Release Notes for Cisco Service Control Application Suite for Broadband (SCAS BB) 2.1.8

June 12, 2005

Release Notes for Cisco Service Control Application Suite for Broadband (SCAS BB) 2.1.8

Supports: SCAS BB 2.1.8, SCAS BB 2.1.7, SCAS BB 2.1.6, SCAS BB 2.1.5, SCAS BB 2.1.2, SCAS BB 2.1.1

OL-7020-03

These release notes for the Cisco SCAS BB describe the enhancements provided in Cisco Release 2.1.8. These release notes are updated as needed.

For a list of the caveats that apply to Cisco Release SCAS BB 2.1.8 see "Open Caveats – Cisco Release SCAS BB 2.1.8, page 17.

Corporate Headquarters:

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

Contents

Introduction

Cisco is proud to release version 2.1.8 of its SCAS BB solution. Release 2.1.8 of the SCAS BB solution is a new product version introducing new platforms, features and services for broadband network operators and service providers using Cisco’s Service Control products.

This document outlines the new features and enhancements to the SCAS BB solution, states known problems and last minute notifications. For additional information, please refer to the Cisco SCAS BB documentation.

This document is updated for version 2.1.8.

New and Changed Information

New Functionality in Release 2.1.8

This section provides information on maintenance release 2.1.8, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features and Protocols

2.1.8 resolves a number of protocol classification caveats (see Resolved Caveats below) and an incorrectly set default as described below.

Winny Classification Default Settings

Release 2.1.8 changes the default inspection behavior for the Winny P2P protocol which was incorrectly set to in the previous release.

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

- ***Default***: Suitable for networks that are **not** expected to see significant amounts of Winny traffic. This is the most likely case in all geographies except Japan.
- ***Detailed***: Suitable for networks where Winny traffic is expected to be common. This should be the case in Japanese networks only.

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

Note that in the previous release (2.1.7), the default value was incorrectly set to ***detailed***.

Note: Since the other changes in this release are minimal, customers in Japan may consider remaining on the 2.1.7 release. Japanese customers upgrading to 2.1.8 should enable Winny ***detailed*** mode according to the instructions below. Customers from other regions should upgrade.

ACTIVATING DETAILED WINNY INSPECTION MODE:

Activation of the detailed Winny inspection mode is performed by running a CLI script on the SCE. The script file, *`winny2.cli`*, is included in this release.

To run the *`winny2.cli`* script, follow these steps:

Step 1. Login to the SCE CLI as root (“enable 15”).

Step 2. Upload the file *`winny2.cli`* to the SCE file system

Step 3. In the SCE CLI prompt, type:

```
run script winny2.cli
```

Resolved Caveats

Caveats resolved in this release:

- On rare occasions, HTTP was classified as Gnutella.

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

- SIP classification sometimes failed when the media flows were carried on a port number higher than 32,767.

Compatibility Information

SCAS BB 2.1.8 should be used with the following components:

- SCOS 2.0.8 or 2.0.9 (previously P-Cube SEos)
- SCMS-SM 2.2.1 or 2.03 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.1 or 2.5.1 (previously P-Cube Data Collector). Note that the use of SCMS-CM has several limitations. Consult customer support for further information.
- SCAS Reporter 2.1.1 (previously P-Cube Reporter)

Capacity Information

SCAS BB 2.1.8 supports the following flow and subscriber capacity numbers, for the two main capacity options. (See notes on SCAS BB 2.1.5 for details on how to select a capacity option other than the default.)

Table 1 Flow and Subscriber Capacity in SCAS BB 2.1.8

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2000 (EngageDefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SE2000 (SubscriberLessSE2000)	2,000	2M [1M bi-directional]
SE1000 (EngageDefaultSE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SE1000 (SubscriberLessSE1000)	1,000	1M [500K bi-directional]
SE100 (EngageDefaultSE100) **DEFAULT**	10,000	200K [100K bi-directional]
SE100 (SubscriberLessSE100)	1,000	200K [100K bi-directional]

New Functionality in Release 2.1.7

This section provides information on maintenance release 2.1.7, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features and Protocols

P2P Protocol Support update

P2P support includes the following:

- Update of the Winny protocol signature
- Added support for the following protocols: Waste, Mute, Nodezilla, Napster, iTunes, Filetopia and Soulseek

External Quota Provisioning Enhancements

The following quota provisioning enhancements were added:

- Quota modifications (setQuota, addQuota) can now be queued.
- Quota modifications can take place when the subscriber is not introduced in the SE or is inactive.

