Release Notes for Catalyst 6500 Series Switch SSL Services Module Software Release 2.x

Current Release: 2.1(13)—November 16, 2010
Previous releases: 2.1(12), 2.1(11), 2.1(10), 2.1(9), 2.1(8), 2.1(7), 2.1(6), 2.1(5), 2.1(4), 2.1(3), 2.1(2), 2.1(1)

The SSL Services Module is a Layer 4 through Layer 7 service module that you can install into the Catalyst 6500 series switch. The module terminates secure sockets layer (SSL) transactions and accelerates the encryption and decryption of data used in SSL sessions.

This publication describes the features, modifications, and caveats for the Catalyst 6500 series SSL Services Module software release 2.*x*.

Note For detailed installation and configuration procedures for the SSL Services Module, refer to the Catalyst 6500 series SSL Services Module documentation at this URL: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/Install/78_15947.html

Contents

This document consists of these sections:

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 SSL Services Module, software release 2.x:

Hardware Requirements

The Catalyst 6500 series SSL Services Module is supported in systems with a Supervisor Engine 2 with an MSFC2 or a Supervisor Engine 720 with an MSFC3, and any module with ports that connect server and client networks.

Software Requirements

Note Starting with maintenance image release 2.1(1), there is a single maintenance image for services modules. Refer to this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

Table 1 lists the SSL software versions supported by Catalyst operating system and Cisco IOS software.

Table 1 SSL Software Compatibility

Product Number	Minimum SSL Software Version		Recommended SSL Software Version		Minimum Cisco IOS Software	Minimum Catalyst Software
	Application Image	Maintenance Image	Application Image	Maintenance Image		
WS-SVC-SSL-1 with Supervisor Engine 720	1.2(2)	1.2(1)[1]	2.1(9)	2.1(3)	12.2(17a)SX1	8.2(1)
					12.2(14)SX1	–
WS-SVC-SSL-1 with Supervisor Engine 2	1.2(2)	1.2(1)[1]	2.1(9)	2.1(3)	12.1(13)E3	7.5(1)
					12.1(13)E	–

1. Do not use the 1.2(2) maintenance image.

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the SSL software.

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number
2.1(13)	c6svc-ssl-k9y9.2-1-13.bin	SC-SVC-SSL-2.1.13-K9
2.1(12)	c6svc-ssl-k9y9.2-1-12.bin	SC-SVC-SSL-2.1.12-K9
2.1(11)	c6svc-ssl-k9y9.2-1-11.bin	SC-SVC-SSL-2.1.11-K9

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number
2.1(10)	c6svc-ssl-k9y9.2-1-10.bin	SC-SVC-SSL-2.1.10-K9
2.1(9)	c6svc-ssl-k9y9.2-1-9.bin	SC-SVC-SSL-2.1.9-K9
2.1(8)	c6svc-ssl-k9y9.2-1-8.bin	SC-SVC-SSL-2.1.8-K9
2.1(7)	c6svc-ssl-k9y9.2-1-7.bin	SC-SVC-SSL-2.1.7-K9
2.1(6)	c6svc-ssl-k9y9.2-1-6.bin	SC-SVC-SSL-2.1.6-K9
2.1(5)	c6svc-ssl-k9y9.2-1-5.bin	SC-SVC-SSL-2.1.5-K9
2.1(4)	c6svc-ssl-k9y9.2-1-4.bin	SC-SVC-SSL-2.1.4-K9
2.1(3)	c6svc-ssl-k9y9.2-1-3.bin	SC-SVC-SSL-2.1.3-K9
2.1(2)	c6svc-ssl-k9y9.2-1-2.bin	SC-SVC-SSL-2.1.2-K9
2.1(1)	c6svc-ssl-k9y9.2-1-1.bin	SC-SVC-SSL-2.1.1-K9

New Features in Software Release 2.1

This section describes the new features available in SSL software release 2.1:

- SSL initiation

  This feature allows you to configure the SSL Services Module as an SSL client. When you configure an SSL proxy service for SSL client functionality, the SSL Services Module negotiates an SSL session with the server and uses that session to encrypt the clear-text data coming from the client connection.

