Release Notes for Cisco Service Control Operating System, Release 3.5.0

Revised: September 15, 2009, OL-19144-01

These release notes for the Cisco Service Control Operating System describe the functional enhancements and fixes provided in Cisco Service Control Operation System (SCOS) Release 3.5.0. These release notes are updated as needed.

For a list of the caveats that apply to Cisco Service Control Operation System (SCOS) Release 3.5.0, see the "Open Caveats" section on page 5. Some caveats apply only to the Cisco SCE8000, some apply to the SCE 2000 and SCE 1000, and others apply to all SCE platforms.

For related information regarding SCOS Release 3.1.7, see the *Release Notes for Cisco Service Control Operating System (SCOS), Release 3.1.7*.

Supports: SCOS Release 3.5.0

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

Introduction

Cisco Service Control Operating System (SCOS) Release 3.5.0 for the SCE platforms includes new features, as well as fixes of issues that were identified during internal testing and customer interaction.

This document outlines the functional enhancements and resolved issues delivered in SCOS Release 3.5.0. It assumes the reader has substantial knowledge of the Cisco Service Control solution. For additional information, refer to the Cisco Service Control Engine documentation.

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

1. At Cisco.com, go to:http://www.cisco.com/cisco/web/psa/default.html?mode=prod
2. From the Products list, select **Service Exchange**.
3. From the list that appears, select **Cisco Service Control**.
4. From the list that appears, select a Cisco Service Control product.

SCOS Release 3.5.0

-
-
-

Compatibility Information

You may install SCOS Release 3.5.0 on the following service control engine platforms:

- Cisco SCE8000 2 x10 GBE
- Cisco SCE8000 4 x10 GBE
- Cisco SCE 2000 4 x GBE
- Cisco SCE 1000 2 x GBE (2-U only)

SCOS Release 3.5.0 is not compatible with the following service control engine platforms:

- Cisco SCE 1000 2 x GBE (1.5 U)
- Cisco SCE 2000 4/8 x FE

Functional Enhancements

For information regarding the functional enhancements in Release 3.5.0, see the *Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.5.0*.

Resolved Issues

Resolved Issues—All Platforms

CSCso19855

When the SNMP agent was restarted on the SCE platform, the coldStart trap was not sent.

This issue is fixed in SCOS Release 3.5.0.

CSCsr30215

tpServiceLoss indicated an incorrect value for service loss. The service loss calculation did not take into consideration the accurate amount of packets bypassed from side-to-side during congestion.

Additionally, the calculation returned the average of aggregative counters, so that all past events of service loss were accounted (even long after they ended).

These issues are fixed in SCOS Release 3.5.0. The service loss calculation was changed to be the average service loss per second measured in the last minute. In SCE8000 (only), the system accurately counts and considers the packets that are bypassed during congestion

CSCsu63708

Upgrading or downgrading SCOS from admin level resulted in a failure message, even though the operation was successful.

This issue is fixed in SCOS Release 3.5.0.

Resolved Issues—SCE8000 Only

CSCsv88499

When MIB requests were received using a string index (as in RDR MIB), the SNMP agentx task stopped responding, where the string was lengthier than 13 characters.

This problem occurred when the RDR destination was configured on the device and authentication was required.

This issue is fixed in SCOS Release 3.5.0.

Limitations and Restrictions

The upgrade to SCOS Release 3.5.0 may result in re-initialization of the SCE 1000 or SCE 2000 hardware bypass module. This re-initialization process may cause a failure of the GBE link where the system stalls for a period of less than 1 second.

Table 1 lists cases in which re-initialization may occur (marked Yes).

Table 1 Cases in Which Upgrading May Cause System Re-initialization

To / **From**		2.5.9	3.0.0	3.0.1	3.0.3	3.0.4	3.0.5	3.0.6	3.1.0	3.1.1	3.1.5	3.1.6	3.1.7
2.5.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.8	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.9	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.0.0	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.0.1	—	—	—	—	—	—	—	—	—	—	—	—	—
3.0.3	—	—	—	—	—	—	—	—	—	—	—	—	—
3.0.4	—	—	—	—	—	—	—	—	—	—	—	—	—
3.0.5	—	—	—	—	—	—	—	—	—	—	—	—	—
3.0.6	—	—	—	—	—	—	—	—	—	—	—	—	—
3.1.0	—	—	—	—	—	—	—	—	—	—	—	—	—
3.1.1	—	—	—	—	—	—	—	—	—	—	—	—	—
3.1.5	—	—	—	—	—	—	—	—	—	—	—	—	—
3.1.6	—	—	—	—	—	—	—	—	—	—	—	—	—

When you perform a port scan operation on the SCE platform management port, the SCE platform may experience a reboot. The reboot is initiated by the SCE platform due to scheduling optimization for detecting failover conditions in periods of less than 1 second in a configuration of two cascaded SCE platforms. The following is recommended:

- Use IP access lists to eliminate port scans that take place due to actual attacks.
- If the system administrator must perform a port scan operation as part of a security check, it is advisable to disable the SCE watchdog only for the period of time in which the port scan is performed.