Resolved Caveats

Caveats resolved in this release:

- 13405
  Classification of Generic TCP/UDP/IP protocols with an IP lists to a service
- 13232
  Quota threshold was configured to be 16 times larger than what the user defines in the Engage Console

Compatibility Information

SCAS BB 2.1.7 should be used with the following components:

- SCOS 2.0.7 (previously P-Cube SEos)
- SCMS-SM 2.2 or 2.03 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.1 or 2.5.1 (previously P-Cube Data Collector). Note that the use of SCMS-CM has several limitations; Consult customer support for further information.

Capacity Information

SCAS BB 2.1.7 supports the following flow and subscriber capacity numbers, for the two main capacity options. (See notes on SCAS BB 2.1.5 for details on how to select a capacity option other than the default.

Table 2 Flow and Subscriber Capacity in SCAS BB 2.1.7

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2000 (EngageDefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SE2000 (SubscriberLessSE2000)	2,000	2M [1M bi-directional]
SE1000 (EngageDefaultSE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SE1000 (SubscriberLessSE1000)	2,000	1M [500K bi-directional]
SE100 (EngageDefaultSE100) **DEFAULT**	10,000	200K [100K bi-directional]
SE100 (SubscriberLessSE100)	1,000	200K [100K bi-directional]

New Functionality in Release 2.1.6

New Features and Protocols

P2P Support for P2P Applications

This feature includes the following:

- Update of L7-pattern detection for Winny2.724. Please refer to known-bug “Winny Classification” below.
- Added signature for the Support for Share P2P (1.0 build 40) (*PROTOCOL_ID* is 27)

Winny and Share are common protocols in Japan and it is recommended that all SCAS BB customers in this market upgrade to this release.

Support for SM 2.2

SCAS BB 2.1.6 works with SM 2.2 which supports high-availability configurations using a Veritas Cluster.

File Transfer extension reporting

SCAS BB 2.1.6 extracts and reports on file extensions of files transferred in P2P networks. This can be used for statistical purposes and to understand which type of files are being shared by the local community.

Protocols Supported: Supports the FastTrack/KazaA and eDonkey/eMule/Overnet protocols only.

Activating Capability: This capability is disabled by default and can only be activated through a certified technician. Please contact Cisco support for additional details.

New Reports: The “Top P2P File Extension” has been added to generate a report of this information. The report provides a graph of the most popular file extensions.

Note

The New Reports capability has to be activated. If it has not been activated, empty results will be returned.

RDR Changes: Once enabled, the **Info-String** field in the TRANSACTION RDR reports on the file extension.

Service Configuration Apply Logging & Traps

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

```
#logger get user-log file-name log.txt
#more log.txt
...
2004-07-15 15:33:44 | INFO | CPU #000  Engage policy applied:
omert@10.1.12.224, Box17.pqb
```

Apply operations also generate an SNMP trap with a similar message.

Terminology Changes in Filtered Traffic window in Engage Console

Confusing use of terms in the Filtered Traffic window was changed as follows:

- **Source** was changed to **Subscriber Side.**
- **Destination** was changed to **Network Side.**
- **Flows** was changed to **Packets.**

These terms are more consistent with the actual semantics of the filter.

Resolved Caveats

All the caveats in this section are resolved in SCAS BB Release 2.1.2

- 12868, 12899

  In rare occasions SMTP and RTSP traffic was mistakenly blocked by the solution.
- 12708

  Service Specific Post Breach was not activated when the total traffic rule was breached.

