Release Notes for Catalyst 6500 Series Switch Content Switching Module with SSL Software Release 2.1(14)

Revised: January 27, 2012, OL-7028-14

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module with SSL (CSM-S) software release 2.1(14) operating on a Catalyst 6500 series switch with a Supervisor Engine 2 with MSFC2 and Cisco IOS Release 12.2(18)SXD or higher or with a Supervisor Engine 720 and Cisco IOS Release 12.2(18)SXE or higher, or Supervisor Engine 720-10G and Cisco IOS Release 12.2(33)SXI2 or higher.

Note Except where specifically differentiated, the term "Catalyst 6500 series switches" includes both Catalyst 6500 series and Catalyst 6000 series switches.

Contents

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

System Requirements

This section describes the system requirements for the Catalyst 6500 series CSM-S software release 2.1(14).

Memory Requirements

The minimum recommended memory for a chassis with a CSM-S must include a Supervisor Engine with 256 MB of DRAM and an MSFC2 with 256 MB of DRAM. For specific requirements, consult the Cisco Feature Navigator (http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp).

Hardware Supported

Before you can use the Catalyst 6500 series CSM-S, you must have a Supervisor Engine 2 with an MSFC2 or a Supervisor Engine 720 and any module that has ports to connect server and client networks.

Caution The WS-X6066-SLB-S-K9 CSM-S are not fabric enabled, but the module can operate in a fabric-enabled chassis like any other nonfabric module.

Product Number	Minimum Cisco IOS Software	Recommended Cisco IOS Software	Recommended Catalyst Operating System Software
Content Switching Module			
Supervisor Engine 2 with MSFC2	12.2(18)SXD	12.2(18)SXD and higher	Not applicable
Supervisor Engine 720	12.2(18)SXE	12.2(18)SXE and higher	Not applicable
Supervisor Engine 720 -10G	12.2(33)SXI2	12.2(33)SXI2	Not applicable
Console Cable			
72-876-01		Not applicable	
Accessory Kit			
800-05097-01		Not applicable	

Software Requirements

Caution The CSM-S release is not supported by the Catalyst operating system software.

Table 1 lists the software releases for the CSM-S.

Table 1 CSM-S Software Requirements

CSM-S Software	Software Part Number	Hardware Module	Catalyst Operating System Software	Cisco IOS Software
2.1(14)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(13)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(12)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(11)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(10)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(9)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(8)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(7)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(6)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(5)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(4)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(3)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(2a)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher

Table 1 CSM-S Software Requirements (continued)

CSM-S Software	Software Part Number	Hardware Module	Catalyst Operating System Software	Cisco IOS Software
2.1(14)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(13)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(12)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(11)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(10)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(2)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
2.1(1)	SC6K-2.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher

Software Compatibility

The minimum version that is listed is required to support the CSM-S hardware with a given supervisor engine to perform basic CSM-S configuration.

The recommended version is the base version to support new commands for a given CSM-S release.

Table 2 and Table 3 list the CSM-S software release compatibility.

Note Support for the CSM-S is removed in Cisco IOS Software Release 12.2(33)SXH and later releases up to Release 12.2(33)SXI. The support for the CSM-S is reenabled in Cisco IOS Software Release 12.2(33)SXI2.

Table 2 Cisco IOS Software on the Supervisor Engine and MSFC

CSM-S Software	Cisco IOS Software
2.1(14)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(14).
2.1(13)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(13).

Table 2 Cisco IOS Software on the Supervisor Engine and MSFC

CSM-S Software	Cisco IOS Software
2.1(12)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(12).
2.1(11)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(11).
2.1(10)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(10).
2.1(9)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(9).
2.1(8)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(8).
2.1(7)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(7).
2.1(6)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(6).
2.1(5)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(5).
2.1(4)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(4).
2.1(3)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(3).
2.1(2a)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(2a).
2.1(2)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(2).
2.1(1)	12.2(18)SXD or higher for the features new to CSM-S release 2.1(1).

Table 3 Catalyst Operating System Software on the Supervisor Engine and Cisco IOS Software on the MSFC

CSM-S Software	Catalyst Operating System Software
2.1(x)	The CSM-S is not supported by the Catalyst operating system software.

Software Release 2.1(14)

CSM-S software release 2.1(14) is a maintenance release with no new features.

The CSM-S software release 2.1(14) is a combination of the following software releases:

- CSM software release 4.2(15)
- SSL software release 2.1(13s)

Software Release 2.1(13)

CSM-S software release 2.1(13) is a maintenance release with no new features.

The CSM-S software release 2.1(13) is a combination of the following software releases:

- CSM software release 4.2(14)
- SSL software release 2.1(13s)

Software Release 2.1(12)

CSM-S software release 2.1(12) is a maintenance release with no new features.

The CSM-S software release 2.1(12) is a combination of the following software releases:

- CSM software release 4.2(13)
- SSL software release 2.1(13s)

Software Release 2.1(11)

CSM-S software release 2.1(11) is a maintenance release with no new features.

The CSM-S software release 2.1(11) is a combination of the following software releases:

- CSM software release 4.2(12)
- SSL software release 2.1(13s)

Software Release 2.1(10)

CSM-S software release 2.1(10) is a maintenance release with no new features.

The CSM-S software release 2.1(10) is a combination of the following software releases:

- CSM software release 4.2(11)
- SSL software release 2.1(12s)

Software Release 2.1(9)

CSM-S software release 2.1(9) is a maintenance release with no new features.

The CSM-S software release 2.1(9) is a combination of the following software releases:

- CSM software release 4.2(10)
- SSL software release 2.1(12s)

Software Release 2.1(8)

CSM-S software release 2.1(8) is a maintenance release with no new features.

The CSM-S software release 2.1(8) is a combination of the following software releases:

- CSM software release 4.2(9)
- SSL software release 2.1(11)

Software Release 2.1(7)

CSM-S software release 2.1(7) is a maintenance release with no new features.

The CSM-S software release 2.1(7) is a combination of the following software releases:

- CSM software release 4.2(8)
- SSL software release 2.1(11)

Software Release 2.1(6)

CSM-S software release 2.1(6) is a maintenance release with no new features.

The CSM-S software release 2.1(6) is a combination of the following software releases:

- CSM software release 4.2(7)
- SSL software release 2.1(9)

Software Release 2.1(5)

CSM-S software release 2.1(5) is a maintenance release with no new features.

The CSM-S software release 2.1(5) is a combination of the following software releases:

- CSM software release 4.2(6)
- SSL software release 2.1(9)

Software Release 2.1(4)

CSM-S software release 2.1(4) is a maintenance release with no new features.

The CSM-S software release 2.1(4) is a combination of the following software releases:

- CSM software release 4.2(5)
- SSL software release 2.1(9)

Software Release 2.1(3)

CSM-S software release 2.1(3) is a maintenance release with no new features.

The CSM-S software release 2.1(3) combines the following software releases:

- CSM software release 4.2(4)
- SSL software release 2.1(9)

Software Release 2.1(2a)

The CSM-S software release 2.1(2a) combines the following software releases:

- CSM software release 4.2(3a)
- SSL software release 2.1(8)

Software Release 2.1(x) Features

CSM-S software release 2.1(x) contains feature sets that support SSL and functionality from earlier CSM-S releases. The tables in this section list supported feature sets.

Table 4 lists the CSM-S features available in this release and earlier CSM-S software releases.

Table 4 CSM-S Feature Set Description

Features
Supported Hardware
Supervisor 2 with MSFC2 with Cisco IOS software Release 12.2(18)SXD and higher
Supervisor Engine 720 Cisco IOS software Release 12.2(18)SXE and higher
Supported Protocols
TCP load balancing
UDP generic IP protocol load balancing
Special application-layer support for FTP and the Real Time Streaming Protocol (RTSP)
Layer 7 Functionality
Full regular expression matching
URL, cookie switching, Generic HTTP header parsing, HTTP method parsing
Miscellaneous Functionality
VIP connection watermarks
Backup (sorry server) and server farm
Optional port for health probes
IP reassembly
TCL (Toolkit Command Language) scripting
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)–requires a license
Resource usage display
Configurable idle and pending connection timeout
Idle timeout for unidirectional flows
SSL Services Module (SSLM) integration for SSL load balancing
Real server names
TCP connection redundancy for all types of flows (TCP, UDP, and IP)

Table 4 CSM-S Feature Set Description (continued)

Features
Fault tolerant **show** command enhancements
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)
Multiple CSMs in a chassis
CSM and Cisco IOS-SLB functioning simultaneously in a chassis
Configurable HTTP 1.1 persistence (either all GETs are made to the same server or are balanced to multiple servers)
Fully configurable NAT
Server-initiated connections
Route health injection
Load-balancing Algorithms
Round-robin
Weighted round-robin (WRR)
Least connections
Weighted least connections
URL hashing
Source IP hashing (configurable mask)
Destination IP hashing (configurable mask)
Source and destination IP hashing (configurable mask)
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-IPSec load balancing
Generic IP devices and protocols
Stickiness
Cookie sticky with configurable offset and length
SSL ID
Source IP (configurable mask)
HTTP redirection
Redundancy
Sticky state
Full stateful failover (connection redundancy)
Health Checking

Table 4 CSM-S Feature Set Description (continued)

Features
HTTP
ICMP
Telnet
TCP
FTP
SMTP
DNS
Return error-code checking
Inband health checking
User-defined TCL scripts
Management
SNMP traps
Full SNMP and MIB support
XML interface for remote CSM configuration
Back-end encryption support
Workgroup Manager Support
Server Application State Protocol (SASP)

Table 5 lists the CSM-S features in this release.

Table 5 CSM-S Feature Set Description

Features
Supported Hardware
Supervisor Engine 2 with MSFC2
Supervisor Engine 720
Supported Software
Cisco IOS software Release 12.2(18)SXD with the Supervisor Engine 2
Cisco IOS software Release 12.2(18)SXE and higher with Supervisor Engine 720
SSL Features
SSL initiation
SSL version 2.0 forwarding
URL rewrite
HTTP header insertion
Wildcard proxy
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0

Table 5 CSM-S Feature Set Description (continued)

Features
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Session timeout
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA
Hash Algorithms
MD5
SHA1
Cipher Suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CSC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
Public Key Infrastructure
RSA key pair generation for certificates up to 2048-bit
Secure key storage in CSM-S flash memory device
Certificate enrollment for client and server-type proxy services
Importing and exporting of key and certificate (PKCS12 and PEM)
Duplicating keys and certificates on standby CSM-S using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring keys and certificates
Auto-enrollment and auto-renewal of certificates
Importing of certificate authority certificates by cut-and-paste or TFTP
Up to 8 levels of certificate authority in a certificate chain
Generating of self-signed certificate
Manual certificate enrollment using cut-and-paste or TFTP of PKCS10 CSR file
Peer (client and server) certificate authentication
Peer (client and server) certificates
Certificate security attribute-based access control lists
Certificate revocation lists (CRL)

Table 5 CSM-S Feature Set Description (continued)

Features
Certificate expiration warning
TCP Termination
RFC 1323
Connection aging
Connection rate
NAT[1]/PAT[2]
Client and server
Redundancy
No SSL access in standby state
For redundancy, use either two CSMs or two CSM-S not a mix of CSM and CSM-S for supported redundancy configuration
High Availability
Failure detection (SLB health monitoring schemes)
Module-level redundancy (stateless)
Serviceability
Password recovery
Statistics and Accounting
Total SSL connections attempt per proxy service
Total SSL connections successfully established per proxy service
Total SSL connections failed per proxy service
Total SSL alert errors per proxy service
Total SSL resumed sessions per proxy service
Total encrypted/decrypted packets/bytes per proxy service
Statistics displayed at 1 second, 1 minute, and 5 minutes traffic rate for CPU utilization and SSL-specific counters

1. NAT = Network Address Translation
2. PAT = Port Address Translation

New and Changed Information

- CSCsv78324

  A new environmental variable CLIENT_NAT_NO_PAT is introduced to allow the disabling of port address translation (PAT) when client network address translation (NAT) is enabled. A new counter is added in the dump of LB Statistics to indicate that PAT was necessary due to a port collision.

  In normal client NAT operation, a client packet's source IP address is translated (NAT) and the source port number is translated (PAT). When the environmental variable CLIENT_NAT_NO_PAT is set, the CSM retains the original source port number when possible. If the original source port number is already in use by another connection, the CSM-S must perform PAT to avoid port collision.

The CLIENT_NAT_NO_PAT variable has the following syntax:

Name: CLIENT_NAT_NO_PAT
Rights: RW
Default: 0
Valid values: Integer (0 to 1)
Description: Disables (1 = no PAT) PAT where possible when client NAT is performed.

This example shows how to configure the environment variable to disable PAT where possible:

```
Router(config-module-csm)# variable CLIENT_NAT_NO_PAT 1
```

To track instances when PAT was necessary to avoid a port collision, a new client NAT source port collision counter ("Cl NAT src port collis.") is introduced in the LB Statistics, which are displayed using the Venus Console. This counter is updated only when CLIENT_NAT_NO_PAT is set.

This example shows how to display the client NAT source port collision counter:

```
VENUS# dump_lb_stats
------------------------------------------------------------
...
----------------------- LB Statistics ----------------------
------------------------------------------------------------
...
        LB Rjct: no cl NAT port                         0
        Cl NAT src port collis.                         0
```

This change appears in CSM-S software release 2.1(10).

- CSCsl42088

  A new subcommand **min-chain-length** is added to the **crypto pki trustpoint** command.

  When a trustpoint is associated with an SSL-proxy service, it is subjected to several validity checks. One such check requires that the trustpoints on the SSLM can be chained together to form a full certificate chain that terminates with a self-signed root CA certificate. The new **min-chain-length** command allows this requirement to be modified. The default value of **min-chain-length** is zero, which means that a full certificate chain must be present. If **min-chain-length** is set to a nonzero value, the check passes if the chain either terminates in a root CA certificate or if the number of certificates in the chain is at least the **min-chain-length** value.

  The **min-chain-length** command was introduced because an HTTPS server does not need to present a full certificate chain to a browser, because the browser can complete the chain using its preinstalled root CA certificates. In fact, it may be desirable for the server to present a partial certificate chain to support a range of browsers with varied root CA certificates. If the browser has a root CA certificate that can be used to complete the certificate chain, the server's certificate will be accepted.

  This command affects the check only at the time that the trustpoint is associated with the service. After making a change to the **min-chain-length** value, you should disassociate the trustpoint from the service, and then reassociate it.

  Following is an example of the **min-chain-length** command:

  ```
  Router# config terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  Router(config)# crypto pki trustpoint server1
  Router(ca-trustpoint)# min-chain-length 3
  ```

  This change appears in CSM-S software release 2.1(9).

- CISCO-SLB-MIB, CISCO-SLB-EXT-MIB, and CISCO-SLB-HEALTH-MON-MIB are supported for the CSM. Some of the tables defined earlier in CISCO-SLB-EXT-MIB have since been moved to the CISCO-SLB-HEALTH-MON-MIB. This change does not affect the behavior of the SNMP walk on those tables.

  The new CISCO-SLB-HEALTH-MON-MIB can be found at this location:

  ftp://ftp-sj.cisco.com/pub/mibs/v2/CISCO-SLB-HEALTH-MON-MIB.my

- CSCeg51185

  To improve the ability of SNMP trap receivers to display meaningful alarm and event messages, additional varbinds have been added in the following traps:

  - ciscoSlbVirtualStateChange - slbVirtualServerFarmName, slbVirtualIpAddress, slbVirtualPort
  - ciscoSlbRealStateChange - slbRealServerFarmName, slbRealIpAddress, slbRealPort

  This change appears in CSM-S software release 2.1(6).

- CSCsj26953

  A new state, standby(16), has been added to the MIB object slbRealServerState.

  This change appears in CSM-S software release 2.1(7).

- CSCsg90464

  In a fault tolerant (FT) application, the primary CSM-S can become unresponsive when the workload of the onboard IXP network processor exceeds 100 percent. Because the CSM-S software does not check the status of the network processor, this condition may not be detected and CSM-S failover may not occur. Two environment variables are added to cause the CSM-S to check the network processor utilization and to set a network processor utilization limit that, if exceeded, will result in a forced reset and a core dump of the CSM-S.

  The new environment variables have the following syntax:

  Name: IXP1_UTIL_CHECK
  Rights: RW
  Default: 0 (Disabled)
  Valid Values: Integer (0 to 1)
  Description: (Enable = 1) If the CPU utilization of the IXP network processor exceeds the value set in IXP1_OVERLOAD, a CSM reset and a core dump will result.
  Name: IXP1_OVERLOAD
  Rights: RW
  Default: 101
  Valid Values: Integer (101 to 1431655764)
  Description: Sets the CPU utilization percentage of the IXP network processor that will trigger a forced reset of the CSM-S. We recommend a setting of 101 percent.

  This example shows how to configure the environment variables to trigger a forced reset and core dump of the CSM if the network processor workload exceeds 101 percent:

  ```
  Router(config-module-csm)# variable IXP1_OVERLOAD 101
  Router(config-module-csm)# variable IXP1_UTIL_CHECK 1
  ```

  This change appears in CSM-S software release 2.1(6).

- CSCsg48830

  The FTP_CLOSE_DATA_CONN environment variable controls how the CSM-S treats an FTP Transfer Complete (226) response. Some FTP servers will continue to use the same data ports after issuing a Transfer Complete response. Because the CSM-S closes the connection after the Transfer Complete response, it does not recognize the additional traffic on the old data port. The new

environment variable allows the server to reuse the same port after sending the Transfer Complete response. Because this function is only required for specific server or customer configurations, the function is selected through the environment variable.

The FTP_CLOSE_DATA_CONN variable has the following syntax:

Name: FTP_CLOSE_DATA_CONN
Rights: RW
Value: 0
Default: 0
Valid values: Integer (0 to 1)
Description: Close data channels after a Transfer Complete response (0) or allow data port reuse (1).

This example shows how to configure the environment variable:

```
Router(config-module-csm)# variable FTP_CLOSE_DATA_CONN 1
```

This change appears in CSM-S software release 2.1(5).