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

```
configure
watchdog software-reset disabled
interface linecard 0
no watchdog
```

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

```
configure
watchdog software-reset enabled
interface linecard 0
watchdog
```

Open Caveats

Open Caveats—All Platforms

CSCsd48922

The configured attack threshold is set for each PPC separately. For certain types of attacks, an attack is detected by the SCOS attack-filter module only if it is three times stronger (as measured by flow rate per second) than the configured value.

This occurs when the IP address common to all the flows of the attack is on the network side of the SCE platform, so all attacks of the single-side-network type have this issue.

CSCsg46885

When link reflection on all ports with line- card aware is configured, a link failure may be reflected to all ports (rather than only to the relevant link) if one of the ports that is connected to the failed line card is flickering due to a hardware problem.

CSCsi80337

If stalled by flow control, the SCE may reload.

By design, the SCE platform reacts to Ethernet flow control and does not activate it. Therefore, a situation could arise in which flow control stalls the SCE platform by overflowing the SCE platform queues and thereby causing traffic to be dropped on the RX interfaces. If this situation persists for more than 5 seconds. It may trigger the SCE platform internal sanity checks mechanism, which may in turn trigger a reload of the SCE platform in an attempt to recover.

CSCsm01291

Issues may occur when an SCE that is configured to create anonymous subscribers is connected to a subscriber manager that is working in push mode. Subscriber login may fail, or the subscriber may log in successfully, but not receive any traffic.

This occurs because, by design, the combination of anonymous subscribers and introduced subscribers is not supported.

Workaround: None

CSCsm19587

Quota events are not received by the SCE subscriber API client or QM because the internal RDR connection to destination 127.0.0.1 port 33001 is not configured.

Workaround: Configure the internal RDR connection as follows:

Step 1 Configure the internal connection on category 4 to destination 127.0.0.1. port 33001.

Step 2 Name category 4 with a special, fixed name. Do not configure any additional destinations on category 4.

CSCsm52337

When the system is in L2TP skip mode, non-first fragments of pure IP traffic (not tunneled) are not managed correctly. Incorrect UDP/TCP ports are assumed, and the fragment is mapped to the incorrect flow, causing flow mismatch.

Workaround: Configure traffic rules that correctly define the ports. Refer to the CLI sample for specific command formats.

Step 1 Configure a traffic rule to set all traffic for quick-forwarding.

Step 2 Configure one traffic rule for UDP with Subscriber side Port=0 and Network side Port=0 with bypass action.

Step 3 Configure one traffic rule for TCP with Subscriber side Port=0 and Network side Port=0 with bypass action.

Step 4 Save the configuration.

Step 5 Reload the SCE platform.

```
configure
interface LineCard 0
traffic-counter name tcp_frag count-packets
traffic-counter name udp_frag count-packets
traffic-rule name quick-forward-all IP-addresses all protocol all direction both
traffic-counter none action quick-forwarding
traffic-rule name tcp_frag IP-addresses all protocol TCP ports subscriber-side 0
network-side 0 flags all direction both traffic-counter name  tcp_frag action ignore
traffic-rule name udp_frag IP-addresses all protocol  UDP ports subscriber-side 0
network-side 0  direction both traffic-counter name  udp_frag action ignore
exit
exit
copy running-config-all startup-config-all
reload
```

CSCsu88206

When a pull response includes an IP range (as opposed to one IP address), the QM might mistakenly allocate two times the configured dosage.

This occurs because when a pull response includes an IP range, the subscriber is first overwritten with the new name and tunables, then removed, and then a new subscriber is recreated with the specified IP range and tunables. This results in the QM quota being allocated two times.

Workaround: If applicable (in single IP environments), make sure the SM holds single IP addresses rather than IP ranges.

There is currently no workaround for IP ranges.

CSCsw37717

Configuring two anonymous groups with overlapping IP ranges based on IP address 0.0.0.0 causes continuous reboot of the SCE platform, either immediately during reboot or later during PQI installation.