Compatibility Information

SCAS BB 2.1.6 should be used with the following components:

• SCOS	2.0.6 (P-Cube SEos)
• SCMS-SM	2.2 or 2.03 (P-Cube smartSUB Manager)
• SCMS-CM	2.1.0 or 2.0.1 (P-Cube Data Collector)

Note

The use of SCMS-SM 2.0.3 requires manual installation of SCOS 2.0.6. Consult Cisco support for further information.

Capacity Information

Capacity Numbers: The following table displays flow and subscriber capacity numbers for the two main capacity options (See notes on SCAS BB 2.1.5 for details on how to select a capacity option other than the default.).

Table 3 Flow and Subscriber Capacity in SCAS BB 2.1.6

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2020 (EngageDefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SE2000 SubscriberLesssSE2000	2,000	2M [1M bi-directional]
SCE 1010 (EngageDefaultSE1000) **DEFAULT**	40,000	700K [350K bi-directional]

New Functionality in Release 2.1.5

New Features and Protocols

Vonage Support

SCAS BB 2.1.5 adds a new classification code to specifically identify Vonage voice sessions.

Functionally this means:

- While Vonage makes use of the SIP protocol, a specific L7 inspection has been added (by looking at specific fields in the SIP messages indicating this is a Vonage service).
- Report of the Vonage user-name (mapped to the phone number) is performed as part of the Transaction Usage RDR. The user-name is sent by default to CSV text files in the Cisco DC and can be used by external systems as well.

Quota Functionality Enhancements

Changes in the Quota API were introduced to facilitate and simplify quota integration. The SE device can now generate a new threshold RDR when a subscriber’s quota reaches less than a certain threshold. This makes it simple for an external system to work in a “quota-chunk” model, by breaking a subscriber’s quota into chunks, and provisioning these chunks incrementally on the device. (Adding more each time the remaining quota reaches below the specified threshold.)

Default Traffic Filters

Traffic filters were added to the system to boost performance in default use-cases. This can be disabled or enabled by the user at any time. Performance improves when appropriate filters are applied.

When creating a new PQB file with SCAS BB 2.1.5, the following traffic filters will be enabled by default: ICMP, DNS & NET-BIOS. This can be changed using the “Filtered Traffic” configuration screen in the SCAS BB Console.

Compatibility Information

SCAS BB 2.1.5 should be used with the following components:

• SCOS	2.0.5 (SEos)
• SCMS-SM	2.03 (smartSUB Manager)
• SCMS-CM	2.1.0 (2.0.1 is also supported) (Data Collector)

Capacity Information

Capacity Numbers: The following table displays flow and subscriber capacity numbers for the two main capacity options (see notes on SCAS BB 2.1.5 for details on how to select a capacity option other than the default).

Table 4 Flow and Subscriber Capacity in SCAS BB 2.1.5

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2000 (Engage DefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SE2000 SubscriberLesssSE2000	2,000	2M [1M bi-directional]
SCE 1010 (Engage DefaultSCE 1010)	40,000	700K [350K bi-directional]

Device (Capacity Option)	Number of Subscribers	Number of Flows
DEFAULT		
SCE 1010 (SubscriberLessSCE 1010)	2,000	1M [500K bi-directional]

Capacity options are an advanced feature that allows the operator to tune the system’s use of internal resources according to its needs. It is especially useful when using SCAS BB in a subscriber-less mode, in a network with a particularly large number of flows (such as a main peering connection). Following is an explanation on how to select the capacity mode during system installation.

Installing the PQI on the SE with non-default capacity:

```
option:SE#configure
SE(config)#interface LineCard 0
SE(config if)#pqi install file eng21207.pqi options
capacityOption=<option-name>
```

New Functionality in Release 2.1.2

New Features and Protocols

Release 2.1.2 contains no software or hardware updates except for resolving caveats.

Resolved Caveats

All the caveats in this section are resolved in SCAS BB Release 2.1.2

- 11064

  Asymmetric global bandwidth configuration on dual link systems (SE2000) is not preserved during fail-over transitions

- 11791

  Subscriber Notification on Denial of Service Attacks cannot be saved.