- SSL version 2.0 forwarding

  This feature allows you to configure the SSL Services Module to forward SSLv2 connections to another server. When you configure the SSLv2 server IP address, the SSL Services Module transparently forwards all SSLv2 connections to that server.

- URL rewrite

  URL rewrite rules resolve the problem of a website redirecting you to a nonsecure HTTP URL by rewriting the domain from http:// to https://. By configuring URL rewrite, all client connections to the web server are SSL connections, ensuring the secure delivery of HTTPS content back to the client.

- HTTP header insertion

  This feature provides support for servers that require information inserted into an HTTP header.

- Wildcard proxy

  Wildcard SSL proxy provides a flexible network configuration interface if you have a large number of servers in your network.

- Client certificates

  This feature allows you to configure a certificate for a client-type proxy service. When acting as an SSL client, the SSL Services Module sends this certificate for authentication if the SSL server requests it, and the issuer of this certificate is on the server's list of acceptable certificate authorities.

- Client and server certificate caching

  This feature allows you to cache peer certificates that have been authenticated within a configurable time interval.

- Client and server certificate authentication

  This feature allows you to configure the option to request and authenticate the client certificate when the SSL Services Module acts as a SSL server. The SSL Services Module automatically authenticates the server certificate when it acts as a SSL client. The feature specifies a set of trusted certificate authorities and the scope of validation for each proxy service.

- Certificate security attribute-based access control lists

  This feature allows you to configure an access control list (ACL) that filters certificates based on certificate attribute values.

- Certificate revocation lists (CRL)

  A CRL is a time-stamped list that identifies certificates that should no longer be trusted. When a participating peer device uses a certificate, that device not only checks the certificate signature and validity but also checks that the certificate serial number is not on that CRL.

- Certificate expiration warning

  When you enable certificate expiration warnings, the SSL Services Module checks every 30 minutes for expiration information. The SSL Services Module can log warning messages and send SNMP traps when certificates have expired or will expire within a specified amount of time.

- Module-level redundancy with multiple SSL Services Modules configured with HSRP

  You can configure HSRP to provide redundancy when the SSL Services Module is used in a standalone configuration (using policy-based routing).

- TACACS/TACACS+/RADIUS

  The feature allows you to configure external servers for authentication, authorization, and accounting (AAA).

- Password recovery

  This feature allows you to access the SSL Services Module without any authentication using the password recovery script.

Note You can download the password recovery script from the Cisco.com software center.

- SNMP support
  - CISCO-SSL-PROXY-MIB (All objects are read-only)

    cspGlobalConfigGroup

    cspProxyServiceConfigGroup

    cspProxyServiceNotificationGroup

    cspSslGroup

    cspSsl3Group

    cspTls1Group

    cspSslErrorGroup

    cspCpuStatusGroup

  - CISCO-SSL-PROXY-CAPABILITY

- CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 (CVDM-SSLSM)

  CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL Services Module. It is a task-based tool that allows users to take advantage of the versatility of their SSL Services Module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.

  To access all CiscoView Device Manager documentation, go to this URL:

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

Features in Software Release 1.1 Through 1.2

For a complete list of features for SSL software releases 1.1 through 1.2, refer to the *Release Notes for Catalyst 6500 Series SSL Services Module Software Release 1.x* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3396.htm

New and Changed Information

This section describes new and changed information for all 2.1(x) software releases:

- The **ssl-proxy device-check interval** *msec* **reset-limit** *limit* command is introduced. This command is normally disabled (device check interval is 0). If the command is enabled, the SSLM checks the crypto device at every interval for proper operation. If there are outstanding requests older than the request interval, the crypto device is reset to return to operational status. A reset limit can also be configured. If the reset limit is set to default (zero), there is no limit. If the reset limit is non zero, the SSLM reboots if the device is reset for more than the reset-limit number of consecutive poll intervals. The change is added in SSL software release 2.1(13). (CSCtj13900)

- The following new counters are introduced to the **show ssl-proxy stats ssl** command. The change is added in SSL software release 2.1(13). (CSCti85702, CSCtj13900)

  Http headers removed: The number of headers removed.

