscribers active in the package.

  This issue is resolved in this release.

POP3 account not inserted into INFO_String field (Thunderbird)

- Cisco number: CSCsk09944

  When Thunderbird is used as the mail user agent, POP3 account is not inserted into the INFO_String field on Transaction RDR, even though Thunderbird successfully sends the POP3 account to the mail server.

  This issue is resolved in this release.

New service with SIP protocol and flavor does not appear in VoIP report

- Cisco number: CSCsk61917

  When a new service is created with SIP protocol and SIP flavor as service elements and assigned to a dedicated global counter, the new global counter does not appear with the VoIP services list under the VoIP reports.

  This issue is resolved in this release.

Oracle 10 error when running malicious traffic reports

- Cisco number: CSCsj86050

  When using Oracle 10, running one of the following reports produces only a 'Not a GROUP BY expression' error message and no report:

  - Malicious traffic: Infected subscribers
  - Malicious traffic: Dos Attacked subscribers

  This issue is resolved in this release.

Oracle 10 error when running Web and P2P reports

- Cisco number: CSCsj86031

  When using Oracle 10, running one of the following reports produces only an 'Invalid Identifier' error message and no report:

  - Web and streaming: Web host distribution by subscriber package
  - Web and streaming: RTSP host distribution by subscriber package
  - P2P: Top P2P file extension

  This issue is resolved in this release.

Quick forwarding filtering documentation is misleading

- Cisco number: CSCsj07509

  The description of the Filtered-Traffic / Quick-Forwarding functionality in the *Cisco Service Control Application for Broadband (SCA-BB) User Guide* is misleading. The following improvements are suggested:

  – Make the description of the interaction between control action and quick forwarding more accurate and more concise.

  – Enhance the overall description of this functionality; especially the cases in which quick forwarding is useful.

  This issue is resolved in this release.

Malicious Traffic reports showing wrong numbers

- Cisco number: CSCsj77887

  Malicious Traffic reports show wrong numbers when the action is set to 'Block'. The following reports are affected and show extreme numbers:

  – Global Scan / attack rate

  – Global DoS rate

  This issue is resolved in this release.

Virtual links GC configuration pane may be shifted

- Cisco number: CSCsj05767

  On the pane displaying the GC configuration of the virtual links, the upstream and downstream GCs may not be available and may be shifted far to the right and almost not visible.

  This issue is resolved in this release.

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.

  This issue is resolved in this release.

Service configuration is not marked as changed after certain modifications

- Cisco number: CSCsj95319

  When a service configuration is modified in the console, its name is marked with an asterisk (*). For some changes the asterisk is not added.

  This issue is resolved in this release.

DSCP Markers can have empty names

- Cisco number: CSCsj34098

  A DSCP Marker can be assigned an empty name

  This issue is resolved in this release.

DSCP marking in filter rule not reflected in GUI

- Cisco number: CSCsj16417

  If DSCP marking is selected for a filter rule, this is not shown in the summary on the final page of the Add Filter Rule Wizard, nor in the summary of the filter rule list.

  This issue is resolved in this release.

Bypass and Quick Forward should be mutually exclusive in Filter Rule wizard

- Cisco number: CSCsi96301

  Bypass and Quick Forward should be mutually exclusive, but they are both checkboxes and so both can be selected.

  This issue is resolved in this release.

Cannot copy/paste from Problems View

- Cisco number: CSCsh83021

  This issue is resolved in this release.

Compatibility Information

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

Capacity Information

SCA BB 3.1.5 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 1

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]

SCA BB Release 3.1.1

This section describes functional enhancements, resolved issues, capacity, and known caveats of SCA BB release 3.1.1.

Information About Functional Enhancements

The following sections list the functional enhancements in SCA BB 3.1.1. See the *Cisco Service Control Application for Broadband User Guide* for a complete description of these features.

Protocol Support

The following table lists the new protocols that were added in SCA BB 3.1.1. These protocols are also available in Protocol Pack 10. (See the Cisco Service Control Protocol Pack download pagefor links to Protocol Pack 10 files and information.)