Compatibility Information

SCAS BB 2.1.2 should be used with the following components:

- SEos 2.0.3
- smartSUB Manager 2.03
- Data Collector 2.1.0 (2.0.1 is also supported)

Capacity Information

Capacity Numbers: The following table displays flow and subscriber capacity numbers for SCAS BB 2.1.2.

Table 5 Flow and Subscriber Capacity in SCAS BB 2.1.2

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2000	80,000	1.4M [700K bi-directional]
SCE 1010	40,000	700K [350K bi-directional]

New Functionality in Release 2.1.1

SCAS BB 2.1.1 is released under beta status. The new features and capabilities of the SCAS BB 2.1 version are described in detail in the document titled: “SCAS BB 2.1 New Features & Capabilities”. The content of that document is not reiterated here and can be obtained by contacting Cisco support.

Capacity Numbers: The following table displays flow and subscriber capacity numbers for SCAS BB 2.1.1.

Table 6 Flow and Subscriber Capacity in SCAS BB 2.1.1

Device (Capacity Option)	Number of Subscribers	Number of Flows
SE2000	80,000	1.4M [700K bi-directional]
SCE 1010	40,000	700K [350K bi-directional]

Dynamic Signatures

At the time of the release, dynamic signatures are supported for the following protocols. Please contact Cisco support for obtaining the signature-file and for latest updates on available signatures.

- Kuro (Taiwanese P2P protocol)

Important Changes from Previous Release

Note the following important change from the 2.0 version:

- In order to connect to the SE, the SCAS BB Console requires that the Telnet daemon on the SE be enabled on port 23 (this is the case by default). The connection password is that of the admin user (*`enable 10`*).
- In order to connect to the SM, the SM GUI requires that the FTP server on the SM machine be enabled on port 21. The connection password is that of the Cisco account.

Caveats

Open Caveats – Cisco Release SCAS BB 2.1.8

Traffic Analysis & Control Issues

Resolution Limitation on Quota Breach Detection

- Cisco number: 10470

  The SCAS BB application enforces policies at fixed time intervals during each session. This means that quota breach detection and the corresponding policy enforcement take place with this predefined accuracy (default is 30 seconds).

  Workaround: This is the normal system behavior and provided here for clarification. When defining quota breach rules, expect up to 30 seconds (or the configured duration set in the ongoing-policy-check option) where a subscriber may have exceeded his quota but the new enforcement did not take place.

BW Reports May Contain Spikes after DoS Attacks

- Cisco number: 10822

  At times when a Denial-of-Service attack has been detected by the SCE device, the bandwidth reports may show a “spike” in the Generic TCP traffic (that is, a significant increase in traffic) at the time when the attack subsided.

  Workaround: While viewing bandwidth reports bear in mind that spikes in TCP traffic could be as a result of a denial-of-service attack.

Application Management, Configuration and User Interface

Removal of Subscriber Notifications

- Cisco number: 8391

  PQI installation (for example, of a new SCAS BB revision) automatically removes the settings of Subscriber Notifications on Network (or denial of service) Attack.

  Workaround: When possible, perform the following:

Step1. A PQI upgrade instead of a PQI installation

Step2. Verification of Subscriber Notification settings after performing a PQI upgrade or an install

Incorrect Mapping of Transactions

- Cisco number: 11773

  Transactions may not be properly mapped to a service defined by the Generic TCP/UDP Protocol + IP address List, if a more specific service, defined by a Port-based Protocol + Initiating-side + the same IP address list, exists.

  The following scenario is an example:

  A Service Configuration contains these three services:

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

  The mapping result is the following:

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

  There are no known workarounds.

List Selection Clears during Editing of Service Transaction Mapping

- Cisco number: 10609

  The definitions of a Service’s transaction-mapping in the SCAS BB Console include the following configuration order:

Step 1. Select a protocol

Step 2. Select an initiating side (optional)

Step 3. Select lists (optional)

Changing the protocol selection after the lists are selected clears the lists selection.

Workaround: Re-configure the lists of the transaction-mappings when changing the protocol.