Workaround: Any anonymous groups with an IP range based on IP address 0 (with the exception of 0.0.0.0:0x00000000) must be deleted from the SCE configuration file. Do this by manually editing the file */system/config.txt*.

CSCsw49078

TCP RST packets that are injected during the blocking of TCP flows are padded in the L7 layer instead of Layer 2, with the result that they are padded to 80 bytes in total length rather than 60 bytes.

Workaround: None

CSCsw79718

If failover occurs in a pair of cascaded SCE platforms, mirrored packets enter an infinite loop under the following conditions:

- Failover occurs and one of the SCE platforms becomes the stand-alone
- Mirrored traffic exists
- The configured VAS traffic link is link-1 (the default)

In normal operation, the packets that are passed on the cascade ports are forwarded by the cascade bypass mechanism to the other link. If either SCE platform enters a stand-alone state, the cascade ports no longer perform a cascade bypass and instead they move the packets from one port to the other (0<->1, 2<->3). In such a case, if the mirroring is performed to the cascade ports link (usually link-1), the SCE duplicates packets from the other link into link-1, which is now functioning as a loop. The loop stops after the boxes are out of the stand-alone state.

The following error message is written in the log file:

```
Detected packets loop between a VAS server designated for mirroring and the SCE. This
indicates an installation problem
```

Workaround: Configure the VAS traffic link on both SCE platforms to be link-0, so that packets are not mirrored over the cascade ports:

```
>configure
>interface LineCard 0
>VAS-traffic-forwarding traffic-link link-0
>exit
>exit
>copy running-config startup-config
```

CSCsw80782

After a number of imports of URLs from an encrypted CSV file to the URL blacklist, the system may perform a preventive reload due to a lack of heap space, as a part of memory leakage and fragmentation detection mechanism. Up to the stage of the reload, the system functions properly.

The number of file imports that trigger the reload by the mechanism depends on the number of URLs imported. For example:

- Importing 100,000 URLs each time causes the system to stop responding after about 8 to 10 imports.
- Importing 10,000 URLs each time causes the system to stop responding after about 50 imports.

The reboot is caused by a preventive mechanism that detects a memory leakage or fragmentation.

Workaround: Perform an initiated reload before the triggering of the detection mechanism.

Calculate the expected reboot time based on the import frequency and the number of URLs imported, and then plan an initiated reboot (use the **reload** command) at a convenient time before it is expected to happen spontaneously.

For example, based on the figures above:

- Assuming that importing 100,000 URLs causes the system to stop responding after about 8 to 10 imports, performing a weekly import would cause a crash after about two months.
- Assuming that importing 10,000 URLs causes the system to stop responding after about 50 imports, performing a weekly import would cause a crash after nearly a year.

You can monitor the memory status using the following ROOT CLI command:

```
SCE#> debug slot 0 ppc 0 func memShow



   free  44845608     1862      24084  42556192
  alloc  424822576    27725      15322        -
cumulative
  alloc  284816368  2565976        110        -
Return value is: 0 = 0x0.
```

Monitor the value in the 'free' (row) 'max block' (column) size in the output. The value may decrease after each successive URL file import. When the value approaches 500,000, the system should be reloaded. (If it falls under 500,000, the system reloads automatically.)

Open Caveats—Cisco SCE8000

CSCsm12163

SNMP protocol version v1 does not present 64-bit fields properly.

Workaround: Use SNMP v2.

CSCsq33416

FRU modules that are added after startup, such as an additional pluggable SPA optic, may not appear correctly in the entity MIB.

Workaround: After you install any new FRU units, execute a system reload.

CSCsq94141

In rare cases, a condition in which the SNMP agent does not respond to new SNMP requests exists.

Workaround: If the SNMP does not respond, use the following CLI commands to disable and enable it again:

```
SCE> enable 10
SCE# configure
SCE(config)# no snmp-server
SCE(config)#snmp-server enable
```

CSCsq95048

The IP table contains entries for internal IP addresses and interfaces. This results in an inconsistency in the If index representation of the following components of the IP table:

- ipAddrTable
- ipRouteTable
- ipNetToMediaTable

Workaround: Ignore all entries in the IP tables, with the exception of the management interface. Refer to the following example:

The If MIB represents five interfaces as follows:

1. if index 1—mng port
2. if index 2—Traffic port 0
3. If index 3—Traffic port 1
4. If index 4—Traffic port 2
5. If index 5—Traffic port 3

The Ip tables and the at tables represent six interfaces as follows:

1. if index 1—eth0 - currently simba to simba
2: if index 2—eth1 - mng port
3. if index 3—eth2 - cofico 1 that is not connected
4. if index 4—lo
5. ifDescr.5—dummy0 - configure to skynet
6. ifDescr.6—skynet0

The only relevant ifIndex in these tables is the management interface, with IfIndex 1 in the IF table being equal to IfIndex 2 in the IP tables.