Table 2

Protocol List	Protocol ID	Description	Changes to the Default Service Configuration
Live Messenger (MSN) v8.1	883	Instant messaging client	Added as a new protocol and to Instant Messaging Service
Location Free	1045	TV broadcast streaming	Added as a new protocol and to P2P Service
Joost	1046	P2P TV	Added as a new protocol and to P2P Service
Zattoo	1047	P2P TV	Added as a new protocol and to P2P Service
MS Push Mail	1048	E-mail to PDA/Smartphone Windows	Added as a new protocol and to new MS Push Mail Service
Pando	1049	P2P file sharing	Added as a new protocol and to P2P Service
Kugoo	1050	P2P music file sharing	Added as a new protocol and to P2P Service
ICQ Voice	1051	Instant messaging voice	Added as a new protocol and to VoIP Service
Fring	1052	Instant messaging mobile phone client	Added as a new protocol and to Instant Messaging 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 3.1.1. These updated protocols are also available in Protocol Pack 10. (See the Cisco Service Control Protocol Pack download pagefor links to Protocol Pack 10 files and information.)

Table 3

Protocol Name	Description	Cisco Number
Gnutella	Support enhanced	CSCsi52884
ICQ	Voice recognition enhanced	CSCsi96940
PPLive	V1.6.19 classification enhanced	CSCsi25885
PPLive	Support enhanced	CSCsj53023 CSCsj75652
PPStream	Updated to support v2.0	CSCsj76001
Poco	Updated to support 2007 beta version	CSCsi87040
SIP	Added bundling of RTP flow when the connection information of the WAN IP to bundle appears only in the SDP "Ringing" status	CSCsi25885
SMTP	Improved classification of non-standard SMTP sessions	CSCsi87468
Skype	Misclassifications resolved	CSCsj14278 CSCsj43543
Vonage	Support enhanced	CSCsh84903
Yahoo Messenger	Updated to support v8.1.0	CSCsi96962
eMule	Updated to support v0.48	CSCsj48543

Information About Resolved Caveats

This section describes caveats that are resolved in SCA BB release 3.1.1.

Cannot install new OS from the SCA BB console

- Cisco number: CSCsh49525

  This issue is resolved in this release.

Cannot apply service configuration created in SCA BB 3.0.6

- Cisco number: CSCsi40599

  Apply Protocol Pack pp08 in SCA BB 3.0.6, and create and save a service configuration.

  Open the saved service configuration in SCA BB 3.1.0 console, and apply the service configuration. An error is returned.

  This issue is resolved in this release.

Cannot update Global Controller parameters via console after upgrade

- Cisco number: CSCsj68015

  After upgrading from SCA BB 3.0.6 to SCA BB 3.1.0, if any of the Global Controller parameters had nonintegral values, then all Global Controller parameters are not accessible through the SCA BB console. Clicking on the "Global Controller" menu option results in no action.

  This issue is resolved in this release.

In pull mode, the quota for the first flow is not accounted

- Cisco number: CSCsi70169

  When working in pull mode, the first flow of a subscriber is initially classified under the default package. Then, upon login, it is assigned to the proper package. The quota consumed during the time that the subscriber was assigned to the default package is lost.

  This issue is resolved in this release.

RDR RADIUS: no RDRs sent after PQI install or application assignment

- Cisco number: CSCse19753

  IF RADIUS RDRs are being generated, and the RADIUS transaction rate is high, installing and applying a PQI means that no further RADIUS RDRs are generated.

  This issue is resolved in this release.

Compatibility Information

SCA BB 3.1.1 should be used with the following components:

Table 4

HW Platform	SCE-1010-2XGBE 2U SCE-2020-4XGBE SCE-2020-4/8XFE
SCOS	3.1.1, 3.1.0
SCMS-SM	3.1.1, 3.1.0
SCMS-CM	3.1.1, 3.1.0, 3.0.6, 3.0.5, 3.0.3 Virtual Links reporting capabilities are only supported with CM 3.1.0 or later.
SCA Reporter	3.1.1, 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 3.1.1 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 5

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]

SCA BB Release 3.1.0

Information About 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.)