Persistent Storage of Service Configuration May Fail

- Cisco number: 10609

  On rare occasions, the persistent storage of Service Configuration on the SCE Platform may fail, even though the new configuration is applied. This means that after SCE reboot, the configuration will reset to its previous state. When this occurs, the SCAS BB Console displays an error message in its message pane, prompting the user to apply the configuration again.

  Workaround: If the SCAS BB Console displays the following error message, reapply the service configuration.

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

Invalidating SCAS BB CSV Files

- Cisco number: 10658

  SCAS BB CSV files consist of rows of comma-separated values. When the values in the end of a row are empty, they are denoted with consecutive commas. Microsoft 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 SCAS BB.

  Workaround: Add the missing commas using a text editor, ensuring that each row contains the same number of commas.

Closing and Opening SCE Connections Properly

- Cisco number: 10580

  SCAS BB API can be used to program automated Service Configuration tasks, such as opening a connection to an SCE platform and applying a Service Configuration file. During the process, since each connection consumes resources on the SCE device, it is necessary to close SCE connections that are no longer needed and minimize the number of concurrently open ones.

  Workaround: When programming with SCAS BB API it is recommended to do the following:

  - Refrain from creating multiple simultaneous connections to the same SCE.
  - Reuse an existing single connection that you already created instead of opening multiple ones.
  - Make sure to properly close the connection by calling the logout method.

Quota Provisioning API

- Cisco number: 11821

  Quota modification of a subscriber whose quota is not externally managed does not cause an exception. Subscriber’s quota is externally managed when the subscriber belongs to a package that is working in “external” quota management mode.

  There are no known workarounds.

Installation Error

- Cisco number: 10637

  While installing the SCAS BB clients' setup on a Windows PC, the following error message may appear: "`The InstallShield Engine (iKernel.exe) could not be launched - The RPC server is unavailable`".

  Workaround: To resolve this issue perform the following in your Windows application:

Step 1. Click Start.

Step 2. Click Run.

Step 3. In the Open box, type **`net start rpcss`**.

Step 4. Click OK.

Step 5. Test to see if this resolves the issue.

If the issue still occurs, restart your PC and launch the setup again.

Data-Collection and Reporting

Data-Collection (Service Control Management Suite - Collection Manager

Under Cisco, P-Cube's Data-Collection software has been renamed to Service Control Management Suite - Collection Manager (SCMS-CM). The text below uses the original name.

Sybase Installation Always Places Data on the 2nd Disk

- Cisco number: 9118

  The Sybase installation script, *`installsyb.sh`* will always use the 2nd disk as a data repository, regardless of how many disks are available or where the system root is mounted.

  Workaround: Before using this script to install Sybase, ensure that the second disk (usually c0t1) is currently not used for any other purpose.

sybback.sh Script Requires a Full Path as the Argument

- Cisco number: 8810

  When using the -f option of `sybback.sh` to specify a path where the backup is to be created, and the path is relative, the script may fail.

  Workaround: Specify the path in absolute form, when using this flag, for example use -f `/tmp/somedir` and not `somedir`.

Warning Message in the./dbperiodic.py –load Output

- Cisco number: 9959

  The following warning message may appear when running the script `./dbperiodic.py --load`:

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

  Workaround: Ignore this message.

dc-install.sh Does Not Check if SCMS CM is Running

- Cisco number: 9978

  When upgrading the Service Control Management Suite - Collection Manager (installing over an existing one), if there is already a running SCMS CM, the script does not detect it and fails to complete the installation.

  Workaround: Before upgrading the SCMS CM, stop it using **`~/pump/bin/pump stop`**.

SCMS CM/Sybase - When 2 NIC's are Present, Sybase Always Listens on the Primary One

- Cisco number: 10789

  When Sybase comes up it starts listening on one network interface (in addition to localhost). The interface selected is the one associated with the current host name (as returned by the "hostname" command).

  This means that the default behavior is for Sybase to listen on the primary interface (called eri0 on a Netra, and physically labeled as "Net 0" on the back of the machine). Therefore, connections from the Reporter must come via this interface.