- CSCek56247

  The **count_sticky_entries** command has been added to display the number of active sessions in the sticky table. This command has no arguments, and returns the number of sessions reported by the **show mod csm <> sticky** command.

  This command is added in CSM-S software release 2.1(5).

- CSCsg29140

  The environment variable MAX_COOKIE_SIZE will now be automatically set to the size of the largest cookie currently configured. The user can change the value of this variable, but if cookies are subsequently added, deleted, or changed, the value may be automatically revised.

  This change appears in CSM-S software release 2.1(5).

- CSCsa58499

  The sticky entry times out with active flows. The sticky timer resets when new connections encounter a sticky entry. Sticky entries are kept in the sticky table only as long as the client keeps opening new connections at an interval smaller than the sticky timeout. If there is an open connection from a client, that connection is not enough to maintain the sticky entry associated with it in the sticky table. For example, with a sticky timer of 30 minutes and a connection open for one hour, after 30 minutes the sticky entry for that client is removed although that client has an open connection.

  The NO_TIMEOUT_IP_STICKY_ENTRIES environment variable is introduced to configure timeout policy for IP sticky entries with active sessions. The problem is resolved by having the sticky timer for a specific entry reset from the point where the last session ends. When NO_TIMEOUT_IP_STICKY_ENTRIES is set to 1, this timeout policy applies to sessions using IP sticky only. Sessions using other forms of persistence (for example cookie, SSL ID) are not affected by the environment variable.

  The NO_TIMEOUT_IP_STICKY_ENTRIES variable has the following syntax:

  Name: NO_TIMEOUT_IP_STICKY_ENTRIES
  Rights: RW
  Value: 0
  Default: 0
  Valid values: Integer (0 to 1)
  Description: Timeout (1 = no timeout) policy for IP sticky entry with active sessions

  This example shows how to configure the sticky environment variable:

```
Router(config-module-csm)# variable NO_TIMEOUT_IP_STICKY_ENTRIES 1
```

- CSCek02947

  The SASP_RETRY_COUNT variable is introduced to configure the Server/Application State Protocol (SASP) retry count. The default value is 8; valid values are from 2 to 30.

- CSCsj26680

  The CHECK_REALS_PERIOD environment variable is introduced to rate-limit the checking of the number of available real servers when a server farm threshold has been configured. If the period since the last counting of servers has not exceeded the configured value (from 1 to 10 seconds), the result from the previous count will be used when making a load-balancing decision. The default value is 0 seconds.

  This change appears in CSM-S software release 2.1(7).

Limitations and Restrictions

- A CSM-S will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

  ```
  vserver test
   virtual a.b.c.d  tcp 0 service termination
   serverfarm servers1
   persistent rebalance
   domain shrun
   inservice
  ```

  If you need to ping the virtual server, do not configure service termination on the virtual server.

- Do not use the **ping** command in a TCL script for a destination that is one or more hops away.

  The **TCL ping()** command uses an underlying ping function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a “destination unreachable” message to the CSM-S if the router determined that the subnet for this IP address is unknown.

- The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. This situation can occur when you configure a virtual server, which the CSM-S uses to parse the RSTP service, and on the same virtual server that you configure a client NAT on the server farm. In this situation, we recommend that you either remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- If your configuration contains a pair of CSM-Ss in a single fault-tolerant group, and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group. This action causes the fault-tolerant pair of CSM-Ss to enter an invalid active-active state. In this case, remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- Configure a client NAT pool with the server farm IP address instead of using the **static nat** command. The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a server farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.
- On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.
- When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
   backup real name SERVER-A
   inservice
 probe <NAME>
```

  If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.
- Internal ports on the CSM-S (dot1q, trunk, port-channel, and so on) are automatically configured, with the exception of the VLANs on the trunk, which must be manually added using the **set trunk** *slot* 1 *vlan-list* command in Catalyst operating system.
- When configuring Route Health Injection (RHI), proxy ARP must be disabled on the Catalyst 6500 series chassis (proxy-ARP is enabled by default). You must disable proxy ARP on a per-interface basis in the interface submode. We recommend that you disable proxy ARP on the VLAN level using the **no ip proxy arp** command.
- Check the documentation for your chassis to determine whether any slot restrictions apply.
- There is no support for client NAT of IP protocols other than TCP or UDP.
- If neither a real server nor a corresponding virtual server has an explicitly configured TCP/UDP port, then probes requiring such a port are not activated. All CSM-S health probes other than ICMP periodically create connections to specific TCP or UDP ports on configured real servers. If a health probe is configured on a real server without a configured TCP or UDP port, the CSM-S chooses the TCP or UDP port to probe from the virtual servers with which the real server is associated. If neither the real server nor the virtual server has a configured port, the CSM-S simply ignores any configured probes requiring ports to that real server.
- When cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal, use Telnet instead of the console port to avoid a serial buffer overrun.
- After upgrading the SSL software, the SSL proxy service might remain in a down state when displaying a “No Server/Next HOP MAC” message, even though the server is reachable. This situation might occur after reload. If this situation occurs, remove the server IP addresses from the proxy service, and reconfigure the proxy service to restart the service. (CSCei12818)

- Windows 2000 certificate authorities occasionally reject certificate enrollment requests that are issued by the SSL Services Module. The problem originated with the SCEP DLL and is fixed on the .net version of the certificate authority but not on the Windows 2000 version. If this situation occurs, restart the certificate authority, and issue the enrollment request again. (CSCea53069)
- The SSL Services Module with a virtual TCP policy that is configured with a low TCP maximum segment size (MSS) value (for example, 256), and with the default SYN timeout on the server side, might experience a software-forced reset due to exhausted resources if the following events occur simultaneously:
  - The real server is unreachable.
  - There is a burst of approximately 26,000 TCP SYN requests to establish a client connection.
  - All connections enter the ESTABLISHED state in TCP before the HTTP requests are sent on any of the connections.
  - The HTTP requests are more than three times the size of the negotiated MSS value.

  If this situation occurs, do one of the following:
  - Stabilize the real server so that it is reachable.
  - Enable the health probe for a real server on the CSM-S. (CSCed53976)
- The module might take longer to boot if there are client NAT pools in the startup configuration. The delay is proportional to the number of NAT pools in the configuration. With the maximum supported number of NAT pools (64), the delay is up to 4 minutes. (CSCdy56573)
- If you enter the **clear arp** command on the SSL Services Module, all proxy services go into a down state and then go into an up state. (CSCdy77843)
- When 828 days have elapsed since the CSM-S was booted, the HTTP probe will fail and will stay in the down state for about 18 minutes. Reboot the CSM-S before 828 days have elapsed. (CSCso08858)
- When configuring the CSM-S for fault tolerance, we recommend that you configure a dedicated link for the fault-tolerant VLAN.

  Note Configuring stateful redundancy with the CSM-S in separate chassis requires a gigabit link between the CSM-S.

  Note CSM-S configuration synchronization is supported if the system uses Cisco IOS software in the supervisor engine. It is not supported if the system uses Catalyst operating system software in the supervisor engine.
- The total conns established counter applies only to an active CSM-S. The standby CSM-S might display the total established connections when there is a fault-tolerance switchover, but the total conns established counter remains unchanged. (CSCtn16345)

Caveats

These sections describe the open and resolved caveats in CSM-S software:

- Open Caveats in Software Release 2.1(14) for CSM, page 20
- Resolved Caveats in Software Release 2.1(14) for CSM, page 20

Open Caveats in Software Release 2.1(14) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(14), see the "Resolved Caveats in Software Release 2.1(14) for CSM" section on page 20.

There are no open CSM caveats in CSM-S software release 2.1(14).

Resolved Caveats in Software Release 2.1(14) for CSM

Note For a description of open caveats in CSM software release 2.1(14), see the "Open Caveats in Software Release 2.1(14) for CSM" section on page 20.

This section describes resolved caveats in CSM software release 4.2(15):

- CSCtg41899

  If a new regular expression domain match is added to the GSLB configuration, CSM does not match specific regular expression domains and a wrong A-record response is returned that does not match the correct policy map.

Workaround: None.

- CSCtn86332

  If a serverfarm going down or up is configured on multiple VIPs, the VIP state change syslog is sent for only one VIP and not for all the VIPs.

  Workaround: None.

- CSCtj90108

  With the static NAT configured, server initiated connections may fail on a higher traffic rate.

  Workaround: Disable static NAT.

- CSCtk63031

  The FTP connections do not time out and prevent new connections.

  Workaround: Clear all connections associated with the server. Downgrade your CSM to any CSM release below 4.2(14). Clear all slowpath connections using slowpath_reap_sessions in VENUS.

- CSCts71706

  The sticky replication is not working on CSM 4.2(14).

  Workaround: None.

Open Caveats in Software Release 2.1(14) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(14), see the "Resolved Caveats in Software Release 2.1(14) for SSL" section on page 21.

This section describes the open SSL caveats in CSM-S software release 2.1(14):

- No new open caveats for SSL.

Resolved Caveats in Software Release 2.1(14) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(14), see the"Open Caveats in Software Release 2.1(14) for SSL" section on page 21.

This section describes the SSL caveats resolved in CSM-S software release 2.1(14):

- No new resolved caveats for SSL.

Open Caveats in Software Release 2.1(13) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(13), see the "Resolved Caveats in Software Release 2.1(13) for CSM" section on page 22.

There are no open CSM caveats in CSM-S software release 2.1(13).

Resolved Caveats in Software Release 2.1(13) for CSM

Note For a description of open caveats in CSM software release 2.1(13), see the "Open Caveats in Software Release 2.1(13) for CSM" section on page 21.

This section describes resolved caveats in CSM software release 4.2(14):

- CSCte28717

  The source-ip sticky may stop working after an extended uptime of approximately 470 days or more. The CSM will not create a new sticky entry.

  Workaround: None.

- CSCte39053

  The default expiration date of the cookies inserted by the CSM is Thursday, 1 Jan 2099, 01:01:50 GMT. After this time, the cookie-insert sticky will not work as expected.

  Workaround: The default cookie expiration date can be changed by setting the COOKIE_INSERT_EXPIRATION_DATE environment variable on the CSM. For example, you can move the expiration date to May 25, 2020, by using the following commands:

  ```
  Router# config t
  Router(config)# mod csm 8
  Router(config-module-csm# variable COOKIE_INSERT_EXPIRATION_DATE "Mon, 25 May 2020
  08:00:00 GMT"
  ```

  Make sure to change the slot number. The new expiration date changes in the inserted cookies immediately because this change does not require a reboot of the CSM. This change will not affect the network traffic.

- CSCtg56193

  When the uptime of CSM is more than 828 days, the FTP or RTSP Layer 7 connections are not timing out.

  Workaround: None.

- CSCth52331

  When a standby CSM reaches an uptime of 828 days, the standby CSM can assert mastership for a very short period (around 2 seconds), which creates an active/active situation.

  Workaround: None.

- CSCtg45008

  A new variable, L7_TX_CORE_QUEUE_TIMEOUT, is added to address CSCsh53633, where the CSM that runs release 4.2(6) might reboot due to an IXP 3 and the type of crash is "L7 abort."

  Variable Name: L7_TX_CORE_QUEUE_TIMEOUT

  Rights: RW

  Value: 1

  Default: 1

  Valid values: Integer (1 to 10).

  Description: Time (in seconds) to wait for the Layer 7 TX Core queue to come out of the full state before asserting a core.

  Workaround: None.

Open Caveats in Software Release 2.1(13) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(13), see the "Resolved Caveats in Software Release 2.1(13) for SSL" section on page 23.

This section describes the open SSL caveats in CSM-S software release 2.1(13):

- No new open caveats for SSL.

Resolved Caveats in Software Release 2.1(13) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(13), see the"Open Caveats in Software Release 2.1(13) for SSL" section on page 23.

This section describes the SSL caveats resolved in CSM-S software release 2.1(13):

- No new resolved caveats for SSL.

Open Caveats in Software Release 2.1(12) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(12), see the "Resolved Caveats in Software Release 2.1(12) for CSM" section on page 23.

This section describes the open CSM caveats in CSM-S software release 2.1(12):

- CSCte28717

  The source-ip sticky may stop working after an extended uptime of approximately 470 days or more. The CSM will not create a new sticky entry.

  Workaround: Reboot the CSM.

Resolved Caveats in Software Release 2.1(12) for CSM

Note For a description of open caveats in CSM software release 2.1(12), see the "Open Caveats in Software Release 2.1(12) for CSM" section on page 23.

This section describes resolved caveats in CSM software release 4.2(13):

- CSCtd31622

  The default expiration date of the cookies inserted by the CSM is Friday, 1 Jan 2010, 01:01:50 GMT. After this time, the cookie-insert sticky will not work as expected.

  Workaround: The default cookie expiration date can be changed by setting the COOKIE_INSERT_EXPIRATION_DATE environment variable on the CSM. For example, you can move the expiration date to May 25, 2020, by using the following commands:

```
Router# config t
Router(config)# mod csm 8
Router(config-module-csm# variable COOKIE_INSERT_EXPIRATION_DATE
"Mon, 25 May 2020 08:00:00 GMT"
```

Make sure to change the slot number. The new expiration date changes in the inserted cookies immediately as this change does not require a reboot of the CSM. This change will not affect the production traffic.

- CSCtc25780

  In rare cases, when CSM fault tolerant (FT) synchronization is performed with the **hw-module csm** *mod* **standby config-sync** command and FT VLAN is intermittently down, the standby CSM may send out an ARP packet towards the Layer 2 adjacent nodes using its physical MAC-address, instead of its virtual MAC-address. This causes an outage until the ARP table cache is either cleared or times out.

  Workaround: To prevent rapid failover in the standby CSM2 node, increase the failover timer to 120 seconds on both CSM nodes (active and standby).

Open Caveats in Software Release 2.1(12) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(12), see the "Resolved Caveats in Software Release 2.1(12) for SSL" section on page 24.

This section describes the open SSL caveats in CSM-S software release 2.1(12):

- No new open caveats for SSL.

Resolved Caveats in Software Release 2.1(12) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(12), see the"Open Caveats in Software Release 2.1(12) for SSL" section on page 24.

This section describes the SSL caveats resolved in CSM-S software release 2.1(12):

- No new resolved caveats for SSL.

Open Caveats in Software Release 2.1(11) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(11), see the "Resolved Caveats in Software Release 2.1(11) for CSM" section on page 25.

This section describes open caveats in CSM software release 2.1(11):

- CSCsz25520

In rare cases, CSM may propagate an invalid MAC address table for VLAN 1 with an invalid MAC address back plane across the CSM port channel Po259 to the back plane on management VLAN 1.

The following output displays an invalid MAC address across the CSM port channel Po259 to the back plane on management VLAN 1.

```
Console> enable show mac-address-table | inc 259
*     1  4000.6806.14d9   dynamic  Yes         205   Po259
*     1  4000.6c06.1eb1   dynamic  Yes          90   Po259
*     1  4000.3806.4227   dynamic  Yes          50   Po259
*     1  4000.2e06.47c0   dynamic  Yes         150   Po259
*     1  4000.6c06.916b   dynamic  Yes         255   Po259
*     1  4000.6b06.fe6b   dynamic  Yes         240   Po259
*     1  4000.3406.a2ce   dynamic  Yes         175   Po259
*     1  0000.3206.79e0   dynamic  Yes          15   Po259
*     1  0000.3206.8c3a   dynamic  Yes         135   Po259
*     1  4000.6806.13b8   dynamic  Yes          55   Po259
*     1  0000.3206.69d4   dynamic  Yes          10   Po259
```

Note Only the last 4 bytes of the MAC address change and point to VLAN 1 on the CSM port channel.

Workaround: None.

- CSCsx64648

  On a CSM module, the configuration synchronization times out with a large configuration that ranges from 23 K to 125 K. For example, the configuration synchronization that occurs at 16 K and fails at 23 K.

  Workaround: None.

Resolved Caveats in Software Release 2.1(11) for CSM

Note For a description of open caveats in CSM software release 2.1(11), see the "Open Caveats in Software Release 2.1(11) for CSM" section on page 24.

This section describes resolved caveats in CSM software release 4.2(12):

- CSCsu92969

  Configuring multiple server load balancing (SLB) policies in a particular order causes the connection counter in a real server in the server farm to erroneously report the default maximum connection (MAXCONN) limit of 4294967295 connections. When this condition occurs, the real server refuses new connections.

  Workaround: Remove multiple SLB policies.

- CSCsz81265

  When configuring two virtual servers (Layer 3 and Layer 4) with the same virtual IP address, CSM drops the ICMP request to the virtual IP address. This condition occurs when both virtual servers are operational, and when there is no connection to the Layer 3 virtual server.

  Workaround: Ensure that the Layer 3 virtual server is configured after the Layer 4 virtual server.

- CSCsx37458

Under certain conditions, one or more VIPs on the CSM will not respond to the ping. This condition occurs when the same VIP is used in the virtual server and in a static NAT entry. The VIP may be displayed in the CSM ARP table as an SVR NAT entry instead of a virtual server entry. You can display the CSM ARP table by using **show mod csm** *slot* **arp** command.

Workaround:

1. Suspend all virtual servers for the VIP address that is uncertain.
2. Remove the static NAT configuration for that VIP.
3. Reactivate the virtual servers.
4. Add the static NAT again.

- CSCsz81041

  The CSM does not send a reset upon receiving a synchronize acknowledge (ACK) packet sent to a synchronize start (SYN) packet. This condition occurs in Layer 7 mode when the CSM opens a connection on the backend server, and if the server responds to the SYN with an ACK that has an invalid sequence number.

  Workaround: None.

Open Caveats in Software Release 2.1(11) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(11), see the "Resolved Caveats in Software Release 2.1(11) for SSL" section on page 26.

This section describes the open SSL caveats in CSM-S software release 2.1(11):

- No new open caveats for SSL.

Resolved Caveats in Software Release 2.1(11) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(11), see the"Open Caveats in Software Release 2.1(11) for SSL" section on page 26.

This section describes the SSL caveats resolved in CSM-S software release 2.1(11):

- CSCsy05771

  On a CSM-S module, the TCP or SSL processor fails to boot. This problem occurs after you reboot the module. The processor failure information is not saved.

  Workaround: None.

- CSCsx37391

  On a CSM-S module, the TCP processor fails to boot when you configure the rewrite policy by using **ssl-proxy policy url-rewrite URL-REWRITE** command.

  The following error message is displayed:

```
ssl-proxy policy url-rewrite URL-REWRITE
 url *jp
 url *com
```

```
 url *1
 url *2
 url *3
 url *4
 url *5
 url *6
 url *7
 url *8
 url *9
 url *0
 url 157.2.163.93 clearport 443

0x20D28C:memmove(0x20d200)+0x8c
0x236804:http_rewrite(0x2364b0)+0x354
0x23E1E8:app_do_port_rewrite(0x23e0f0)+0xf8
0x23EBEC:app_do_url_rewrite(0x23e570)+0x67c
0x23B7F4:app_handle_data_from_tcp(0x23b604)+0x1f0
0x23D128:app_handle_st_establish(0x23cfdc)+0x14c
0x23D698:app_ssl_fsm(0x23d3fc)+0x29c
0x23B94C:app_process_tcp_pak(0x23b894)+0xb8
0x23C1BC:app_service_tcp_paks(0x23c0c0)+0xfc
0x231A90:main(0x231494)+0x5fc
```

Workaround: None.

Open Caveats in Software Release 2.1(10) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(10), see the "Resolved Caveats in Software Release 2.1(10) for CSM" section on page 28

This section describes open caveats in CSM-S software release 2.1(10):

- CSCsu92969

  Configuring multiple server load balancing (SLB) policies in a particular order causes the connection counter in a real server in the server farm to erroneously report the default maximum connection (MAXCONN) limit of 4294967295 connections. When this condition occurs, the real server refuses new connections.

  Workaround: Remove multiple SLB policies.

- CSCsv97952

  In rare cases, a CSM-S reloads unexpectedly with the following log message:

  ```
  "%CSM_SLB-3-UNEXPECTED: Module 6 unexpected error: IXP3 exception encountered."
  ```

  A core dump is produced with this header:

  ```
  "IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(00000000h'."
  ```

  Workaround: None.

- CSCsh53633

  In rare cases, a CSM-S rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 2.1(10) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(10), see the"Open Caveats in Software Release 2.1(10) for CSM" section on page 27

This section describes resolved caveats in CSM-S software release 2.1(10):

- CSCsr79179

  When the same gateway IP address is configured in both the **gateway** and **route** statements, the **gateway** statement will be ignored, although it will appear in the running configuration. After a failover or a reconfiguration, the active CSM-S will have no default route, and will drop traffic.

  Workaround: Possible workarounds include the following:

  - Use the **route 0.0.0.0 0.0.0.0 gateway x.x.x.x** command to install the default route.
  - Reload the CSM-S after the configuration synchronization.
  - Use a configuration that does not specify the same gateway address in the **gateway** and **route** statements.

- CSCsq36042

  When SSL stickiness is configured on a backup server farm, the CSM-S fails to perform NAT in some cases.

  Workaround: Disable SSL stickiness on the server farm.

- CSCsu39853

  In rare cases, the CSM-S will stop responding to the CLI but will continue to pass traffic.

  Workaround: None.

Open Caveats in Software Release 2.1(10) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(10), see the "Resolved Caveats in Software Release 2.1(10) for SSL" section on page 28.

This section describes the open SSL caveats in CSM-S software release 2.1(10):

- No new open caveats for SSL.

Resolved Caveats in Software Release 2.1(10) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(10), see the"Open Caveats in Software Release 2.1(10) for SSL" section on page 28 .

This section describes the SSL caveats resolved in CSM-S software release 2.1(10):

- No new resolved caveats for SSL.

Open Caveats in Software Release 2.1(9) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(9), see the "Resolved Caveats in Software Release 2.1(9) for CSM" section on page 29.

This section describes open caveats in CSM-S software release 2.1(9):

- CSCsh53633

  In rare cases, a CSM-S rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 2.1(9) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(9), see the "Open Caveats in Software Release 2.1(9) for CSM" section on page 29.

This section describes resolved caveats in CSM-S software release 2.1(9):

- CSCsm33035

  When the CSM-S starts to load balance using the default policy, and then a GET request matches a URL under a subpolicy, the CSM-S forwards traffic to the real server without modifying the TCP acknowledgement number.

  Workaround: Disable persistent rebalance.

- CSCso00578

  A CSM-S configured for redundancy may have its CSRP replication status stuck in the INIT state.

  Workaround: None.

- CSCso33427

  When the CSM-S is configured to load balance IPsec using one Layer 4 virtual server for IKE and another for ESP, the CSM-S fails to forward to the backend real server any "ICMP can't fragment" messages received at the CSM-S's virtual IP address and relating to the ESP flow.

- CSCso69828

  When cookie-insert is configured on the CSM-S and the server sends the FIN/ACK immediately after its HTTP 200 OK response, the CSM-S may send some subsequent packets out of order and with an incorrect TCP sequence number.

- CSCso81900

  When a NAT pool is modified while configured as part of an SLB policy to a virtual server, traffic is sent to the virtual server with a NAT-supplied source address of 0.0.0.0.

  Workaround: Reboot the CSM-S.

- CSCsq84207

  Path MTU discovery (PMTUD) performed by a server behind a CSM-S is not working correctly if the CSM-S is performing cookie insertion.

  Workaround: Possible workarounds include the following:

- Reduce the server MSS to a value that allows the cookie insertion without exceeding the MTU of the path to the client.
- Reduce the CSM-S default MSS using the environment variable TCP_MSS_OPTION.
- Use a different type of stickiness for the server (for example, application cookies).

Open Caveats in Software Release 2.1(9) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(9), see the "Resolved Caveats in Software Release 2.1(9) for SSL" section on page 32.

This section describes the open SSL caveats in CSM-S software release 2.1(9):

- Configuring NTP on the SSL-M or CSM-S SSL-DC may interfere with the clock synchronization. If the CSM-S SSL-DC is configured to synchronize its clock using NTP, the clock might go out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSL-M. The DC clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)

- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)

- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(9) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(9), see the "Open Caveats in Software Release 2.1(9) for SSL" section on page 30.

This section describes the SSL caveats resolved in CSM-S software release 2.1(9):

- When a backend server redirects a connection from the client to another server by providing a URL, the redirection is successful but the URL is not rewritten. (CSCsi22668)
- A certificate renewal fails when the original trustpoint was created using the **crypto ca import** *name* **pem terminal** *password* command. (CSCsj89254)
- In rare cases, the SSLM may reload when client authentication is enabled with the **authenticate verify all** command and a CRL download is performed while there is significant network congestion.

  Workaround: Disable full client authentication by entering either the **authenticate verify signature-only** command or the **no authenticate verify all** command. (CSCsl10317)
- Custom header insertion fails for consecutive POSTs in a TCP connection. (CSCsl35144)
- The SSLM may reset connections using a timeout interval lower than the defined timeout handshake value for an SSL policy.

  Workaround: Remove the timeout handshake value. The default value of 0 will cause the SSLM to wait until the connection closes for the handshake to complete. (CSCsl54156)
- The SSLM content-scanning logic does not recognize the WebDav HTTP methods identified in RFC-2518. If a header insertion policy is configured, the WebDav request will fail with no response from the SSLM. (CSCsq48567)
- When a URL-rewrite policy is configured with a prefix wildcard, and the URL to be rewritten does not contain a trailing slash (/) or carriage-return (\r), the module resets. (CSCsq57256)
- When the **show ssl-proxy buffers** command shows that the number of TCP ingress data buffers used Current has reached 40 percent of the TCP ingress buffer pool size, the SSLM will not accept any new connections. (CSCso09564)

Open Caveats in Software Release 2.1(8) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(8), see the "Resolved Caveats in Software Release 2.1(8) for CSM" section on page 33.

This section describes open caveats in CSM-S software release 2.1(8):

- CSCso00578

  A CSM configured for redundancy may have its CSRP replication status stuck in the INIT state.

  Workaround: None.

- CSCsh53633

  In rare cases, a CSM rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 2.1(8) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(8), see the "Open Caveats in Software Release 2.1(8) for CSM" section on page 33.

This section describes resolved caveats in CSM-S software release 2.1(8):

- CSCsl40722

  The CSM stops servicing load-balanced connections and probes due to a buffer leak.

  Workaround: Periodically enter the **show mod csm** *slot* **tech-support all | i outstanding** command. If small buffers reach 24500 or medium buffers reach 20000, the buffers are full and you must reboot the CSM.

- CSCsi58089

  The CSM drops SASP server messages that are larger than 2816 bytes.

  Workaround: Reduce the number of servers participating in SASP to reduce the length of the SASP messages.

- CSCsk50939

  The CSM stops responding to CAPP-UDP requests from a Global Site Selector (GSS) after changing the CAPP-UDP setting from secure to no secure.

  Workaround: Reload the CSM.

- CSCsl59508

  When a server farm contains many real servers (for example, 100), the CSM may reboot and create a core dump when you add the **predictor leastconns slowstart** *num* command to the server farm configuration.

- CSCsh94471

  In rare cases, the CSM console becomes unresponsive, and the **show module csm** *num* command indicates that the CSM is offline.

- CSCsl72371

When an XML call is contained in a TCL script probe, the CSM probe fails with a memory allocation failure and the CSM console becomes unresponsive.

- CSCsm84686

  When a client sends a SYN packet to a virtual server with the Explicit Congestion Notification (ECN) and Congestion Window Reduced (CWR) flags set, the CSM drops the SYN packet.

  Workaround: Disable ECN on the client.

- CSCsi85407

  In rare cases, when the CSM-S is load balancing with a URL that spans multiple packets, the CSM will reboot and create a core dump.

- CSCsi82468

  If persistent rebalance is enabled in a virtual server that contains a redirect server farm, the CSM will send two redirect responses for multipacket GET requests. This condition causes high CPU usage.

  Workaround: Disable persistent rebalance on the virtual server that contains a redirect server farm.

- CSCsj05855

  In rare cases, the CSM may reboot and create a core dump due to memory corruption.

Open Caveats in Software Release 2.1(8) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(8), see the "Resolved Caveats in Software Release 2.1(8) for SSL" section on page 36.

This section describes the open SSL caveats in CSM-S software release 2.1(8):

- Configuring NTP on the SSL-M or CSM-S SSL-DC may interfere with the clock synchronization. If the CSM-S SSL-DC is configured to synchronize its clock using NTP, the clock might go out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSL-M. The DC clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)
- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)
- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)
- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(8) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(8), see the "Open Caveats in Software Release 2.1(8) for SSL" section on page 34.

This section describes the SSL caveats resolved in CSM-S software release 2.1(8):

- No new resolved caveats for SSL.

Open Caveats in Software Release 2.1(7) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(7), see the "Resolved Caveats in Software Release 2.1(7) for CSM" section on page 37.

This section describes open caveats in CSM-S software release 2.1(7):

- CSCsh53633

  In rare cases, a CSM-S rebooted because of IXP 3. The type of crash was "L7 abort."

Workaround: None.

Resolved Caveats in Software Release 2.1(7) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(7), see the "Open Caveats in Software Release 2.1(8) for CSM" section on page 33.

This section describes resolved caveats in CSM-S software release 2.1(7):

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM-S traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCsk29021

  When persistent rebalance is configured, the CSM-S will reexamine a persistent GET and remap it if it matches a different policy. As part of the remapping, the CSM-S will send a reset to the old connection. If the header insert feature is configured, this reset message has an incorrect sequence number.

  Workaround: None.

- CSCsg40988

  The CSM-S halts with the following system log (syslog) error: "%CSM_SLB-3-UNEXPECTED: Module 3 unexpected error: FPGA3 exception encountered."

  Workaround: None.

- CSCsg84530

  The CSM-S reloads unexpectedly with the following syslog error: "%CSM_SLB-3-UNEXPECTED: Module 3 unexpected error: PPC exception." The console displays the error message "PPC exception type 1792 on FTReplFlow(0C247500h)" followed by a core dump.

  Workaround: None.

- CSCsi29132

  Clients sending persistent connections to a CSM-S virtual server may see a long delay after an HTTP request. This situation can occur when the virtual server is configured with persistence rebalance and with sticky cookies learned through the server. The CSM-S may not be forwarding the request to the server if the preceding request had an out-of-order response from the server.

  Workaround: Remove persistence rebalance or remove cookies from the virtual server.

- CSCsj26410

  When one of the multiple virtual IP addresses monitored by KeepAlive-Appliance Protocol (KAL-AP) is brought down, the Content and Application Peering Protocol (CAPP) incorrectly returns a load value of 128 rather than the correct load value of 255.

  Workaround: None.

- CSCsj26680

  When you enter the **serverfarm threshold** (vserver submode) command, a CLI lockup can occur. This condition can occur when the primary server farm contains hundreds of real servers that are down and the backup server farm takes over immediately. In this case, the CSM-S performance drops and the CLI becomes unresponsive.

  Workaround: None.

- CSCsj75481

  The CSM-S is not passing SYN-ACK in a policy-based routing (PBR) network when the ROUTE_UNKNOWN_FLOW_PKTS environment variable is set to 2. This environment variable specifies whether to route SYN or non-SYN packets that do not match any existing flows.

  Workaround: Downgrade to a CSM-S version earlier than 2.1(3).

- CSCsj82230

  After removing service termination from a virtual server's virtual IP address, the IP address no longer responds to ping requests.

  Workaround: None.

- CSCsj88014

  A large delay in updating LOAD can occur when using KAL-AP. When a Global Site Selector (GSS) is configured to probe a large number of virtual IP addresses with KAL-AP, the response to the KAL-AP queries slows down, causing the GSS to consider the virtual IPs to be down.

  Workaround: Consolidate virtual servers to reduce their number, or use TCP keepalives instead.

- CSCsk43903

  A pair of CSM-Ss configured for fault-tolerant operation will both enter the active state after 828 days.

  Workaround: None.

- CSCsi96851

  If the CSM-S is configured to track a nonexistent group, and the group ID is the same as a VLAN ID in which an HSRP group is configured, the CSM-S will failover with the syslog message, "Forced failover due to HSRPGroup tracking failures."

  

  Note This resolution is effective only with Cisco IOS Release 12.2SXF10 or later releases, which resolve the associated caveat CSCse54191.

Workaround: None.

- CSCsl23801

  HSRP causes CSM-S static ARP entries to be overwritten with all zeros (00-00-00-00-00-00). This is an unintended result of a previous caveat resolution.

  Workaround: None.

- CSCsk98543

  The CSM-S console might lock up when a backup server farm is configured with a threshold and contains few real servers (for example, less than ten real servers).

  Workaround: Remove the threshold command.

Open Caveats in Software Release 2.1(7) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(7), see the "Resolved Caveats in Software Release 2.1(7) for SSL" section on page 41.

This section describes the open SSL caveats in CSM-S software release 2.1(7):

- Configuring NTP on the SSL-M or CSM-S SSL-DC may interfere with the clock synchronization. If the CSM-S SSL-DC is configured to synchronize its clock using NTP, the clock might go out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSL-M. The DC clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)

- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)

- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(7) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(7), see the "Open Caveats in Software Release 2.1(7) for SSL" section on page 39.

This section describes the SSL caveats resolved in CSM-S software release 2.1(7):

- After normal operation, the SSLM stops inserting the headers to the clear text traffic. This problem happens with software release 2.1.10 only.

  Workaround: Reload the SSLM. (CSCsh79045)

- HTTP POST transactions fail when the total header size is exactly 1536 bytes and when the HTTP header insert policy is used. (CSCsh30757)
- When an HTTP header insert policy is used, an HTTP client will receive an intermittent "Page can not be displayed" error when accessing a secure site. This error occurs because the HTTP header insert feature incorrectly inserts a configured value at the beginning of an HTTP request rather than at the end. (CSCsg82285)
- The location string for URL rewrites is being incorrectly rewritten in some cases. For example, a URL rewrite rule is given in the configuration for the URL, www.cisco.com, and the redirected location field contains the following string:

  http://user.microsoft.com/dir/test.jsp?login=https://www.cisco.com

  The location string is being incorrectly rewritten as follows:

  http://user.microsoft.com/dir/test.jsp?login=httpswww.cisco.com

The rule is supposed to be rewritten if the host portion of the URL matches www.cisco.com. In the situation described here, that is not the case. No rewrite is supposed to occur. In addition, the rewrite should not affect the string https://www.cisco.com so far into the location field. (CSCsg65505)

- SSLM stops accepting new SSL connections because of a depletion of connection IDs on the TCP processor. Enter the **show ssl-proxy stats** command. The condition can occur when there is an approximately 65 KB difference between the conn alloc counters and dealloc counters under TCP. Eventually when all the connection IDs are exhausted, the SSLM will not be able to initiate any more connections to the backend servers.

  Workaround: Reload the module. (CSCek50983)

- When performing a URL rewrite, the location URL in a 302 redirect includes an 80. For example, http://192.168.45.10:80/. (CSCse92180)

- The SSLM fails to pass the entire POST to a server when the header insert is configured in SSL proxy service. This occurred with a POST that had a large payload.

  Workaround: Remove the header insert configuration from the proxy service. (CSCse31785)

Open Caveats in Software Release 2.1(6) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(6), see the "Resolved Caveats in Software Release 2.1(6) for CSM" section on page 43.

This section describes open caveats in CSM-S software release 2.1(6):

- CSCsh53633

  In rare cases, a CSM-S rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

- CSCse91983

  The **show mod csm** *slot* **tech all** command may display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active and CSM-S traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsb56078 (duplicate of CSCei73146)

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

Resolved Caveats in Software Release 2.1(6) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(6), see the "Open Caveats in Software Release 2.1(8) for CSM" section on page 33.

This section describes resolved caveats in CSM-S software release 2.1(6):

- CSCsh25401

  After repeated copying of the startup configuration to the running configuration, the active CSM-S will no longer send its configuration to the standby CSM-S. The active CSM-S will display the following log message: "%CSM_SLB-3-REDUNDANCY: Module 3 FT error: Active: Manual bulk sync timed out."

  Workaround: None.

- CSCsi53667

  Due to a communications error between the CSM motherboard and the SSL daughtercard, the daughtercard will sometimes fail to reload, giving the console message "BOOTP failed to reply. Resend BOOTP REQUEST."

  Workaround: Configure FT tracking from the CSM motherboard to ping the SSL daughtercard to detect a boot failure.

- CSCse93972

  Unless the virtual servers are configured for replication, after a failover from one CSM-S to another, the formerly active CSM-S will send idle resets for persistent flows that it hosted before the failover. If the virtual servers are configured for replication, the backup CSM-S will not send resets.

  Workaround: Configure the virtual servers for replication.

- CSCek31065

  A CSM-S in a redundant configuration with duplicate entries configured under IOS/SLB can generate the following log message: "9w3d: CSM9: Invalid encaps ID for get info." This message can also occur if the user shuts down or advertises PVLANs, or clears the CSM-S arp-cache, or configures "secondary" addresses on an MSFC interface VLAN that is associated with the CSM-S's client/server VLAN.

  Workaround: None.

- CSCek51742

  Under some conditions, the CSM-S will wait more than nine seconds before sending an ARP request for a locally connected device not in the ARP table. This situation occurs when traffic is sent directly through the CSM-S in routed mode with ROUTE_UNKNOWN_FLOW_PKTS set to 2.

Workaround: None.

- CSCek71183

  When using the header insert feature with a header longer than 127 bytes, the rest of the header insert will fail.

  Workaround: Header insert strings within the same map should have the combined length of no more than 127 bytes, including string names and delimiters.

- CSCsd98833

  When a real server is added to a SASP group and the Global Workload Manager (GWM) assigns the new server a weight of 0, the status of the new server should be DFP_THROTTLED. Instead it is shown as OPERATIONAL.

  Workaround: None.

- CSCse93972

  The backup CSM-S can send resets for flows that correspond to virtual servers that are not configured for replication. This can happen after a failover where a long lived flow occurred over the CSM-S when it was the master, but the CSM-S is now the backup. After the idle timeout, the backup CSM-S will send a reset. The backup CSM-S will not send a reset if replication is configured on the virtual server.

  Workaround: Configure replication on the virtual server.

- CSCsg16726

  The CSM-S ignores an initial SYN packet if the push (PSH) bit is set in the SYN packet.

  Workaround: None.

- CSCsg37513

  The CSM-S erroneously classifies certain traffic as cookie-insert, and replicates all Layer 7 sessions as insert sessions, causing an exception crash.

  Workaround: None.

- CSCsg82885

  The CSM-S will not boot after the user configures close to the maximum number of virtual servers and scripted probes attached to the server farm. A warning has been added when the number of TCL scripted probes exceeds 900.

  Workaround: If you need a large number of probes, use CSM-S native probes rather than TCL scripted probes, because native probes consume less memory space.

- CSCsg91075

  A core dump can occur when the CSM-S is handling connections using both Server/Application State Protocol (SASP) and Dynamic Feedback Protocol (DFP).

  Workaround: None.

- CSCsg94630

  An expired sticky entry may become active again when the sticky timer wraps around at 497 days.

  Workaround: Before 497 days, either reboot the CSM-S or clear the sticky table manually.

- CSCsh43381

  When the backup server farm is out of service, the partial serverfarm failover feature ignores failover threshold parameters.

  Workaround: None.

- CSCsh52256

  The CSM-S does not generate a syslog message if a virtual server dynamically goes out of service because all the real servers failed.

  Workaround: None.

- CSCsh83504

  The CSM-S may generate conflicting cookie hashes rather than unique values, leading to incorrect load balancing decisions by the CSM-S. When a cookie is long enough to cross a packet boundary, a partial hash is created. When the rest of the cookie is received, the rest of the hash is created, possibly taking input from the previous partial hash.

  Workaround: Remove cookie configuration, or use another type of sticky marker such as source IP address, or make sure cookies are short enough to not span packets.

- CSCsh90755

  The CSM-S may not insert a cookie if the real server sends a return code of 302 with a “Connection: close” header.

  Workaround: None.

- CSCsh96686

  The Server/Application State Protocol (SASP) task can become stuck in a loop. This situation can occur when communications are disrupted between the CSM-S and a SASP server.

  Workaround: None.

- CSCsh98223

  A CSM-S core dump can occur with the message, “FPGA4 exception 1 IDLE - idle.”

  Workaround: None.

- CSCsi35629

  No SNMP trap is sent when a real server returns to the operational state after a probe failure.

  Workaround: None.

- CSCsi36092

  When a TCP connection to the CSM-S is being established using a SYN cookie, the CSM-S can send IP fragments to a Layer 7 virtual server.

  Workaround: None.

- CSCsi36168

  Connections can fail when traffic is sent to a Layer 7 virtual server that has service termination configured.

  Workaround: Do not configure service termination to a Layer 7 virtual server.

Open Caveats in Software Release 2.1(6) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(6), see the “Resolved Caveats in Software Release 2.1(6) for SSL” section on page 48.

This section describes the open SSL caveats in CSM-S software release 2.1(6):

- Configuring NTP on the SSL-M or CSM-S SSL-DC may interfere with the clock synchronization. If the CSM-S SSL-DC is configured to synchronize its clock using NTP, the clock might go out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSL-M. The DC clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

- SSLM stops accepting new SSL connections because of a depletion of connection IDs on the TCP processor. Enter the **show ssl-proxy stats** command. The condition can occur when there is an approximately 65 KB difference between the conn alloc counters and dealloc counters under TCP. Eventually when all the connection IDs are exhausted, the SSLM will not be able to initiate any more connections to the backend servers.

  Workaround: Reload the module. (CSCek50983)

- The SSLM fails to pass the entire POST to a server when the header insert is configured in SSL proxy service. This occurred with a POST that had a large payload.

  Workaround: Remove the header insert configuration from the proxy service. (CSCse31785)

- When performing a URL rewrite, the location URL in a 302 redirect includes an 80. For example, http://192.168.45.10:80/. (CSCse92180)

- The location string for URL rewrites is being incorrectly rewritten in some cases. For example, a URL rewrite rule is given in the configuration for the URL, www.cisco.com, and the redirected location field contains the following string:

  http://user.microsoft.com/dir/test.jsp?login=https://www.cisco.com

  The location string is being incorrectly rewritten as follows:

  http://user.microsoft.com/dir/test.jsp?login=httpswww.cisco.com

  The rule is supposed to be rewritten if the host portion of the URL matches www.cisco.com. In the situation described here, that is not the case. No rewrite is supposed to occur. In addition, the rewrite should not affect the string https://www.cisco.com so far into the location field. (CSCsg65505)

- HTTP POST transactions fail when the total header size is exactly 1536 bytes and when the http-hdr insert policy is used. (CSCsh30757)

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows “No Server VLAN,” even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

Workaround: Specify the filename in the URL. (CSCea32058)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)
- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)
- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(6) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(6), see the "Open Caveats in Software Release 2.1(6) for SSL" section on page 45.

This section describes the SSL caveats resolved in CSM-S software release 2.1(6):

- No new resolved caveats.

Open Caveats in Software Release 2.1(5) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(5), see the "Resolved Caveats in Software Release 2.1(5) for CSM" section on page 49.

This section describes open caveats in CSM-S software release 2.1(5):

- CSCse93972

  Unless the virtual servers are configured for replication, after a failover from one CSM-S to another, the formerly active CSM-S will send idle resets for persistent flows that it hosted before the failover. If the virtual servers are configured for replication, the backup CSM-S will not send resets.

  Workaround: Configure the virtual servers for replication.

- CSCse91983

  The **show mod csm** *slot* **tech all** command may display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active and CSM-S traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsb56078 (duplicate of CSCei73146)

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

Resolved Caveats in Software Release 2.1(5) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(5), see the "Open Caveats in Software Release 2.1(8) for CSM" section on page 33.

This section describes resolved caveats in CSM-S software release 2.1(5):

- CSCse97201

  If you configure the CSM-S with two virtual servers, each with the same virtual IP address but with different subnet masks, the CSM-S will not redirect traffic to the other server when one of the servers is taken out of service. Changing the subnet masks to be identical will not solve the problem unless you also reboot the CSM-S.

  Workaround: None.

- CSCsg48830

  Outbound FTP connectivity will hang if the remote FTP server reuses the data port after sending a Transfer Complete response. A new environment variable allows the CSM-S to accommodate this server behavior. Configuration of the new environment variable is described in "New and Changed Information" section on page 12.

Workaround: None.

- CSCsg18828

  When you configure session cookies, the CSM-S includes the attribute **expires=** in the cookie string. This attribute should only appear for persistence cookies, which have a defined expiration date. A new session cookie string format is defined that deletes the attribute.

  Workaround: None.

- CSCej70864

  When a ping request is sent to the virtual server IP address, the CSM-S will sometimes attempt to reply to the ping rather than forwarding it. In these cases, the CSM-S will now drop the request rather than reply.

  Workaround: None.

- CSCse50544

  If cookie insertion is configured, the CSM-S behaves incorrectly when the HTTP server response arrives out of order (data first, then HTTP header in the last packet). In this case, the CSM-S inserts the cookie in the first packet received (the data packet) rather than in the HTTP header. As a resolution, the CSM-S will not insert a cookie when the server response is out of order.

  Workaround: Ensure that the HTTP server responses are always received in order.

- CSCsd97668

  When using a DNS probe that expects more than one IP address to be returned, the probe can fail if the DNS server does not return the second address.

  Workaround: Configure the probe to expect only one IP address, and configure the DNS server to return only one IP address.

- CSCsf11010

  When Global Site Selector (GSS) is configured to probe the virtual IP address with KAL-AP, the CSM-S will answer the probe, even though CAPP UDP is not configured.

  Workaround: Configure CAPP UDP on the CSM-S.

- CSCsg37187

  The CSM-S occasionally forgets to send ICMP echo, causing probe failure messages. This situation occurs when the probe parameters for **retries** or **failed** are configured for a value less than their default values.

  Workaround: Use default values for probe **retries** and **failed** parameters.

- CSCsg93384

  Under heavy backpressure from the Catalyst 6500 series switch backplane, the CSM-S's NAT processor can stop handling traffic until the backpressure subsides. In severe cases, a Layer 7 abort failure can occur in the NAT module.

  Workaround: None.

- CSCsd99863

  When performing Layer7 load balancing, the CSM-S will generate easily predictable TCP Initial Sequence Numbers (ISN), weakening security.

  Workaround: Use a firewall in front of the CSM-S.

- CSCek58878

  When using 2- or 3-tiered virtual server tracking, the dependent CSM-S virtual servers can remain outofservice after the tracked virtual server has recovered to operational status.

  Workaround: None.

- CSCsf99484

  A CSM-S core dump occurs that is related to the redirect process.

  Workaround: None.

- CSCsd52775

  When IP header insertion is used along with multiple Layer 7 policies in a persistent connection, the CSM-S sends an incorrect ACK number to finish the TCP handshake.

  Workaround: None.

- CSCsg51792

  A buffer leak can occur when fragmented TCP requests are sent to a virtual server configured for service termination. The resulting loss of buffers can lead to full system failure of load-balancing traffic.

  Workaround: Disable service termination on the virtual server, which will make it a Layer 4 virtual server only.

- CSCse45390

  When the virtual server is configured for service termination, the virtual server may not be listed when you enter the **show mod csm** *$slot* **conns vserver** *$nameOfVserver* command.

  Workaround: Enter the **show mod csm** *$slot* **conns detail** command to display the connections.

- CSCek39783

  If a route entry in the ARP table has the same MAC address as a learned ARP entry, the CSM-S will reset all connections associated with the route entry whenever the learned entry is updated with a new MAC address.

  Workaround: In the CSM-S configuration, add a static ARP entry for the learned ARP entry.

- CSCek50448

  During some conditions (for example, rate limiting), the CSM-S fails to increment the debug counter for packets dropped due to unknown MAC address. As a resolution, a new session statistics counter is added in this version to display the Packets with no SMAC, sent to slowpath message.

  Workaround: None.

- CSCse90720

  When hosting a Layer 7 virtual server, the CSM-S will answer a client's TCP handshake with an incorrect SYN/ACK sequence number, preventing the connection from establishing. This situation occurs under heavy load when the client resends the initial SYN packet.

  Workaround: None.

- CSCse98829

  In the webhost relocation line of a redirect-vserver configuration, when you use the %p extension to instruct the CSM-S to append the trailing URI, the URI may not be appended. This situation occurs when the HTTP GET request is smaller than 119 bytes. In response to the small GET request, the redirect is sent out, but the extension is not appended.

  Workaround: Use a larger GET request.

- CSCse93460

  When a server is hosting multiple IP addresses on a single MAC address, the CSM-S may not remap all flows to the server if the MAC address changes.

  Workaround: For UDP flows, clear the unmapped connections and allow them to reestablish.

- CSCsg40777

  Inbound traffic on a port of the supervisor engine does not reach the virtual IP address of the CSM-S if the supervisor engine is performing NAT on the virtual IP address.

  Workaround: Initialize register PI_PN_NONMOD_CRC_CFG_REG to a value of 0x40.

- CSCsg20504

  If the status-tracking feature is enabled, the CSM-S may stop executing **show** commands and displays the message %No ICC response for TLV. The traffic flow remains normal.

  Workaround: Do not enable the status-tracking feature.

- CSCsf16722

  If you configure the CSM-S with many virtual servers, the CSM-S may delay sending responses to KAL-AP queries from the Global Site Selector (GSS). If the response is too slow, the GSS times out and reports that the virtual server is offline.

  Workaround: Reduce the number of virtual servers on the CSM-S, or use TCP keepalives instead of KAL-AP keepalives.

- CSCsc25061

  When running TCP, if fragmented IP packets are processed on a server farm with the NAT server option enabled, the recalculated TCP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on the server farms that receive fragmented TCP packets.

- CSCek22782

  A configuration synchronization check for the active and standby CSM-Ss may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands, and then you change configurations only in the active or the standby CSM-S, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

  Resolved in Cisco IOS Release 12.2(18).

  Workaround: None.

Open Caveats in Software Release 2.1(5) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(5), see the "Resolved Caveats in Software Release 2.1(5) for SSL" section on page 55.

This section describes the open SSL caveats in CSM-S software release 2.1(5):

- Configuring NTP on the SSL-M or CSM-S SSL-DC may interfere with the clock synchronization. If the CSM-S SSL-DC is configured to synchronize its clock using NTP, the clock might go out of synchronization.

Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSL-M. The DC clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

- SSLM stops accepting new SSL connections because of a depletion of connection IDs on the TCP processor. Enter the **show ssl-proxy stats** command. The condition can occur when there is an approximately 65 KB difference between the conn alloc counters and dealloc counters under TCP. Eventually when all the connection IDs are exhausted, the SSLM will not be able to initiate any more connections to the backend servers.

  Workaround: Reload the module. (CSCek50983)

- The SSLM fails to pass the entire POST to a server when the header insert is configured in SSL proxy service. This occurred with a POST that had a large payload.

  Workaround: Remove the header insert configuration from the proxy service. (CSCse31785)

- When performing a URL rewrite, the location URL in a 302 redirect includes an 80. For example, http://192.168.45.10:80/. (CSCse92180)

- The location string for URL rewrites is being incorrectly rewritten in some cases. For example, a URL rewrite rule is given in the configuration for the URL, www.cisco.com, and the redirected location field contains the following string:

  http://user.microsoft.com/dir/test.jsp?login=https://www.cisco.com

  The location string is being incorrectly rewritten as follows:

  http://user.microsoft.com/dir/test.jsp?login=httpswww.cisco.com

  The rule is supposed to be rewritten if the host portion of the URL matches www.cisco.com. In the situation described here, that is not the case. No rewrite is supposed to occur. In addition, the rewrite should not affect the string https://www.cisco.com so far into the location field. (CSCsg65505)

- HTTP POST transactions fail when the total header size is exactly 1536 bytes and when the http-hdr insert policy is used. (CSCsh30757)

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows “No Server VLAN,” even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

```
Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
resetting...
```

The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)

- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)

- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(5) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(5), see the "Open Caveats in Software Release 2.1(5) for SSL" section on page 52.

This section describes the SSL caveats resolved in CSM-S software release 2.1(5):

- No new resolved caveats.

Open Caveats in Software Release 2.1(4) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(4), see the "Resolved Caveats in Software Release 2.1(4) for CSM" section on page 58.

This section describes open caveats in CSM-S software release 2.1(4):

- CSCsf16722

  If you configure the CSM-S with a large number of virtual servers, the CSM-S may delay sending responses to KAL-AP queries from the Global Site Selector (GSS). If the response is too slow, the GSS times out and reports that the virtual server is offline.

  Workaround: Reduce the number of virtual servers on the CSM-S, or use TCP keepalives instead of KAL-AP keepalives.

- CSCse91983

  The **show mod csm** *slot* **tech all** command may display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active and CSM-S traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slowpath messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCsc25061

  When running TCP, if fragmented IP packets are processed on a server farm with the NAT server option enabled, the recalculated TCP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on the server farms that receive fragmented TCP packets.

- CSCek22782

  A configuration synchronization check for the active and standby CSM-Ss may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands and then you change configurations only in the active or the standby CSM-S, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsc14905

  A CSM-S will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

```
vserver test
 virtual a.b.c.d  tcp 0 service termination
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
```

```
  backup real name SERVER-B
  inservice
real nameSERVER-B
  backup real name SERVER-A
  inservice
probe <NAME>
```

Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSM-Ss in a single fault-tolerant group and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group. This action causes the fault-tolerant pair of CSM-Ss to enter an invalid active-active state.

  Workaround: Remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM-S uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a "destination unreachable" message to the CSM-S if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 2.1(4) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(4), see the "Resolved Caveats in Software Release 2.1(5) for CSM" section on page 49.

This section describes resolved caveats in CSM-S software release 2.1(4):

- CSCsd43542

  CSM-S produces a core dump with the following core signature:

```
PPC exception type 1792 on 'Shakira dc probe(0BB46A60h)'
Registers:
 LR =004FF4A0h  PC =00000000h  SP =0BB468D8h
 R00=00000000h  R01=0BB468D8h  R02=00000000h  R03=0B768DC8h
 R04=0B768138h  R05=00000000h  R06=00000000h  R07=00660000h
 R08=0065C8CCh  R09=0000200Fh  R10=000013ACh  R11=00A0D984h
 R12=00000000h  R13=00000000h  R14=00000000h  R15=00000000h
 R16=00000000h  R17=00000000h  R18=00000000h  R19=00000000h
 R20=00000000h  R21=00000000h  R22=00000000h  R23=00000000h
 R24=0000003Ch  R25=0000E5ACh  R26=FFFFFFFFh  R27=00000001h
 R28=00000000h  R29=0B768138h  R30=00000000h  R31=0B768138
```

  This signature indicates a memory corruption in the health probe of the SSL daughtercard task.

  Workaround: None

- CSCse78674

  The CSM-S corrupts fragmented UDP packets on server-initiated traffic. The CSM-S fails to detect that the packet is fragmented and attempts to alter the UPD source port of the packet. This action overwrites the payload data in the fragmented packet and corrupts the packet. Fragmented packets are also corrupted on return flows, because the CSM-S overwrites the payload data by attempting to modify the UDP destination port.

  Workaround: None.

- CSCse98263

  When you configure multiple header sticky policies across more than one virtual server, some of the real servers ignore the header sticky policies. This problem applies only to header sticky policies (cookie sticky policies function correctly).

This caveat was introduced in release 4.2(4). Header sticky policies function correctly in earlier releases.

Workaround: If possible, use cookie sticky policies as an alternative to header sticky policies.

- CSCek49160

  When you use the Server/Application State Protocol (SASP) Global Workload Manager (GWM) test tool, the CSM-S may not register all of the member servers in the SASP group. This problem occurs when the connection between the CSM-S and the SASP GWM terminates in the middle of a session and returns to service after the CSM-S times out.

  This problem will cause the SASP test to fail and may cause the whole SASP test suite to fail.

  Workaround: After a connection failure, remove the SASP agent configuration and add it again to register all the real servers in the server farm.

- CSCek49892

  When a large number of active FTP sessions send messages simultaneously, the CSM-S may delay responding to PORT commands. If a client retransmits the PORT command, the CSM-S refuses to connect the client.

  Workaround: If possible, increase the client retransmit time.

- CSCek49909

  When a large number of passive FTP sessions are open, the CSM-S may delay responding to PASV messages. If a client retransmits the PASV message, the CSM-S responds with an error code that indicates that the port is not available. This scenario occurs only during initial creation of the data channel and does not affect data traffic.

  Workaround: Ensure that clients initiate a reattempt after receiving the error code. Reattempts connect successfully, because the port number in the reattempt is different from the original request.

- CSCek51235

  When failed probes are added to a server farm used in a dependent vserver, the CSM-S may fail and produce a core dump. The syslog header indicates a HealthMon exception.

  Workaround: None.

- CSCsf21551

  When a server responds to an HTTP probe with an OK message and then sends an RST to close the TCP connection, the CSM-S places the server in a failed state.

  Workaround: Prevent the real server from sending RSTs after OK messages.

Open Caveats in Software Release 2.1(4) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(4), see the "Resolved Caveats in Software Release 2.1(4) for SSL" section on page 61.

This section describes the open SSL caveats in CSM-S software release 2.1(4):

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.
  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.
  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)
- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)
- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)
- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)
- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)
- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(4) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(4), see the "Open Caveats in Software Release 2.1(4) for SSL" section on page 59.

This section describes the SSL caveats resolved in CSM-S software release 2.1(4):

- The Content Switching Module with SSL might reboot every 2 to 6 hours when you configure URL rewrite with the default ports (port 80 for cleartext and port 443 for SSL).

  Workaround: Disable URL rewrite.

  This problem is resolved in SSL software release 2.1(9). (CSCsd25820)

- If the Content Switching Module with SSL receives a misaligned TCP selective acknowledgment (SACK) option or a misaligned TCP timestamp option, the module might reload.

  This problem is resolved in SSL software release 2.1(9). (CSCee35357)

Open Caveats in Software Release 2.1(3) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(3), see the "Resolved Caveats in Software Release 2.1(3) for CSM" section on page 64.

This section describes known CSM limitations that exist in CSM-S software release 2.1(3).

- CSCej58455

  A configuration synchronization check for the active and standby CSM-Ss may fail for configurations with the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When using these subcommands, changing configurations only in the active or the standby CSM-S may display the wrong configuration synchronization state. The module may show synchronized configurations as out-of-synchronization, and out of synchronization configurations as in-synchronization.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsc14905

  A CSM-S will not respond to pings to the virtual server when it is configured with service termination. The server is operational and passing TCP flows to the real servers, which are also operational. This example shows the configuration:

```
vserver test
 virtual a.b.c.d  tcp 0 service termination
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server reached through a virtual server that is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
```

```
   backup real name SERVER-A
   inservice
probe <NAME>
```

Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSM-Ss in a single fault-tolerant group and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group, causing the fault-tolerant pair of CSM-Ss to enter an invalid active-active state.

  Workaround: Remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM-S uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example, host-unreachable), that causes the function to not return an error. The function remains in a wait loop until it receives a valid response.

If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a "destination unreachable" message to the CSM-S if the router determined that the subnet for this IP address is unknown.

Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 2.1(3) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(3), see the "Open Caveats in Software Release 2.1(3) for CSM" section on page 62.

This section describes the CSM caveats resolved in CSM-S software release 2.1(3).

- CSCsd93350

  The CSM-S daughter card reboots when configured in a bridged-mode with no NAT server, while under load. Disabling keepalives does stop the reboots but the SSL daughter card still locks up as all communication buffers are depleted.

  Workaround: None

- CSCsd80681

  During a configuration synchronization between the active CSM-S and the standby CSM-S, the supervisor engine might reload either the active or standby CSM-S due to missing keepalives. This action might be related to the number of connections actively getting replicated at the time of the configuration synchronization.

- CSCej80407

  When moderate health-probe traffic is used with the status tracking feature enabled, the CSM-S might display a "% No ICC response for TLV type XX from CSM linecard" error message when entering commands. You can session into the system and traffic continues to pass.

  Workaround: Do not use the status-tracking feature.

- CSCsc18987

  If there are two CSM-Ss running in fault tolerant mode with preempt enabled, and they each have the same priority, the modules will continuously change their roles (flip-flop) between active and standby. The CSM-Ss must have the same priority and must be running with preempt for this situation to occur.

  Workaround: Do not configure two CSM-Ss running in fault tolerant mode with preempt and the same priority configured. If the role-changing (flip-flop) behavior occurs, then you must immediately turn off preempt or give one of the CSM-Ss either a higher or lower priority.

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. The problem does not occur for TCP connections. It affects all CSM-S software releases.

  Workaround: None.

- CSCsb59273

  The CSM-S uses its own MSS when using sticky cookie insert. The CSM-S does not consider the client-sent MSS (from the client SYN signal) but uses its own MSS (the one sent in CSM-Ss SYN-ACK signal) to determine how the server response may increase when inserting a cookie.

  In the client, the CSM-S paths with an effective MSS (due to lower processor maximum transmission unit [PMTU] that is lower than the CSM-Ss MSS causes the server response to be dropped. When the server response is dropped, the client never receives the first segment of the server response.

  Workaround: Manually lower the CSM-S MSS with the **variable TCP_MSS_OPTION** *new_value* command. You may also use a TCP MSS adjustment on a device (such as Cisco PIX Firewall) between the CSM-S and the lower MTU boundary (such as the start of a tunnel).

Open Caveats in Software Release 2.1(3) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(3), see the "Resolved Caveats in Software Release 2.1(3) for SSL" section on page 67.

This section describes the open SSL caveats in CSM-S software release 2.1(3):

- If you delete the route to the real server from the SSL proxy VLAN, and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCee46096)

- The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed, and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module. (CSCin67360)

- When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment. (CSCee69321)

- On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module. (CSCec69592)

- If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string. (CSCec46997)

- Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the **crypto ca trustpoint** *trustpoint_label* and **crypto ca certificate chain** *name* command information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration. (CSCec19596)

- If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem. (CSCec82360)

- The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment. (CSCec74017)

- When you import a certificate from a PKCS12 or PEM file, or when you manually input a certificate authority certificate to the module and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)
- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM. (CSCdz03802)
- Syslog messages indicating that proxy services are in the up state may not be printed for all services configured in the system while booting. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module. (CSCee37656)

Resolved Caveats in Software Release 2.1(3) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(3), see the "Open Caveats in Software Release 2.1(3) for SSL" section on page 65.

This section describes the SSL caveats resolved in CSM-S software release 2.1(3):

- The Content Switching Module with SSL might reboot every 2 to 6 hours when you configure URL rewrite with the default ports (port 80 for cleartext and port 443 for SSL).

  Workaround: Disable URL rewrite.

  This problem is resolved in SSL software release 2.1(9). (CSCsd25820)
- If the Content Switching Module with SSL receives a misaligned TCP selective acknowledgment (SACK) option or a misaligned TCP timestamp option, the module might reload.

  This problem is resolved in SSL software release 2.1(9). (CSCee35357)

Open Caveats in Software Release 2.1(2a) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(2a), see the "Resolved Caveats in Software Release 2.1(2a) for CSM" section on page 70.

This section describes known CSM limitations that exist in CSM-S software release 2.1(2a).

- CSCsd80681

  During a configuration synchronization between the active CSM-S and the standby CSM-S, the supervisor engine might reload either the active or standby CSM-S due to missing keepalives. This action might be related to the number of connections actively getting replicated at the time of the configuration synchronization.

- CSCej80407

  When moderate health-probe traffic is used with the status tracking feature enabled, the CSM-S might display a "% No ICC response for TLV type XX from CSM linecard" error message when entering commands. You can session into the system and traffic continues to pass.

  Workaround: Do not use the status-tracking feature.

- CSCej58455

  A configuration synchronization check for the active and standby CSM-Ss may fail for configurations with the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When using these subcommands, changing configurations only in the active or the standby CSM-S may display the wrong configuration synchronization state. The module may show synchronized configurations as out-of-synchronization, and out of synchronization configurations as in-synchronization.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsc18987

  If there are two CSM-Ss running in fault tolerant mode with preempt enabled, and they each have the same priority, the modules will continuously change their roles (flip-flop) between active and standby. The CSM-Ss must have the same priority and must be running with preempt for this situation to occur.

  Workaround: Do not configure two CSM-Ss running in fault tolerant mode with preempt and the same priority configured. If the role-changing (flip-flop) behavior occurs, then you must immediately turn off preempt or give one of the CSM-Ss either a higher or lower priority.

- CSCsc14905

  A CSM-S will not respond to pings to the virtual server when it is configured with service termination. The server is operational and passing TCP flows to the real servers, which are also operational. This example shows the configuration:

```
vserver test
 virtual a.b.c.d  tcp 0 service termination
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server reached through a virtual server that is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
   backup real name SERVER-A
   inservice
 probe <NAME>
```

Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. The problem does not occur for TCP connections. It affects all CSM-S software releases.

  Workaround: None.

- CSCsb59273

  The CSM-S uses its own MSS when using sticky cookie insert. The CSM-S does not consider the client-sent MSS (from the client SYN signal) but uses its own MSS (the one sent in CSM-Ss SYN-ACK signal) to determine how the server response may increase when inserting a cookie.

  In the client, the CSM-S paths with an effective MSS (due to lower processor maximum transmission unit [PMTU] that is lower than the CSM-Ss MSS causes the server response to be dropped. When the server response is dropped, the client never receives the first segment of the server response.

  Workaround: Manually lower the CSM-S MSS with the **variable TCP_MSS_OPTION** *new_value* command. You may also use a TCP MSS adjustment on a device (such as Cisco PIX Firewall) between the CSM-S and the lower MTU boundary (such as the start of a tunnel).

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Fragmentation counter in the CSM-S increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM-S so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.

Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSM-Ss in a single fault-tolerant group and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group, causing the fault-tolerant pair of CSM-Ss to enter an invalid active-active state.

  Workaround: Remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM-S uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example, host-unreachable), that causes the function to not return an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a “destination unreachable” message to the CSM-S if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 2.1(2a) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(2a), see the “Open Caveats in Software Release 2.1(2a) for CSM” section on page 67.

This section describes the CSM caveats resolved in CSM-S software release 2.1(2a).

- CSCeh61946

  When the CSM-S receives KAL-AP probes from a GSS, the CSM-S loses memory, which results in slowing of commands and eventual lockup of the CSM-S.

  Workaround 1: Do not send GSS KAL-AP keepalives to the CSM-S,

  Workaround 2: When the available memory of the CSM-S falls below 40 percent, reload the CSM-S.

- CSCdy30354

  If heavy cookie-insert traffic is used, the core routine might reboot the system before a core is generated. This action results in a supervisor engine reload without core.

- CSCsd54286

  A cookie insert applied to a jumbo frame causes the module to fail. If the packet is resolved in the Layer 7 module and has four distinct segments to transmit during cookie insert, the Layer 7 module must send two transmit commands. The failure occurs when the second command does not advance the tail pointer in the command queue, causing a repeat of the second partially transmitted command. The invalid transmission may be caught as an illegal header. Sometimes the transmitted command will transmit a faulty packet, also causing a failure. This situation occurs when a packet larger than the configured MSS is received.

- CSCsd58615

  Sending a multi-packet POST to a cookie insert virtual server can cause misclassified packets. When a session becomes invalid, the TCP module attempts to transmit the buffers stored at Layer 7. When those packets are sent from the Layer 7 insert they must be treated differently than packets from other layers. Also, some data packets are processed in Layer 4 and then switched to Layer 7 processing. When this layer switching occurs, data packets are counted twice, once as Layer 4 packets and once as Layer 7 packets.

  Workaround: None.

- CSCsd27478

  The CSM-S might reload with an FPG4 exception in icp.fatPath length error (icpFatErr). This condition occurs when overlapping TCP segments are sent to the CSM-S out of order.

- CSCsc56986

  CSM-S header or cookie insert causes a TCP checksum error when the CSM-S operates under a heavy load (> 1000 conn/sec).The CSM-S may incorrectly set the TCP checksum, causing delays due to retransmission of the packets. This checksum error appears on both the client side and the server side.

  This situation occurs only with a virtual server using a cookie insert sticky group or a header insert function.

  Workaround: None.

- CSCsd27970

  The CSM-S drops HTTP GETs to a server on the back end of the Layer 7 connection.

  Workaround: None.

- CSCek03020

  When sending an incorrect message length from a simulated Server/Application State Protocol (SASP) global workload manager (GWM), the CSM-S logs the following system messages and reboots:

  ```
  %CSM_SLB-3-UNEXPECTED: Module 9 unexpected error: SASP: connected to GWM ac1f6529:5555
  ```