Table 6

Protocol List	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

Table 6 (continued)

Protocol List	Protocol ID	Description	Changes to the Default Service Configuration
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.

Table 7

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

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

Information About Removed Features

This section describes the features removed in SCA BB release 3.1.0.

- Generic Upload/Download Settings, page 17
- Reporting of P2P File Extensions, page 17

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.

Information About Backward Compatibility

This section describes backward compatibility between SCA BB release 3.1.0 and earlier releases of SCA BB.

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.

Information About Resolved Caveats

This section describes caveats that are resolved in SCA BB release 3.1.0.

Traffic Processing

This subsection describes caveats relating to traffic processing that are resolved in SCA BB release 3.1.0.

NTPv2 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

This subsection describes caveats relating to traffic accounting and reporting that are resolved in SCA BB release 3.1.0.

- Counting problem for protocols with different measurement method, page 18
- Malicious Traffic RDR timestamps have mismatch, page 19
- Discrepancy in reported call minutes between Link and Media Reports, page 19

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.

Traffic Control

This subsection describes caveats relating to traffic control that are resolved in SCA BB release 3.1.0.

- QP session limit allows Number of Sessions + 1 before applying breach action, page 19
- QP redirected (due to quote depletion) sessions are counted as used, page 20
- Internal quota with SM pull mode not working properly, page 20
- Quota Replenish Scatter - does not work as expected, page 20
- Concurrent session limitation is not working, page 20

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, that is, subscriber quota is replenished every hour or day, and quota replenish is scattered around the due time, which is either on the hour or at midnight.

  Subscribers whose quota should be replenished before the top of the hour (half of all subscribers) constantly get new quota during the time between their scheduled quota replenish and the top of the hour. For instance, a subscriber that is scheduled for new quota at 11:50 does not receive new quota at 11.50, but at some time 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

This subsection describes miscellaneous caveats that are resolved in SCA BB release 3.1.0.

- Services are sometimes shown by number in reports, page 20
- Subscriber import exception for site with SCE having no service configuration applied, page 21
- Enable/disable of Anomaly Detection does not enable/disable the attack filter, page 21
- PQI install is not saving all the application configuration, page 21

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:

Table 8

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.

Table 9

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]

Open Caveats

Traffic Processing

This section describes open caveats in SCA BB release 3.1.5 that relate to traffic processing.

Traffic Classification

This subsection describes open caveats in SCA BB release 3.1.5 that relate to traffic classification.

Limitations when working with VLANS/VPNs with overlapping IPs

- Cisco number: CSCsi46655

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

  - Classification - no support for zones.
  - Reporting - reports based on IP addresses in Transaction RDRs are not accurate.

  Many reports in the following categories rely on IP uniqueness:

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

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, page 9.

Traffic Accounting and Reporting

This subsection describes open caveats in SCA BB release 3.1.5 that relate to traffic accounting and reporting.

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.

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.

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.

Real-time SUR is always generated if 'monitor' property set to 1

- Cisco number: CSCsj95574

  If the value of the ' *monitor* ' subscriber property is set to '1', the real-time SUR is always generated. It is generated even when the policy is configured not to generate this RDR.

  Workaround:

  Do not set monitor = 1.

Traffic Control

This subsection describes open caveats in SCA BB release 3.1.5 that relate to traffic control.

Virtual links is not supported for the SCE1010 platform

- Cisco number: CSCsi86983

  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.

Release 3.0.3: Invalid injected packet in MPLS Traffic Engineering mode

- Cisco number: CSCsl22211

  When working in 'MPLS Traffic-Engineering skip' mode, a malformed packet is generated by the SCE when MPLS encapsulated flows are redirected or blocked. In the injected packet, the 'next protocol' field of the Ethernet header is 0x8847 (MPLS), but should be 0x0800 (IPv4).