Workaround: If you wish to change this (although it is not recommended), and have Sybase listen on the other interface, perform the following:

Step 1. Change the local hostname to the name associated with the other interface.

This name is usually found in the file */etc/hostname.eri*.

Place this name in the */etc/nodename* file to make it the host name.

Step 2. Reboot.

To locate the interface Sybase is currently listening on, run the command:

```
netstat -a | grep 4100.*LISTEN
```

The output will consist of two lines, one for localhost and one for the host associated with the sought interface.

SCMS CM Reporter Does Not Enforce Maximum Number of Open Connections

- Cisco number: 10791

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

  Workaround: If there is an indication in the SCMS CM log of failures to connect to the database, and you have a Reporter open with many active windows, close the reporter and restart the SCMS CM.

✎		
Note		If the sudo package is installed on the SCMS CM, the DB Adapter will automatically do this by restarting the database.

US English Locale Must Be Used

For correct SCMS CM and Sybase operation, English locale must be used.

Workaround: Set the locale.

The easiest way to set the locale is by performing the following steps:

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

Step 2. Reboot in order for the changes in the file to take effect.

Step 3. Install this locale in Solaris.

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

Posix Format for Time Zone is Not Recommended

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

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

`TZ=Japan`

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

If GMT offset must be used, use the "zoneinfo" format by prepending an '*`:Etc/' prefix`*, for example:

`TZ=:Etc/GMT+5`

Saved Report Templates May Be Unusable After Policy Change

- Cisco number: 10735

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

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

Duplicate Names in Top Service Ports Report

- Cisco Number: n/a

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

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

Tables Always Print on the Default Printer

- Cisco number: 5049

  Tables always print on the default printer.

  Workaround: Change the printer settings.

  To change the settings:

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

The list of printer icons is displayed.

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

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

Help Button in the "Reports Wizard" not Functional

- Cisco number: 5282

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

  There are no known workarounds.

Find Function in Reporter Table View not Functional

- Cisco number: 8111

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

  There are no known workarounds.

Opening the Reporter without Templates Provides no Indication

- Cisco number: 9092

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

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

  To verify that the templates are installed:

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

Step 2. Search for **P-Cube Engage templates**

Reporter DB Error when Refreshing a Report Window

- Cisco number: 8015

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

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

Print Preview of Table (not Chart) Causes Table to Disappear

- Cisco number: 8106

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

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

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

The preview window closes and the table reappears.

Report Cannot Close While it is Produced

- Cisco number: 8128

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

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

Clicking the Report Button while a Query is Running, May Abort the Query

- Cisco number: 8131

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

  There are no known workarounds.

Table Values in the Reporter Cannot be Copied to the Clipboard

- Cisco number: 3116

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

  Workaround: Perform the following steps:

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

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

Step 3. Copy the content to the clipboard.

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

Reporter Displays the Word "Engage" Occasionally in the SE IP Line

- Cisco number: 10137

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

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

Single Quotes Cannot be Used in Arbitrary Strings in the Reporter

- Cisco number: 10287

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

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

Documentation Errors

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

- Cisco number: 10515, 10516, 10517

  The info string for SMTP, NNTP and POP3 incorrectly documents that it contains values in the layer-7 fields for the BLOCKING_RDR. This is not the case; the fields are reported empty (since blocking occurs prior to the information being sent).

Note Transaction RDRs, which many reports are based on, convey the corresponding info strings correctly.

There are no known workarounds.

Limits Exist on the Number of List Items and Protocol Ports in a Service Configuration

- Cisco number: 8358

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

  - Max number of SCE 1010 list items: 10,000 items.
  - Max number of protocol ports: 5000 ports.

  Applying a service configuration that exceeds these limits, causes an error message to display.

  There are no known workarounds.

Incorrect Licensing Documentation

The SCAS BB (Service Control Application Suite for Broadband) User Manual incorrectly documents a license for “capacity-control” and for “tiered-control”. This is incorrect; only the “tiered-control” license exists.

There are no known workarounds.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html