Release Notes for Cisco Service Control Operating System, Release 5.2.0

First Published: September 23, 2015

Note This document supports the 5.2.0 release of the Cisco Service Control Operation System (Cisco SCOS).

The release notes for the Cisco SCOS describe the functional enhancements and fixes provided in the Cisco SCOS Release 5.2.x. These release notes are updated as needed.

For a list of the open caveats that are applicable to Cisco SCOS Release 5.2.0, see the "Open Caveats in Cisco SCOS Release 5.2.0" section on page 4. The caveats are applicable only to the Cisco SCE 8000 platform.

Contents

- Introduction, page 2
- Limitations and Restrictions, page 2
- Cisco Service Control Operating System Release 5.2.0, page 3

Cisco Systems, Inc.
www.cisco.com

Introduction

Cisco SCOS Release 5.2.0 for Cisco SCE platforms contains new features, as well as fixes for issues that were identified during internal testing and customer interaction.

This document outlines the functional enhancements and resolved issues delivered in Cisco SCOS Release 5.2.0. It assumes that the reader has substantial knowledge of the Cisco Service Control solution. For more information Cisco SCE products and features, see the Cisco SCE documentation.

To access the new Cisco Service Control online documentation site, do the following:

1. On Cisco.com, go to http://www.cisco.com/cisco/psn/web/psa/default.html?mode=prod.
2. From the Products list, select **Service Exchange > Cisco Service Control > Cisco Service Control Product**.

Limitations and Restrictions

Port Scan on Cisco SCE

When you perform a port scan operation on the Cisco SCE platform management port, the platform may experience a reboot. This reboot occurs because of scheduling optimization for detecting failover conditions during periods of less than one second in a configuration involving two cascaded Cisco SCE platforms. We recommend the following:

- Use IP access lists to eliminate port scans that take place because of actual attacks.
- If the system administrator must perform a port scan operation as part of the security check, we recommend that you disable the Cisco SCE watchdog only for the period during which the port scan is performed.

  To disable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset disabled
SCE(config)#> interface linecard 0
SCE(config if)#> no watchdog
```

- To re-enable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset enabled
SCE(config)#> interface linecard 0
SCE(config if)#> watchdog
```

Cisco Service Control Operating System Release 5.2.0

This section describes the compatibility information, new features, resolved issues, and open issues pertaining to Cisco SCOS Release 5.2.0:

- Compatibility Information, page 3
- New and Enhanced Features, page 3
- Resolved Caveats in Cisco SCOS Release 5.2.0, page 4
- Open Caveats in Cisco SCOS Release 5.2.0, page 4

Compatibility Information

For information about the Cisco SCE platforms that are compatible with Cisco SCOS Release 5.2.0, see the *Cisco Service Control Application for Broadband Download Guide*.

For SCOS 8000 Platform:

- Cisco SCOS Release 5.2.0 is compatible only with Cisco Service Control Collection Manager Release 4.2.0,5.1.0,5.2.0.
- Cisco SCOS Release 5.2.0 is compatible only with Cisco Service Control Subscriber Manager Release 4.2.0,5.1.0,5.2.0.

New and Enhanced Features

This section describes the major Cisco SCE 8000 platform-related new features and enhancements in Cisco SCOS Release 5.2.0:

- Empty string support for hashed subscriber info in Anonymized RDRs.

Resolved Caveats in Cisco SCOS Release 5.2.0

This section describes the resolved caveats pertaining to the Cisco SCE 8000 platform for Cisco SCOS Release 5.2.0:

CSCut44367
Aging is enabled twice for Static Subscriber when running configuration command.

CSCuu19206
SCE 8000 with DUAL SIMBA crashes without PQI installation.

CSCuu32698
SCE 8000 sends the TACACS+ authorization request with empty user name, during software upgrade.

CSCuu34728
RDR goes Out of Sequence when login-logout happens at same second.

CSCuv13025
Subscription-ID-Type is wrongly updated as E164 during SM resynchronization.

CSCus95925
SCE 8000 high CPU usage during no traffic.

CSCus42922
Open SSL Vulnerabilities released in January 2015.

CSCus55908
SCE unable to terminate user's session, when Credit-Control-Answer message indicating permanent failure 5002, is received.

CSCus82265
CLI support for killing the traffic flow corresponding to each link.

CSCus82176
MIB counts up the traffic volume on a link where there is no traffic.

CSCut46564
Open SSL Vulnerabilities released in March 2015.

CSCuq56128
SCMP gets appended to CLI, when anonymous group is configured via SCABB

Open Caveats in Cisco SCOS Release 5.2.0

This section describes the open caveats pertaining to the Cisco SCE 8000 platform for Cisco SCOS Release 5.2.0:

CSCus27279
December 2014 - NTPd.org Vulnerabilities.

CSCtj50046

"on failure cutoff" command does not work.

CSCtk67558

Delayed notification of first QuotaStatus RDR.

CSCtu12409

IPv6 byte count is displayed in DP L2TP control packets.

CSCty13726

Problem in handling non-first fragments in l2tp skip mode in cascade set.

CSCub93514

3.7.5-p1: diameter Gy interface enabled upon reload.

CSCuh57649

PUR IP_Type_TAS count is incorrect when Subscriber has IPv6 & DSLiteflow.

CSCur56349

SCE/CM: Incorrect value reported for the field TOTAL_ACTIVE_SUBSCRIBERS.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.