  Workaround :

  Configure the system to ‘MPLS VPN skip’. This has a performance penalty, but in this mode the system injects properly formed packets.

DSCP marking injection into tunneled traffic generates malformed injected packets

- Cisco number: CSCsl41385

  When working in DSCP-marking mode and the application injects over encapsulated traffic (VLAN/MPLS), the injected packets are malformed since the DSCP is updated at the wrong offset in the packet.

  The results of this are:

  - In MPLS and VLAN the labels/vlan-id are wrong.
  - The IP header checksum is incorrect.
  - The packets are marked as mid-fragments in the IP header.

SCA BB Console

This section describes open caveats in SCA BB release 3.1.5 that relate to the SCA BB console.

General

This subsection describes open caveats in SCA BB release 3.1.5 that relate to general issues concerning the SCA BB console.

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.

GUI crashes when creating many service rules

- Cisco number: CSCsj85619

  When a very large number of rules are added under a package, the SCA BB console may crash.

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.

Error message appears when opening the console

- Cisco number: CSCsj27060

  In SCA BB 3.1.5, an error message appears when the SCA BB console is opened.

'Apply policy' operation may lead to packet drop on the line interfaces

- Cisco number: CSCsk08433

  When the 'apply policy' operation is invoked and filter rules are set, SCA BB first resets the filter rules and then reapplies the rules as they appear in the applied policy.

  In the interval between resetting the rules and reapplying them, traffic that was previously set to be filtered is not filtered and flows are opened. In an environment with a large portion of traffic being filtered, this burst of new open flows can overload the CPUs, resulting in back pressure, which can even reach the line interfaces and cause them to discard packets.

Installation

This subsection describes open caveats in SCA BB release 3.1.5 that relate to installation of the SCA BB console.

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

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

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the 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.

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 to which the Network Navigator can connect.

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

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

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

  which usually maps to:

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

Service Configuration Editor

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the 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.

Subscriber Manager GUI

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the Subscriber Manager GUI.

Failure message despite successfully importing subscribers

- Cisco number: CSCsk06486

  Rarely, when successfully importing subscribers in the Subscriber Manager tool, a failure message appears.

Window buttons disappear, cannot work with the Subscriber Manager

- Cisco number: CSCsj45511

  Under certain circumstances, adding a subscriber to the SM (from the Subscriber Manager GUI) fails. If this happens, the window buttons disappear.

Signature Editor

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the Signature Editor.

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:

1. Extract the DSS from the protocol pack, by unzipping the protocolpack's SPQI file.
2. Open your DSS and then import the protocol pack's DSS into the signature editor. Make sure there are no overlapping signatures IDs.
3. Save the merged DSS.

DSS: multiple packet deep inspection condition does not work

- Cisco number: CSCsl45039

  When applying a user-defined signature that includes more than one Deep Inspection Condition, only the first Deep Inspection Condition in each signature is checked, while the other conditions are ignored.

  For example, in a signature that looks for a string match on three packets, the top-level condition matches the first packet and the first "Deep Inspection Condition" matches the second packet. However, the classification process then stops; no more conditions are checked and the other conditions are ignored.

Reporter

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the Reporter.

Exporting a chart sometimes fails

- Cisco number: CSCsk19098

  Rarely, exporting a chart will fail with an error message, and the exported file will not be created.

  Workaround :

  Run the report again and re-export it.

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

This section describes open caveats in SCA BB release 3.1.5 that relate to configuration management.

General

This subsection describes open caveats in SCA BB release 3.1.5 that relate to general issues concerning configuration management.

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, page 9, 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
```

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

This subsection describes open caveats in SCA BB release 3.1.5 that relate to the 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.

Obtaining Technical Assistance

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

- Cisco.com, page 33
- Technical Assistance Center, page 33

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 any time, 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 http://www.cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (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, page 33
- Contacting TAC by Telephone, page 34

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website http://www.cisco.com/tac.

P3 and P4 level problems are defined as follows:

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

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

To register for Cisco.com, go to http://tools.cisco.com/RPF/register/register.do.

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