```
%C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not responding to
Keep Alive polling)
%DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimum Diagnostics...
%DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
%OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
```

Workaround: None.

- CSCsc77672

  Running a load test that sends traffic to a single virtual server with cookie sticky configured causes the IXP1 engine to get stuck after a few minutes of operation. The IXP1 engine shows a CPU utilization that exceeds 100%. The ARP table is empty and traffic stops.

  Workaround: None.

- CSCsc53146

  When a virtual server is configured for UDP service per-packet, UDP packets are dropped when performing per packet load balancing. A CSM-S module can drop UDP packets and display them in the "packets dropped" column when you enter the show module c mod number tech-support processor 2 command.

  Workaround: Remove the "service per-packet" option from the virtual address configuration in the virtual server.

- CSCsb59273

  The CSM-S uses its own MSS when using sticky cookie insert. The CSM-S does not consider the client-sent MSS (from the client SYN signal) but uses its own MSS (the one sent in CSM-Ss SYN-ACK signal) to determine how the server response may increase when inserting a cookie.

  In the client, the CSM-S paths with an effective MSS (due to lower processor maximum transmission unit PMTU) that is lower than the CSM-Ss MSS causes the server response to be dropped. When the server response is dropped, the client never receives the first segment of the server response.

  Workaround: Manually lower the CSM-Ss MSS with the variable TCP_MSS_OPTION new value command. You may also use a TCP MSS adjustment on a device (such as Cisco PIX Firewall) between the CSM-S and the lower MTU boundary (such as the start of a tunnel).

Open Caveats in Software Release 2.1(2a) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(2a), see the "Resolved Caveats in Software Release 2.1(2a) for SSL" section on page 75.

This section describes known SSL limitations that exist in CSM-S software release 2.1(2a).

- CSCin67360

  The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module.

- CSCee69321

  When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment.

- CSCee46096

  If you delete the route to the real server from the SSL proxy VLAN and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module.

- CSCee37656

  On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module.

- CSCed14070

  When you import a certificate from a PKCS12 or PEM file or when you manually input a certificate authority certificate to the module, and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module.

- CSCec82360

  If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all the SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem.

- CSCec74017

  The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment.

  Workaround: None.

- CSCec69592

  On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module.

- CSCec46997

  If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string.

- CSCec19596

  Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the "crypto ca trustpoint *trustpoint_label*" and "crypto ca certificate chain *name*" information from the running configuration.

  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.

  c. Paste the trustpoint and certificate chain information to the configuration.

- CSCea71882

  The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate.

- CSCea50887

  There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command.

  Workaround: None.

- CSCea32058

  For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL.

- CSCdz24446

  Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available.

- CSCdz03802

  When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM.

- CSCdy85233

  Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host.

  Workaround: None.

- CSCdy72229

  Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module.

  Workaround: None.

- CSCdy61618

  Syslog messages indicating that proxy services are in the up state may not be printed for all the services configured in the system while booting.

  Workaround: None.

- CSCdy46075

  When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates.

  Workaround: None.

Resolved Caveats in Software Release 2.1(2a) for SSL

Note For a description of open SSL caveats in CSM-S software release 2.1(2a), see the "Open Caveats in Software Release 2.1(2a) for SSL" section on page 72.

This section describes the SSL caveats resolved in CSM-S software release 2.1(2a).

- CSCej75255

  Added content, URL statistics to crash information, regular statistics.

  Workaround: None.

- CSCej38531

  When you add HTTP header insert policies to an SSL proxy service, the Content Switching Module with SSL might reset repeatedly and generate core dumps. This behavior occurs when a large number of end-of-http-headers are lost.

  Workaround: Do not apply policies performing header insertion to ssl-proxy-services.

  This problem is resolved in SSL software release 2.1(8).

- CSCsc26099

  When you configure a client proxy, the Content Switching Module with SSL resets when the backend SSL server does not allow session resumption and returns an empty session ID.

  Workaround: Enable session resumption on the backend SSL server.

  This problem is resolved in SSL software release 2.1(8).

- CSCsc13184

  A configuration option is required to disable the TCP Nagle algorithm.

  Workaround: An extra CLI option, the **no nagle** command, has been added to the software.

- CSCsb77689

If you configure the Content Switching Module with SSL with header insertion, and if the total size of the server cookie, the client request, and the inserted header exceeds the size of the first buffer (1460 bytes) on the Content Switching Module with SSL, the buffer overflows and the Content Switching Module with SSL resets.

Workaround: None.

This problem is resolved in SSL software release 2.1(8).

- CSCej33386

  When you configure URL rewrite, the Content Switching Module with SSL scans the response from the server. Currently, the entire response (headers and data) is scanned, which leads to a drop in performance.

  Workaround: None.

  This problem is resolved in SSL software release 2.1(8).

Open Caveats in Software Release 2.1(2) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(2), see the "Resolved Caveats in Software Release 2.1(2) for CSM" section on page 82.

This section describes known CSM limitations that exist in CSM-S software release 2.1(2).

- CSCej58455

  A configuration synchronization check for the active and standby CSM-Ss may fail for configurations with the following subcommands: script, ARP, variable, match, failaction, NAT client, probe, domain, or url hash. When using these subcommands, changing configurations only in the active or the standby CSM-S may display the wrong configuration synchronization state. The module may show synchronized configurations as out-of-sync, and out of sync configurations as in-sync

  Workaround: For configurations including the subcommands script, ARP variable, match, failaction, NAT client, probe, domain, and url-hash subcommands you must manually ensure that the configuration commands and subcommands are synchronized at both the active and standby modules.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM-S were not the same as the counters on the active CSM-S. The active CSM-S correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM-S, all replicated connections are assigned to a single real server within a server farm.

  Workaround: None.

- CSCsc18987

  If there are two CSM-Ss running in fault tolerant mode with preempt enabled and they each have the same priority the modules will continuously change their roles (flip-flop) between active and standby. The CSM-Ss must have the same priority and both must be running with preempt for this situation to occur.

  Workaround: Do not configure two CSM-Ss running in fault tolerant mode with preempt and the same priority configured. If the role changing (flip-flop) behavior occurs then you must immediately turn off preempt or give one of the CSM-Ss either a higher or lower priority.

- CSCsc14905

  A CSM-S will not respond to pings to the virtual server when it is configured with service termination. The server is operational and passing TCP flows to the real servers, which are also operational. This example shows the configuration:

```
vserver test
 virtual a.b.c.d  tcp 0 service termination
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server reached through a virtual server that is configured with predictor forward the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassigned. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
   backup real name SERVER-A
   inservice
 probe <NAME>
```

  Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. The problem does not occur for TCP connections. It affects all CSM-S software releases.

  Workaround: None.

- CSCsb59273

  If the total of (real server response segment size) + (size of inserted cookie) exceeds the CSM-S MSS value of 1460, the CSM-S splits the result in multiple segments, with a maximum of the CSM-S MSS value.

  Workaround: Manually lower the CSM-S MSS with the **variable TCP_MSS_OPTION** *new value* command.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM-S. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCsa88370

  Due to an ARP failure, a real server that is not directly connected to the CSM-S may become unreachable after a gateway failure occurs, even though there is still a valid gateway or route available.

  This situation occurs when there is more than one route (gateway) configured to reach the real server and the route chosen by the CSM-S becomes unavailable.

  Workaround: Remove the failed gateway from the configuration.

- CSCeh78584

  When you configure an alias IP address on a server VLAN on the CSM-S, you are incorrectly allowed to configure a network address for the alias.

  Workaround: None.

- CSCeh76411

  When you configure **service ftp** on a virtual server and then configure a client NAT pool for that virtual server, the FTP virtual server allocates ports from the NAT pool and does not reclaim them.

  Workaround: Reboot the CSM-S to recover the allocated ports.

- CSCeh60960

  With the ROUTE_UNKNOWN_FLOW_PKTS environmental variable set to either **1** or **2**, ICMP or UDP packets cannot directly access servers behind the CSM-S when the CSM-S is in router mode.

  You can still Telnet to these servers when this environmental variable is set to 2.

- CSCeh60704

  The sticky table does not replicate after a configuration synchronization. This situation occurs when traffic is sent to an SSL virtual server that is configured with the **csrp sticky** (SSL session) and **csrp connection**. Initially, the connection works, but if traffic is stopped and a configuration synchronization operation is performed several times when the traffic is started again, only the connections replicate. Reloading the standby CSM-S does not correct the problem.

  Workaround: Reload the active CSM-S.

- CSCeh41862

  When you configure gateway tracking, if the host or gateway is more than 1 hop away, the CSM-S goes into standby state, even if the CSM-S can ping the host.

- CSCeh34176

  The **show module csm** *slot* **stats** command displays the incorrect value for the **Connections Timed-Out** counter.

  Workaround: Enter the **show module csm** *slot* **tech-support proc 1** to display the correct value.

- CSCeg77526

  After you enter the **script file bootflash:myscript.txt** command to load a script file into the CSM-S, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM-S. When you enter the **no script file bootflash:myscript.txt** command to remove the script file configuration, the **show** command for the script continues to display the same list of script functions.

  This situation occurs because the individual script was loaded into the CSM-S by using the **script file** command, which loads the script into memory. The CSM-S does not have a command that allows you to request a reload of the same script file to update the individual script.

  Do the following to reload the script with the same filename (but with newer content):

a. Remove the script with the **no script file bootflash:myscript.txt** command. This command does not destroy nor stop the current probes that are using the existing scripts.

b. Then, enter the **script file bootflash:myscript.txt** command to reload the new content. The probes will pick up the new script in the next interval of operation.

Workaround: None. This is the current design for reloading a script. The scripts must remain in memory for the probes to operate. If you want to stop the probes from using those scripts, you must remove the probes. Scripts removed from the CSM-S remain in memory.

- CSCeg35110

  When you configure more than one virtual server with an IP address that is being used by a DNS server farm (GSLB feature), the health probe for the real server within this server farm might show as failed. This situation is caused by the probe checking the status of one virtual server instead of checking the status of all virtual servers with this IP address.

  Workaround: Remove those virtual servers which are out-of-service.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Frag counter in the CSM-S increases quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM-S so that it knows where to send reassembled fragments that arrived in a reverse order.

- CSCef76686

  When you configure a server farm with the least-connections algorithm by entering the **predictor leastconns** command and enable the REAL_SLOW_START_ENABLE environment variable with the default rate (3), the slow-start feature might not take effect for newly activated servers in the server farm.

  Workaround: Configure the REAL_SLOW_START_ENABLE environment variable to 2.

- CSCef02629

  During a supervisor engine switch over, the standby CSM-S fails to initialize, and the new standby supervisor engine prints the following message for all CSM-S ports:

  ```
  %PM-STDBY-4-INT_FAILUP:GigabitEthernet7/2 failed to come up.No internal VLAN available
  ```

  Workaround: None.

- CSCee57427

  Starting with software Release 12.2(18)SXD, the CSM-S needed to have identifiers assigned in the MIBs, as shown in this example:

  ```
  CISCO-ENTITY-VENDORTYPE-OID-MIB.my & OLD-CISCO-CHASSIS-MIB.my
  ```

  This situation causes incorrect values to show up through SNMP. New identifier assignments have been made in the MIBs and are available in the 12.2(18)SXD release, as shown in this example:

  ```
  CISCO-ENTITY-VENDORTYPE-OID-MIB.my:
  csm-ssl(442) --  CSM-S is a content switching module with integrated SSL acceleration
  ```

```
OLD-CISCO-CHASSIS-MIB.my:
cevChassisCSMSsl  OBJECT IDENTIFIER ::= { cevChassis 479 }
--  CSM-S is a content switching module with integrated SSL acceleration
```

Workaround: None.

- CSCee33514

  When the module starts up, you may see messages on the CSM-S console, as follows:

```
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Subcommand: COMMAND_MODULE_ONLINE
Module has become online.

SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
```

  Workaround: None. There is no operational impact that results from these messages. They can be safely ignored.

- CSCee26687

  CSM-S does not allow static ARP for the SSL daughter card interface.

  Workaround: None.

- CSCee18203

  Multiple syslog messages may appear under heavy certificate authenticated SSL traffic and the SSL Cisco IOS console may become unresponsive. The heavy traffic is for an SSL proxy-service that has certificate authentication turned on. For example:

```
ssl-proxy(config-ssl-proxy)# authenticate verify { signature-only | all }
```

  The more traffic, the more unresponsive the console becomes. At very high traffic loads the following syslog may appear:

```
*Apr 1 22:39:13.071: %SCHED-3-THRASHING: Process thrashing on
watched boolean 'CSM IOS Watch Bool'.
-Process= "CSM IOS I/O Process", ipl= 5, pid= 27
-Traceback= 5233E8 5234CC 5C6044
```

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the static NAT client into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.

- CSCec21915

  The possible number of VLANs has increased to 511. This limit is the total number of IP interfaces and alias IP interfaces that can be configured on the CSM-S. If you need to configure alias IP addresses, you need to reduce the number of VLAN IP interfaces.

Workaround: Reduce the number of configured VLANs to accommodate the total number of alias IP addresses.

- CSCeb52054

  When the Layer 7 virtual servers have many connections that are in the process of load balancing, the new and existing connections receive a slow response from the CSM-S. The connections, which are still waiting for more data from the client or which are waiting for the response from the server, are considered to be in the process of load balancing.

  Workaround: Configure the max-conns option on the servers for slow response servers, or lower the number for the max-parselen option to reduce the unnecessary wait for invalid HTTP connections.

- CSCeb47499

  The UDP probe configured for a server farm can only detect a failure of a UDP service when the connectivity to the server IP address is opened. The CSM-S relies on the ICMP port unreachable message from the server so that it can detect whether the UDP service is available. If the interface on the server is down, the UDP probe cannot detect this failure condition.

  Workaround: Configure an ICMP probe to the same server farm where the UDP probe is configured.

- CSCea43504

  If your configuration contains a pair of CSM-Ss in a single fault-tolerant group and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group, causing the fault-tolerant pair of CSM-Ss to enter an invalid active-active state.

  Workaround: Remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example host-unreachable), the function does not return with an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a “destination unreachable” message to the CSM-S if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

- CSCdw84018

  The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM-S uses to parse the RSTP service. For this same virtual server, you must also configure a NAT client on the server farm.

  Workaround: Remove the NAT client configuration from the server farm, or remove the service RTSP from the virtual server.

- CSCdv11685

When more than one pair of redundant CSM-Ss are configured to use the same VLAN ID, the CSM-S will accept replication messages from all fault-tolerant groups by using the specified VLAN. In this configuration, the session and sticky replication may not work properly.

Workaround: Configure a unique VLAN trunk for each pair of fault-tolerant groups.

Resolved Caveats in Software Release 2.1(2) for CSM

Note For a description of open CSM caveats in CSM-S software release 2.1(2), see the "Open Caveats in Software Release 2.1(2) for CSM" section on page 76.

This section describes the CSM caveats resolved in CSM-S software release 2.1(2).

- CSCsb71260

  When you configure the cookie insert feature with other map policies under a virtual server, the CSM-S re-inserts a new cookie for each new TCP connection, even if a cookie was inserted previously. The CSM-S re-inserts new cookies when the existing map policies do not have a match, and cookie insert is the default policy.

  Workaround: None

- CSCsb64954

  When configuring the CSM-S with a virtual server using the **service rtsp** command, the MP4 files streaming through the CSM-S may have poor video or audio quality. The data sequence mismatch counter under the TCP statistics section of the **show tech** command will also increment.

  Workaround: Do not use the **service rtsp** command.

- CSCsb46265

  When changing a VLAN IP address, an ARP timeout can be triggered. When this situation occurs, the encapsulated identification table is refreshed and each MAC address in the table may be assigned a new encapsulated identification. This problem occurs because the CSM-S is not updated with the new encapsulated identification. The CSM-S continues using the previous encapsulated identification, which results in traffic being forwarded to the wrong destination.

  Workaround: Configure static ARP entries for the CSM-S gateways.

- CSCsb40988

  After reaching the maximum number of connections, the sticky timer may not start for new traffic flows. This situation occurs with the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command configured on a CSM-S and with the **maxconns** command configured on the real server. The sticky timer also does not start when connections are deleted.

  Workaround: Removing the maximum connections configuration.

- CSCsb17046

  When an associated virtual server goes out of service and then returns to in service, the CSM-S does not use a real server if the traffic load threshold is configured above 254. This situation occurs because the traffic load of a local GSLB real server becomes stuck at a threshold of 255, preventing the CSM-S to use this real server when answering a DNS request.

  Workaround: None.

- CSCsb08993

  On a CSM-S configured with the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command, the sticky timeout counter remains 0 regardless of when the idle timer expires. This situation occurs only after changing the configuration with the **sticky group** command when traffic flows are active.

  Workaround: Do not modify the sticky group configuration when there are active traffic flows.

- CSCsb02873

  Two columns display incorrect values for the total pending counter that is received when using the **show module csm X tech probe** command.

  In the display, the left column is supposed to show the total number of probe attempts, and the right column is supposed to show the difference between the current value and the last time you entered the **show** command.

  Workaround: None.

- CSCsa88370

  When more than one route or gateway is configured to connect to a remotely located real server, the remote real server might experience an ARP failure and become unreachable after one of the gateways fails. This situation occurs although a valid gateway or route may still be available.

  Workaround: Use the s**how mod csm** *slot* **arp** command to locate the unavailable gateway, and remove that gateway from the configuration.

- CSCsa74493

  If you create a serverfarm and a cookie insert sticky group, and a policy to associate both, the CSM-S generates a static cookie entry that is displayed with the **show mod csm** *slot* **sticky** command.

  If you add a new real to the serverfarm, the cookie information is not updated.

  Workaround: Remove the policy and reconfigure it.

- CSCej08044

  Interface device tracking fails when a preempt is configured. The active CSM-S changes its state to standby when the interface and gateway are shut down. When the interface and gateway are returned to operation, the CSM-S state does not return to active as it should.

  Workaround: None.

- CSCei94412

  When the CSM-S is in bridge mode with HSRP configured on the client VALN and the server's default gateway is pointing to that HSRP address, flooding may occur when the HSRP virtual MAC address is aged out from the switches CAM tables (default 5 minutes of inactivity).

  Workaround:

  - Increase the mac-address-table aging timer in the server VLANs
  - Use the **standby use-bia** command.

- CSCei91610

  The CSM-S is not passing ACK or RST requests to real servers.

  Workaround: None.

- CSCei91452

  The FTP data channel crashes 15 minutes into the data transfer as a result of the CSM-S calculation for timestamps. During non-FTP operation, the data plane monitors flows and times out connections. For FTP however, the PPC must monitor the FTP connections and their timestamps.

The session IXP must provide the last time that the flow contained traffic. The PPC will query the session process for the last time (in ticks) that the flow contained traffic and performs a ticks to seconds conversion, multiplying ticks times (134/166) to calculate real seconds.

The conversion function assumes that the maximum possible for the ticks return value was 0x00ffffff. If the number of ticks returned was greater than 0x00ffffff, the conversion function returns a -1. Because the actual maximum return value from session is 0x0fffffff but the timestamp that was calculated was greater than 0x00ffffff, the session is flagged for a timeout, because the conversion was in error and had returned a -1.

Note This problem occurs after the CSM-S has been in operation for (0x00ffffff)*(134/166) seconds, or about 156 days. Also, the FTP data channel is timed out only after 15 minutes, so shorter transfers are unaffected.

Workaround: A work around exists that should be performed at the specific direction of TAC or other Cisco Personnel. This caveat manifests itself after the CSM-S has been up for over 156 days, so please contact TAC if you feel that this bug is affecting you.

- CSCei58018

  When a reset is sent to the CSM-S and merged out of order, packet handling is configured, and the sequence number is set to acknowledge the first packet but not the last packet sent.

  Workaround: None.

- CSCei38917

  The CSM-S is dropping Layer 3 fragmented IP packets on traffic flows destined for a virtual server. This situation occurs in a basic server load balancing (SLB) design that connects to an all zero's virtual server (0.0.0.0/0) with no NAT client and a non NAT server configured on the server farm. The traffic flows are set up properly and fail when packets in both directions are dropped or incorrectly routed to the gateway.

  Workaround: Downgrade to a CSM-S software release earlier than software release 2.1(x).

- CSCei37874

  A server does not enter slow start mode when sending traffic at a slow pace of 1cps with the variable REAL_SLOW_START_ENABLE set to 1. This situation occurs when an IP address on an ICMP probe is configured on a real server and is then activated. The probe receives all of the new connections until it is again load balanced with the other servers. However, the slow start configured server does not appear to be in the slow start mode.

  Workaround: None.

- CSCei35703

  The unsuccessful load-balancing decision message does not display in TCP when the process reaches the maximum parse length value that was configured.

  Workaround: None.

- CSCei34913

  A CSM-S drops the out-of-order TCP segments when load balancing at Layer 7 and is waiting for the client to retransmit the segments. TCP segments must be in order, or they are dropped

  Workaround: None.

- CSCei34381, CSCdy00154

  When testing redundancy failovers, the assumed priority value does not change on the active CSM-S. The priorities are the same between the CSM-S with no preempt configured. Under these conditions, the higher MAC address takes the active role when there is an active CSM-S to active CSM-S situation. The last active CSM-S remains active which is the correct behavior with CSCdy00154.

  Workaround: None.

- CSCei28436

  A TCP segment may be corrupted on the CSM-S during an FTP control session, causing the control session to lose synchronization between the client and the CSM-S. This problem causes the FTP session to fail, usually when file transfers passing several hundreds of files are performed with the same FTP control connection.

  Workaround: None.

- CSCei26434

  In some cases, the CSM-S load-balances to just one real server instead of all operational real servers in a server farm when using predictor least-connections. The conditions which cause this error are:

  a. The real server fails the health probe check to this server farm when the health probe is activated by one of the following:
     - The predictor was changed from other to least-connections
     - The CSM-S was first rebooted.
     - The CSM-S became fault-tolerant (FT) active for the first time.
  b. After traffic goes through this server farm, other servers were selected.
  c. This real server was re-enabled after passing the health probe check and all new connection requests are load-balanced only to this real server.

  Workaround: Use another predictor method, set this server to out-of-service, and then set the server back to in service after it passes the health check.

- CSCei16475

  If a real server crashes, the sticky timer remains disabled. This symptom occurs when you configure the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command on the CSM-S.

  Workaround: Disable the variable command.

- CSCeh76411

  When using the CSM-S NAT pool feature with an FTP virtual server you can allocate ports from the NAT pool and never reclaim those ports. The problem reproduces when a client attempts to re-use an FTP data connection that was used previously in the same session.

  The number of available ports diminish in this configuration if you configure service FTP on a virtual server or you configure client NAT pool for that virtual server.

  The FTP client re-uses the same port when opening the FTP data connections for this same FTP control connection.

  Workaround: Reboot the CSM-S to recover the allocated ports.

- CSCeh73953

  If you add several policies to a virtual server and configure the priority option using the **slb-policy** *policy-name* **priority** *priority_value* command and then remove a policy that is not configured with the highest priority, the CSM-S might reload.

This problem does not exist for policies that are not configured with the **priority** option.

Workaround: Remove only the policy with the highest priority in the list.

- CSCeh64012

  In rare instances due to a message timing problem, when the supervisor engine performs an RPR+ switchover from the active to the standby supervisor engine, the CSM-S might go into offline mode, and you will not be able to enter commands in the CSM-S CLI.

  Workaround: Power reset this CSM-S.

- CSCeh60960

  When running in router mode with the variable var ROUTE_UNKNOWN_FLOW_PKTS set to either 1 or 2, ICMP or UDP packets do not go directly to the access servers located behind the CSM-S. Telnet to these servers works fine when this value is set to 2, which is expected.

  Workaround: None.

- CSCeh60704

  When sending traffic to an SSL virtual server that has the csrp sticky (ssl session) and csrp conn options configured stopping the traffic and performing a configuration synchronization several times causes only the connections to replicate when the traffic is restarted.

  Workaround: Reload the active CSM-S. Reloading the standby CSM-S has no effect on this problem.

- CSCeh55357

  If you configure a virtual server with the **persistent rebalance** option enabled, the first two GET requests of a single TCP connection are load balanced to a regular HTTP real server. However, new HTTP GET requests are load balanced to a configured redirect server. The CSM-S fails to load balance these requests.

  An indication that this condition has occurred is if the output of the **show module csm** *slot* **tech-support proc 1** command shows that the value for the **Attempts to alloc used session** counter has incremented.

  Workaround: Remove the **persistent rebalance** option for this virtual server.

- CSCeh41862

  When the track gateway feature is used for CSM-S failover functionality and the host or gateway is more than one hop away from the CSM-S, the module enters the standby state even if you can ping the host from the CSM-S. The CSM-S is attempting to request ARP for the host.

  Workaround: None.

- CSCeh21118

  If you configure **match protocol http cookie** for a virtual server, the CSM-S might reload after a few million connections have been established to this virtual server. If you have also enabled sticky replication, the CSM-S might reload sooner.

  The core-dump shows:

  ```
  IXP4 Bad Data exception on task +IXP4 SA-CORE (Ex 5)...+
  ```

  Workaround: Remove the configuration for cookie map matching.

- CSCeg69049

  When you configure a scripted probe with a script-name that does not exist, the output of the **show module csm tech-script** command indicates the status of this probe as NOSCRIPT.

After you load a valid script into the CSM by entering the **script file** command, the output of the **show module csm tech-script** command continues to indicate the status of this probe as NOSCRIPT.

This output indicates a display status problem only.

- CSCeg49522

  The ROUTE_UNKNOWN_FLOW_PKTS environment variable accepts a value of 0, 1, or 2. But, when you assign a value of 2 for this variable, the CSM-S changes it to a value of 3. This situation indicates a configuration setting problem only. The value of 3 operates as expected (route SYN and non-SYN packets).

- CSCeg04864

  When configuring cookie switching with multiple cookie values for a specific cookie name, the CSM-S may incorrectly load balance the request.

  This problem occurs only when the “or” pipe (|) is used between cookie values. Using the pipe character causes the CSM-S to incorrectly search the second or later regular expression parameter in all of the cookies in the HTTP header and not just the configured cookie name.

  For the expression *ABC | *XYZ the correct syntax must include parentheses around the alternate OR condition as follows: (*ABC | *XYZ).

  Workaround: Enter the parentheses into the matching string.

- CSCef88345

  A CSM-S may send the synchronize acknowledge (SYN ACK) packet, to the wrong destination in response to a synchronize start (SYN) packet received for a virtual server that requires parsing above Layer 4.

  Workaround: Configure the next-hops as real servers in a dummy server farm.

- CSCed82590

  The CSM-S might forward ICMP reply packets to the backup CSM-S instead of forwarding the packets to the MSFC. This situation results in a communication failure.

  Workaround: Configuring the virtual server for the ICMP traffic with an appropriate idle timeout value.

- CSCec75637

  The CSM-S issues ARP requests only for the configured routers or real servers but not for clients or routers where the client traffic originates. The CSM-S can learn them only from ARP requests received. If there is no ARP entry for a device, traffic is dropped. The traffic to a virtual source from one of these clients is also dropped.

  This situation becomes a problem in a redundancy setup that is configured with preempt. When an initial failover occurs and the preempt CSM-S takes becomes active, the clients that are local to the CSM-S client VLAN (usually a cache or proxy device) are not learned.

  Workaround: Configure a dummy real server to force the CSM-S to ARP, move the client a router hop away, or reduce the ARP timeout on the client.

Open Caveats in Software Release 2.1(2) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(2), see the "Resolved Caveats in Software Release 2.1(2) for SSL" section on page 90.

This section describes known SSL limitations that exist in CSM-S software release 2.1(2).

- CSCin67360

  The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed and the configuration is not accepted. Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) into the request.

  Workaround: Save the configuration, and reset the SSL Services Module.

- CSCee69321

  When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment.

- CSCee46096

  If you delete the route to the real server from the SSL proxy VLAN and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module.

- CSCee37656

  On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module.

- CSCed14070

  When you import a certificate from a PKCS12 or PEM file or when you manually input a certificate authority certificate to the module, and the certificate contains an invalid extension, the SSL peer might reject the certificate.

  Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module.

- CSCec82360

  If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

Workaround: When a certificate authority has renewed its certificate, make sure that you renew all the SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem.

- CSCec74017

  The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment.

  Workaround: None.

- CSCec69592

  On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module.

- CSCec46997

  If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing slash (/) in the URL, the SSL Services Module does not rewrite the URL.

  Workaround: Configure the server to add a trailing slash (/) to the relocation string.

- CSCec19596

  Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a Network Time Protocol (NTP) server.

  Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

  Workaround 2: Reset the enrollment timer by doing the following:

  a. Copy the "crypto ca trustpoint *trustpoint_label*" and "crypto ca certificate chain *name*" information from the running configuration.
  b. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.
  c. Paste the trustpoint and certificate chain information to the configuration.

- CSCea71882

  The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate.

- CSCea50887

  There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command.

  Workaround: None.

- CSCea32058

  For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL.

- CSCdz24446

  Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available.

- CSCdz03802

  When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM.

- CSCdy85233

  Exporting a PKCS12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host.

  Workaround: None.

- CSCdy72229

  Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module.

  Workaround: None.

- CSCdy61618

  Syslog messages indicating that proxy services are in the up state may not be printed for all the services configured in the system while booting.

  Workaround: None.

- CSCdy46075

  When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates.

  Workaround: None.

Resolved Caveats in Software Release 2.1(2) for SSL

Note For a description of SSL caveats open in CSM-S software release 2.1(2), see the "Open Caveats in Software Release 2.1(2) for SSL" section on page 88.

This section describes the SSL caveats resolved in CSM-S software release 2.1(2).

- CSCej75255

  Added content, URL statistics to crash information, regular statistics.

  Workaround: None.

- CSCej38531

  When you add HTTP header insert policies to an SSL proxy service, the Content Switching Module with SSL might reset repeatedly and generate core dumps. This behavior occurs when a large number of end-of-http-headers are lost.

  Workaround: Do not apply policies performing header insertion to ssl-proxy-services.

  This problem is resolved in SSL software release 2.1(8).

- CSCsc26099

  When you configure a client proxy, the Content Switching Module with SSL resets when the backend SSL server does not allow session resumption and returns an empty session ID.

  Workaround: Enable session resumption on the backend SSL server.

  This problem is resolved in SSL software release 2.1(8).

- CSCsc13184

  A configuration option is required to disable the TCP Nagle algorithm.

  Workaround: An extra CLI option, the **no nagle** command, has been added to the software.

- CSCsb77689

  If you configure the Content Switching Module with SSL with header insertion, and if the total size of the server cookie, the client request, and the inserted header exceeds the size of the first buffer (1460 bytes) on the Content Switching Module with SSL, the buffer overflows and the Content Switching Module with SSL resets.

  Workaround: None.

  This problem is resolved in SSL software release 2.1(8).

- CSCej33386

  When you configure URL rewrite, the Content Switching Module with SSL scans the response from the server. Currently, the entire response (headers and data) is scanned, which leads to a drop in performance.

  Workaround: None.

  This problem is resolved in SSL software release 2.1(8).

Open Caveats in Software Release 2.1(1) for CSM

Note For a description of CSM caveats resolved in CSM-S software release 2.1(1), see the "Resolved Caveats in Software Release 2.1(1) for CSM" section on page 97.

This section describes known CSM limitations that exist in CSM-S software release 2.1(1).

- CSCsa88370

  Due to an ARP failure, a real server that is not directly connected to the CSM-S may become unreachable after a gateway failure occurs, even though there is still a valid gateway or route available.

  This situation occurs when there is more than one route (gateway) configured to reach the real server and the route chosen by the CSM-S becomes unavailable.

  Workaround: Remove the failed gateway from the configuration.

- CSCeh78584

  When you configure an alias IP address on a server VLAN on the CSM-S, you are incorrectly allowed to configure a network address for the alias.

- CSCeh76411

  When you configure **service ftp** on a virtual server and then configure a client NAT pool for that virtual server, the FTP virtual server allocates ports from the NAT pool and does not reclaim them.

  Workaround: Reboot the CSM-S to recover the allocated ports.

- CSCeh60960

  With the ROUTE_UNKNOWN_FLOW_PKTS environmental variable set to either **1** or **2**, ICMP or UDP packets cannot directly access servers behind the CSM-S when the CSM-S is in router mode.

  You can still Telnet to these servers when this environmental variable is set to 2.

- CSCeh60704

  The sticky table does not replicate after a configuration synchronization. This situation occurs when traffic is sent to an SSL virtual server that is configured with the **csrp sticky** (SSL session) and **csrp connection**. Initially, the connection works, but if traffic is stopped and a configuration synchronization operation is performed several times when the traffic is started again, only the connections replicate. Reloading the standby CSM-S does not correct the problem.

  Workaround: Reload the active CSM-S.

- CSCeh41862

  When you configure gateway tracking, if the host or gateway is more than 1 hop away, the CSM-S goes into standby state, even if the CSM-S can ping the host.

- CSCeh34176

  The **show module csm** *slot* **stats** command displays the incorrect value for the **Connections Timed-Out** counter.

  Workaround: Enter the **show module csm** *slot* **tech-support proc 1** to display the correct value.

- CSCeg77526

  After you enter the **script file bootflash:myscript.txt** command to load a script file into the CSM-S, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM-S. When you enter the **no script file bootflash:myscript.txt** command to remove the script file configuration, the **show** command for the script continues to display the same list of script functions.

  This situation occurs because the individual script was loaded into the CSM-S by using the **script file** command, which loads the script into memory. The CSM-S does not have a command that allows you to request a reload of the same script file to update the individual script.

  Do the following to reload the script with the same filename (but with newer content):

  a. Remove the script with the **no script file bootflash:myscript.txt** command. This command does not destroy nor stop the current probes that are using the existing scripts.

  b. Then, enter the **script file bootflash:myscript.txt** command to reload the new content. The probes will pick up the new script in the next interval of operation.

  Workaround: None. This is the current design for reloading a script. The scripts must remain in memory for the probes to operate. If you want to stop the probes from using those scripts, you must remove the probes. Scripts removed from the CSM-S remain in memory.

- CSCeg35110

  When you configure more than one virtual server with an IP address that is being used by a DNS server farm (GSLB feature), the health probe for the real server within this server farm might show as failed. This situation is caused by the probe checking the status of one virtual server instead of checking the status of all virtual servers with this IP address.

  Workaround: Remove those virtual servers which are out-of-service.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM-S, and the Packets Repeat Reverse Frag counter in the CSM-S increases quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM-S so that it knows where to send reassembled fragments that arrived in a reverse order.

- CSCef76686

  When you configure a server farm with the least-connections algorithm by entering the **predictor leastconns** command and enable the REAL_SLOW_START_ENABLE environment variable with the default rate (3), the slow-start feature might not take effect for newly activated servers in the server farm.

  Workaround: Configure the REAL_SLOW_START_ENABLE environment variable to 2.

- CSCef09179

  Resetting the CSM-S can cause these messages to appear on the supervisor engine console:

  ```
  %EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt FM_CRC16_ERR occurring in EARL bus
  connection.
  %EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt HD_CRC_ERR occurring in EARL bus connection.
  %EARL-SP-STDBY-4-BUS_CONNECTION: Interrupt ENCAP_ERR occurring in EARL bus connection.
  ```

  This situation happens only when there is a non-fabric-enabled module in the chassis. The CSM-S is a non-fabric-enabled module.

  Workaround: None.

- CSCef02629

  During a supervisor engine switch over, the standby CSM-S fails to initialize, and the new standby supervisor engine prints the following message for all CSM-S ports:

  ```
  %PM-STDBY-4-INT_FAILUP:GigabitEthernet7/2 failed to come up.No internal VLAN available
  ```

  Workaround: None.

- CSCee92560

  If more than one CSM-S in a chassis is reset through the **hw-reset** command, one of the modules may fail to reboot the first time. This failure may be caused when the supervisor engine timeout value for a module attempts to reset itself. In these cases, the module must either be power-cycled or reset.

  Workaround: If the module does not boot after a reset, use the **hw-reset** command to restart the module or power cycle the switch.

- CSCee91798

  In a CSM-S fault tolerant configuration, for a failover might occur between the CSM-S fault-tolerant pair. Failover might not occur if the SSL daughter card fails. When the SSL daughter card failure is detected, the SSL daughter card restarts, causing all SSL flows to fail. The SSL flows will need to be re-established.

  Workaround: None.

- CSCee81437

  The CSM-S module may stop responding to the supervisor engine keep-alive polling. When this situation occurs, the supervisor power cycles the module to restart it. After restarting, the module operates correctly.

  Workaround: None.

- CSCee57427

  Starting with software Release 12.2(18)SXD, the CSM-S needed to have identifiers assigned in the MIBs, as shown in this example:

  ```
  CISCO-ENTITY-VENDORTYPE-OID-MIB.my & OLD-CISCO-CHASSIS-MIB.my
  ```

  This situation causes incorrect values to show up through SNMP. New identifier assignments have been made in the MIBs and are available in the 12.2(18)SXD release, as shown in this example:

  ```
  CISCO-ENTITY-VENDORTYPE-OID-MIB.my:
  csm-ssl(442) --  CSM-S is a content switching module with integrated SSL acceleration

  OLD-CISCO-CHASSIS-MIB.my:
  cevChassisCSMSsl  OBJECT IDENTIFIER ::= { cevChassis 479 }
  --  CSM-S is a content switching module with integrated SSL acceleration
  ```

  Workaround: None.

- CSCee33514

  When the module starts up, you may see messages on the CSM-S console, as follows:

  ```
  SCP:Rcvd an Unknown Opcode 0x3e...
  SCP:Rcvd an Unknown Opcode 0x3e...
  SCP:Subcommand: COMMAND_MODULE_ONLINE
  Module has become online.
  SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
  SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
  ```

  Workaround: None. There is no operational impact that results from these messages. They can be safely ignored.

- CSCee26687

  CSM-S does not allow static ARP for the SSL daughter card interface.

  Workaround: None.

- CSCee18203

  Multiple syslog messages may appear under heavy certificate authenticated SSL traffic and the SSL Cisco IOS console may become unresponsive. The heavy traffic is for an SSL proxy-service that has certificate authentication turned on. For example:

  ```
  ssl-proxy(config-ssl-proxy)# authenticate verify { signature-only | all }
  ```

The more traffic, the more unresponsive the console becomes. At very high traffic loads the following syslog may appear:

```
*Apr 1 22:39:13.071: %SCHED-3-THRASHING: Process thrashing on
watched boolean 'CSM IOS Watch Bool'.
-Process= "CSM IOS I/O Process", ipl= 5, pid= 27
-Traceback= 5233E8 5234CC 5C6044
```

Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the static NAT client into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM-S might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM-S.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the static NAT client into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the static NAT client into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM-S.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCec21915

  The possible number of VLANs has increased to 511. This limit is the total number of IP interfaces and alias IP interfaces that can be configured on the CSM-S. If you need to configure alias IP addresses, you need to reduce the number of VLAN IP interfaces.

  Workaround: Reduce the number of configured VLANs to accommodate the total number of alias IP addresses.

- CSCeb52054

  When the Layer 7 virtual servers have many connections that are in the process of load balancing, the new and existing connections receive a slow response from the CSM-S. The connections, which are still waiting for more data from the client or which are waiting for the response from the server, are considered to be in the process of load balancing.

  Workaround: Configure the max-conns option on the servers for slow response servers, or lower the number for the max-parselen option to reduce the unnecessary wait for invalid HTTP connections.

- CSCeb47499

  The UDP probe configured for a server farm can only detect a failure of a UDP service when the connectivity to the server IP address is opened. The CSM-S relies on the ICMP port unreachable message from the server so that it can detect whether the UDP service is available. If the interface on the server is down, the UDP probe cannot detect this failure condition.

  Workaround: Configure an ICMP probe to the same server farm where the UDP probe is configured.

- CSCea43504

  If your configuration contains a pair of CSM-Ss in a single fault-tolerant group and these paired CSM-Ss are in an active-standby state, the CSM-Ss might not retain the valid active-standby state if you add another CSM-S into this same fault-tolerant group, causing the fault-tolerant pair of CSM-Ss to enter an invalid active-active state.

  Workaround: Remove the third CSM-S from the network and reboot the paired CSM-Ss to allow them to recover their fault-tolerant state.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example host-unreachable), the function does not return with an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-S-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM-S and the destination host could respond with a “destination unreachable” message to the CSM-S if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

- CSCdw84018

  The CSM-S may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM-S uses to parse the RSTP service. For this same virtual server, you must also configure a NAT client on the server farm.

  Workaround: Remove the NAT client configuration from the server farm, or remove the service RTSP from the virtual server.

- CSCdv11685

  When more than one pair of redundant CSM-Ss are configured to use the same VLAN ID, the CSM-S will accept replication messages from all fault-tolerant groups by using the specified VLAN. In this configuration, the session and sticky replication may not work properly.

  Workaround: Configure a unique VLAN trunk for each pair of fault-tolerant groups.

Resolved Caveats in Software Release 2.1(1) for CSM

Note For a description of CSM caveats open in CSM-S software release 2.1(1), see the "Open Caveats in Software Release 2.1(1) for CSM" section on page 91.

This section describes the CSM caveats resolved in CSM-S software release 2.1(1).

- CSCsa74493

  If you create a serverfarm and a cookie insert sticky group, and a policy to associate both, the CSM-S generates a static cookie entry that is displayed with the **show mod csm** *slot* **sticky** command.

  If you add a new real to the serverfarm, the cookie information is not updated.

  Workaround: Remove the policy and reconfigure it.

- CSCeh73953

  If you add several policies to a virtual server and configure the priority option using the **slb-policy** *policy-name* **priority** *priority_value* command and then remove a policy that is not configured with the highest priority, the CSM-S might reload.

  This problem does not exist for policies that are not configured with the **priority** option.

  Workaround: Remove only the policy with the highest priority in the list.

- CSCeh64012

  In rare instances due to a message timing problem, when the supervisor engine performs an RPR+ switchover from the active to the standby supervisor engine, the CSM-S might go into offline mode, and you will not be able to enter commands in the CSM-S CLI.

  Workaround: Power reset this CSM-S.

- CSCeh55357

  If you configure a virtual server with the **persistent rebalance** option enabled, the first two GET requests of a single TCP connection are load balanced to a regular HTTP real server. However, new HTTP GET requests are load balanced to a configured redirect server. The CSM-S fails to load balance these requests.

  An indication that this condition has occurred is if the output of the **show module csm** *slot* **tech-support proc 1** command shows that the value for the **Attempts to alloc used session** counter has incremented.

  Workaround: Remove the **persistent rebalance** option for this virtual server.

- CSCeh21118

  If you configure **match protocol http cookie** for a virtual server, the CSM-S might reload after a few million connections have been established to this virtual server. If you have also enabled sticky replication, the CSM-S might reload sooner.

  The core-dump shows:

  ```
  IXP4 Bad Data exception on task +IXP4 SA-CORE (Ex 5)...+
  ```

  Workaround: Remove the configuration for cookie map matching.

- CSCeg69049

  When you configure a scripted probe with a script-name that does not exist, the output of the **show module csm tech-script** command indicates the status of this probe as NOSCRIPT.

After you load a valid script into the CSM-S by entering the **script file** command, the output of the **show module csm tech-script** command continues to indicate the status of this probe as NOSCRIPT.

This output indicates a display status problem only.

- CSCeg49522

  The ROUTE_UNKNOWN_FLOW_PKTS environment variable accepts a value of 0, 1, or 2. But, when you assign a value of 2 for this variable, the CSM-S changes it to a value of 3. This situation indicates a configuration setting problem only. The value of 3 operates as expected (route SYN and non-SYN packets).

- CSCef88345

  A CSM-S may send the synchronize acknowledge (SYN ACK) packet, to the wrong destination in response to a synchronize start (SYN) packet received for a virtual server that requires parsing above Layer 4.

  Workaround: Configure the next-hops as real servers in a dummy server farm.

- CSCed82590

  The CSM-S might forward ICMP reply packets to the backup CSM-S instead of forwarding the packets to the MSFC. This situation results in a communication failure.

  Workaround: Configuring the virtual server for the ICMP traffic with an appropriate idle timeout value.

Open Caveats in Software Release 2.1(1) for SSL

Note For a description of SSL caveats resolved in CSM-S software release 2.1(1), see the "Resolved Caveats in Software Release 2.1(1) for SSL" section on page 100.

This section describes known SSL limitations that exist in CSM-S software release 1.1(2).

- CSCee46096

  If you delete the route to the real server from the SSL proxy VLAN and then configure another SSL proxy VLAN with the same network as the server IP address, the SSL proxy service goes into a down state and the proxy status shows "No Server VLAN," even though the real server is reachable from the SSL Services Module.

  Workaround: Save the configuration, and reset the SSL Services Module.

- CSCee37656

  On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSL Services Module after a switchover (either from the CLI or the SHUTDOWN button on the front panel), the module will not shut down, and its status will remain as Other.

  Workaround: Reset the module, and then shut down the module.

- CSCed14070

  When you import a certificate from a PKCS12 or PEM file or when you manually input a certificate authority certificate to the module, and the certificate contains an invalid extension, the SSL peer might reject the certificate.

Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module.

- CSCec82360

  If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

  Workaround: When a certificate authority has renewed its certificate, make sure that you renew all the SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem.

- CSCec74017

  The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment.

  Workaround: None.

- CSCec69592

  On systems that are running Catalyst operating system software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switchover, the supervisor engine displays the following error:

  ```
  Console> (enable) Error: Module <mod> didn't shutdown complete within 3 min.Module
  resetting...
  ```

  The supervisor engine then successfully resets the SSL Services Module.

- CSCea71882

  The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure that authentication is successful the first time, and then enroll the router certificate.

- CSCea50887

  There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command.

  Workaround: None.

- CSCea32058

  For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL.

- CSCdz24446

  Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available.

- CSCdy72229

  Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module.

  Workaround: None.

Resolved Caveats in Software Release 2.1(1) for SSL

Note For a description of SSL caveats open in CSM-S software release 2.1(1), see the "Open Caveats in Software Release 2.1(1) for SSL" section on page 98.

This section describes the SSL caveats resolved in CSM-S software release 2.1(1).

- CSCsa75762

  If you configure the Content Switching Module with SSL with **client-ip-port** header insertion, and if the total size of the client cookie and the inserted header exceeds the size of the first buffer (1460 bytes) on the Content Switching Module with SSL, the buffer overflows, and the Content Switching Module with SSL resets.

  This problem is resolved in SSL software release 2.1(5).

- CSCsa57669

  The SSL Services Module does not properly recycle connection IDs. This action causes service to degrade to a point that the module stops responding.

  Workaround: Reboot the SSL Services Module.

  This problem is resolved in SSL software release 2.1(5).

- CSCin67360

  The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service, and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed and the configuration is not accepted.

  Output from the **show running-config** command and the **show ssl-proxy service** *service_name* command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) in the request.

  Workaround: Save the configuration and reset the SSL Services Module.

- CSCeh26040, CSCeh14851

  Applications, such as e-mail clients, Web browsers, and FTP clients, might stop responding after the client receives a certain amount of data, either 32 Kb (the default offered TCP window size) or the maximum receive buffer share as specified in the server policy. This problem occurs when the client offers a zero window size for the TCP connection.

  Workaround: Increase the offered window size of the TCP connection beyond the transaction size by entering the **buffer-share rx** *buffer_limit* command in the server policy and the **buffer-share tx** *buffer_limit* command in the client policy.

  This problem is resolved in SSL software release 2.1(5).

- CSCeh21346

  When the SSL Services Module acts as a client, and a CertReq message spans across multiple buffers, the SSL handshake fails. The "multi buf rec errors" counter is incremented in the output of the **show ssl-proxy stats ssl** command.

  This problem is resolved in SSL software release 2.1(5).

- CSCeh19256

  The SSL Services Module reloads when it accesses a file system that uses secure HTTP (HTTPS) if there are no certificates in the module.

  Workaround: Have a certificate in the module when using HTTPS.

  This problem is resolved in SSL software release 2.1(5).

- CSCeh20306

  The SSL Services Module might incorrectly terminate a backend SSL session. When the problem occurs, the SSL Services Module sends a FIN to the backend SSL server and may increment counters in the **show ssl-proxy stats service** command:

  ```
  data failures       : 26
  fatal alerts sent   : 31
  bad macs received   : 26
  ```

  This problem is resolved in SSL software release 2.1(5).

- CSCef67472

  In SSL software releases 2.1(4) and earlier, when you reset the SSL Services Module after it stops responding, the output of the **show ssl-proxy crash-info** command displays only information related to how the CPU stopped responding. In SSL software release 2.1(5), the output of the **show ssl-proxy crash-info** command contains additional statistics for the TCP, SSL, and FDU processors.

  This problem is resolved in SSL software release 2.1(5).

- CSCee69321

  When you configure trustpoints for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

  Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trustpoints for manual or TFTP enrollment.

- CSCdz03802

  When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM.

- CSCdy85233

  Exporting a PKCS#12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host.

  Workaround: None.

- CSCdy61618

  Syslog messages indicating that proxy services are in the up state may not be printed for all the services configured in the system while booting.

  Workaround: None.

- CSCdy46075

  When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates.

  Workaround: None.

Troubleshooting

CSM-S error messages may be received and reported in the system log (syslog). This section describes these messages.

Message Banners

When syslog messages are received, they are preceded by one of the following banners (where # is the slot number of the CSM-S module):

Error Message `CSM_SLB-4-INVALIDID Module # invalid ID`

```
00:00:00: CSM_SLB-4-DUPLICATEID Module # duplicate ID
00:00:00: CSM_SLB-3-OUTOFMEM Module # memory error
00:00:00: CSM_SLB-4-REGEXMEM Module # regular expression memory error
00:00:00: CSM_SLB-4-ERRPARSING Module # configuration warning
00:00:00: CSM_SLB-4-PROBECONFIG Module # probe configuration error
00:00:00: CSM_SLB-4-ARPCONFIG Module # ARP configuration error
00:00:00: CSM_SLB-6-RSERVERSTATE Module # server state changed
00:00:00: CSM_SLB-6-GATEWAYSTATE Module # gateway state changed
00:00:00: CSM_SLB-3-UNEXPECTED Module # unexpected error
00:00:00: CSM_SLB-3-REDUNDANCY Module # FT error
00:00:00: CSM_SLB-4-REDUNDANCY_WARN Module # FT warning
00:00:00: CSM_SLB-6-REDUNDANCY_INFO Module %d FT info
00:00:00: CSM_SLB-3-ERROR Module # error
00:00:00: CSM_SLB-4-WARNING Module # warning
00:00:00: CSM_SLB-6-INFO Module # info
00:00:00: CSM_SLB-4-TOPOLOGY Module # warning
00:00:00: CSM_SLB-3-RELOAD Module # configuration reload failed
00:00:00: CSM_SLB-3-VERMISMATCH Module # image version mismatch
00:00:00: CSM_SLB-4-VERWILDCARD Received CSM-SLB module version wildcard on slot #
00:00:00: CSM_SLB-3-PORTCHANNEL Portchannel allocation failed for module #
00:00:00: CSM_SLB-3-IDB_ERROR Unknown error occurred while configuring IDB
```

Server and Gateway Health Monitoring

Error Message `SLB-LCSC: No ARP response from gateway address A.B.C.D.`

Explanation The configured gateway A.B.C.D. did not respond to ARP requests.

Error Message `SLB-LCSC: No ARP response from real server A.B.C.D.`

Explanation The configured real server A.B.C.D. did not respond to ARP requests.

Error Message `SLB-LCSC: Health probe failed for server A.B.C.D on port P.`

Explanation The configured real server on port P of A.B.C.D. failed health checks.

Error Message `SLB-LCSC: DFP agent <x> disabled server <x>, protocol <x>, port <x>`

Explanation The configured DFP agent has reported a weight of 0 for the specified real server.

Error Message `SLB-LCSC: DFP agent <x> re-enabled server <x>, protocol <x>, port <x>`

Explanation The configured DFP agent has reported a non-zero weight for the specified real server.

Diagnostic Messages

Error Message `SLB-DIAG: WatchDog task not responding.`

Explanation A critical error occurred within the CSM-S hardware or software.

Error Message `SLB-DIAG: Fatal Diagnostic Error %x, Info %x.`

Explanation A hardware fault was detected. The hardware is unusable and must be repaired or replaced.

Error Message `SLB-DIAG: Diagnostic Warning %x, Info %x.`

Explanation A non-fatal hardware fault was detected.

Fault Tolerance Messages

Error Message `SLB-FT: No response from peer. Transitioning from Standby to Active.`

Explanation The CSM-S detected a failure in its fault-tolerant peer and has transitioned to the active state.

Error Message `SLB-FT: Heartbeat intervals are not identical between ft pair.`
`SLB-FT: Standby is not monitoring active now.`

Explanation Proper configuration of the fault-tolerance feature requires that the heartbeat intervals be identical between CSM-Ss within the same fault-tolerance group, which is currently not the case. The fault-tolerance feature is disabled until the heartbeat intervals have been configured identically.

Error Message `SLB-FT: heartbeat interval is identical again`

Explanation The heartbeat intervals of different CSM-Ss in the same fault-tolerance group have been reconfigured to be identical. The fault-tolerance feature will be re-enabled.

Error Message `SLB-FT: The configurations are not identical between the members of the fault tolerant pair.`

Explanation In order for the fault-tolerance system to preserve the sticky database, the different CSM-Ss in the fault-tolerance group must be identically configured, which is not currently the case.

Regular Expression Errors

Error Message
```
SLB-LCSC: There was an error downloading the configuration to hardware
SLB-LCSC: due to insufficient memory. Use the 'show ip slb memory'
SLB-LCSC: command to gather information about memory usage.
SLB-LCSC: Error detected while downloading URL configuration for vserver %s.
```

Explanation The hardware does not have sufficient memory to support the desired set of regular expressions. A different set of regular expressions must be configured for the system to function properly.

Error Message
```
SLB-REGEX: Parse error in regular expression <x>.
SLB-REGEX: Syntactic error in regular expression <x>.
```

Explanation The configured regular expression does not conform to the regular expression syntax as described in the user manual.

Error Message
```
SLB-LCSC: Error detected while downloading COOKIE policy map for
vserver <x>.
SLB-LCSC: Error detected while downloading COOKIE <x> for vserver <x>.
```

Explanation An error occurred in configuring the cookie regular expressions for the virtual server. This error is likely due to a syntactic error in the regular expression (see below), or there is insufficient memory to support the desired regular expressions.

XML Errors

When an untolerated XML error occurs, the HTTP response contains a 200 code. The portion of the original XML document with the error is returned with an error element that contains the error type and description.

This example shows an error response to a condition where a virtual server name is missing:

```
      <?xml version="1.0"?>
      <config>
       <csm_module slot="4">
        <vserver>
         <error code="0x20">Missing attribute name in element

vserver</error>
        </vserver>
       </csm_module>
      </config>
```

The error codes returned also correspond to the bits of the error tolerance attribute of the configuration element. Returned XML error codes are as follows:

```
XML_ERR_INTERNAL          = 0x0001,
XML_ERR_COMM_FAILURE      = 0x0002,
XML_ERR_WELLFORMEDNESS    = 0x0004,
XML_ERR_ATTR_UNRECOGNIZED = 0x0008,
XML_ERR_ATTR_INVALID      = 0x0010,
XML_ERR_ATTR_MISSING      = 0x0020,
XML_ERR_ELEM_UNRECOGNIZED = 0x0040,
XML_ERR_ELEM_INVALID      = 0x0080,
XML_ERR_ELEM_MISSING      = 0x0100,
XML_ERR_ELEM_CONTEXT      = 0x0200,
XML_ERR_IOS_PARSER        = 0x0400,
XML_ERR_IOS_MODULE_IN_USE = 0x0800,
XML_ERR_IOS_WRONG_MODULE  = 0x1000,
XML_ERR_IOS_CONFIG        = 0x2000
```

The default error_tolerance value is 0x48, which corresponds to ignoring unrecognized attributes and elements.

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Content Switching Module Configuration Note*
- *Catalyst 6500 Series Content Switching Module Command Reference*
- *Catalyst 6500 Series Content Switching Module Installation and Verification Note*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- For information about MIBs, refer to this URL:

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

Cisco IOS Software Documentation Set

Cisco IOS Configuration Guides and Command References—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.