CSCsq96310

The default gateway cannot be configured before there is an IP address already configured. Trying to set the default gateway when IP address is set results in an error.

Workaround: Before adding the default gateway, configure the IP address.

CSCsr83407

The input and output interface byte counters are not consistent with each other. The input counters include the 4 bytes of the CRC, while the output counters do not include those 4 bytes.

Workaround: None

CSCsw34368

Attempting to modify only the subnet mask of the management IP using the **ip address** command results in the following error:

```
Error - Cannot replace management IP. Invalid state or parameters.
```

Workaround: If the IP address is modified as well as the subnet mask, the change is successful. Therefore, perform the change in two steps, as follows:

1. Change the IP address.
2. Change the IP address back to the original IP address and also modify the subnet mask to the desired value.

This example shows how to change the subnet mask from 255.255.255.0 to 255.255.254.0 for IP address 10.10.10.10:

```
SCE(config if)#> ip address 20.20.20.20 255.255.255.0
SCE(config if)#> ip address 10.10.10.10 255.255.254.0
```

CSCsw48843

Insertion and removal of either the fan tray or a PSU is not properly indicated in the system. Refer to the following list.

- User message log:
  - Shows messages for fan tray and PSU insertion
  - Does not show messages for fan tray and PSU removal
- SNMP traps
  - SNMP trap exists for PSU removal
  - No SNMP trap exists for fan tray removal
  - No SNMP traps exist for fan tray or PSU insertion

Workaround: To obtain information regarding fan tray and PSU insertion or removal, use the following commands:

- Fan tray—**show environment cooling**
- PSU—**show environment power**

These commands must originate with the operator rather than providing an alert to the operator.

CSCsw79802

A second PP upgrade on top of the SCE8000 might end with hardware watchdog and a reload. The probability of this scenario occurring is about 1 in 10.

Workaround: None

CSCsx40066

When you establish a connection to Cisco SCE8000 using Telnet, the client failed to acquire the IP address and the connection is aborted.

Workaround: Implement any of the following workarounds:

- Modify the DNS server entries to map the client IP address and hostname correctly.
- Use a client with IP address which does not exist in the DNS table to avoid the IP address being converted to a hostname by the DNS.
- Remove the DNS configuration from the Cisco SCE8000. Use the console to remove the DNS configuration.
- Use SSH instead of Telnet.

Open Caveats—Cisco SCE 1000 and Cisco SCE 2000

CSCpu11798

When a PQI application file is installed or upgraded on the SCE, the SCE may lose a few packets for a few seconds. The overall percentage of this phenomenon is very low.

Workaround: Perform the upgrade in non-peak time.

CSCsc49573

When VAS mode is enabled, the system generally assumes that traffic with a VLAN tag is VAS traffic coming from the VAS servers, and therefore forwards it to the non-VAS link.

However, under the following conditions, a flow is forwarded by the SCE platform on the same link on which it was received and with no VLAN tag:

- VAS mode is enabled
- The FIF packet has a VLAN tag
- A traffic rule to bypass the flow exists, or the SCE platform is in congestion

In some topologies, this behavior may cause VAS traffic to be incorrectly routed back to the VAS link.

CSCse05325

When the VAS Health Check initializes, the **show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>** command shows the server being UP even if it is actually Down

The operative state of a VAS server while the Health Check is in Init state is considered to be Up as shown in the CLI command **show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>**. In addition, during this time, the SCE platform may forward VAS traffic to this server.

CSCsj32282

A tunnel-id-based traffic rule defining DSCP marking applies the DSCP marking to non-tunneled traffic, also.

Workaround: When you define the traffic rule, always set the URG flag. For existing rules, replace with a new rule that is identical, with the addition of setting the URG flag.

CSCsj85601

When you remove all VPNs from the SM using the **--force** option, some management operations cannot be performed on the SCE until the operation completes. This occurs only when you remove several VPNs that have active subscriber mappings in the SCE.

Workaround: Instead of removing the VPNs along with their subscriber mappings by using the **--force** option, remove the subscribers first, and only then remove the VPNs (without the **--force** option).

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.