  Http header removal errs: The number of parse errors encountered while attempting to remove a header.

  available ctx count: The number of free-request elements in the free pool. Under no-load conditions, the available ctx count should be 64. Values less than 64 correspond to pending requests for the crypto device.

  ctx cleanup count: The number of request elements that were made available by resetting the crypto device.

  device reset count: The number of times the crypto device was reset.

- The **pre-remove-http-hdr** option in the **policy http-header** command is introduced. This command instructs the SSLM to remove HTTP headers from the requests received by the SSLM if the field name exactly matches a header that the SSLM may insert. The header field names are:

  Client-IP

  Client-Port

  Session-Id

  Session-Step-Up

Session-Initial-Cipher-Name

Session-Initial-Cipher-Key-Size

Session-Initial-Cipher-Use-Size

Session-Cipher-Name

Session-Cipher-Key-Size

SSL-ClientCert-Valid

SSL-ClientCert-Error

SSL-ClientCert-Fingerprint

SSL-ClientCert-Subject-CN

SSL-ClientCert-Issuer-CN

SSL-ClientCert-Certificate-Version

SSL-ClientCert-Serial-Number

SSL-ClientCert-Data-Signature-Algorithm

SSL-ClientCert-Subject

SSL-ClientCert-Issuer

SSL-ClientCert-Not-Before

SSL-ClientCert-Not-After

SSL-ClientCert-Public-Key-Algorithm

SSL-ClientCert-RSA-Public-Key-Size

SSL-ClientCert-RSA-Modulus-Size

SSL-ClientCert-RSA-Modulus

SSL-ClientCert-RSA-Exponent

SSL-ClientCert-X509v3-Authority-Key-Identifier

SSL-ClientCert-X509v3-Basic-Constraints

SSL-ClientCert-Signature-Algorithm

SSL-ClientCert-Signature

SSL-ClientCert-PE

The change is added in SSL software release 2.1(13). (CSCti85702)

- The **timeout time-wait** *seconds* subcommand is introduced for the **policy tcp** *name* command. The TIME_WAIT timeout ensures that delayed TCP segments from an old connection are not incorrectly determined to be part of a new connection. The TIME_WAIT state is entered if the SSLM initiates the close TCP protocol with a FIN, and when the SSLM receives a FIN from the remote host. The SSLM in the TIME_WAIT state ignores all TCP messages except another FIN, which causes the TIME_WAIT timer to restart. When the TIME_WAIT timer expires, the connection is closed. The TIME_WAIT timeout on the SSLM defaults to 16 seconds. The TIME_WAIT timeout can be tuned to a value between 1 and 240 seconds. The change is added in SSL software release 2.1(13). (CSCsy92231)
- In the output display of the **show ssl-proxy stats service context** command, the **valid session** counter is renamed to **session cache entry**. The counter displays the number of SSL session IDs in the cache. The change is added in SSL software release 2.1(12). (CSCek28849)

- New CLI command **min-chain-length** is added in SSL software release 2.1(12). (CSCsl42088)

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

Limitations and Restrictions

This section describes general limitations and restrictions for all 2.1(x) software releases:

- You can install a maximum of four SSL Services Modules in a chassis.
- Although Cisco IOS Release 12.1(13)E and later releases support 4096 VLANs, the SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.
- The SSL software does not monitor the health of the real (HTTP) servers. If a real server goes into a down state, the system shows that the service status is up until the Cisco IOS software retries and fails ARP after the default timeout period.

  Workaround 1: If you know that the HTTP server is down, enter the **no inservice** command for the corresponding SSL proxy service.

  Workaround 2: If you are using the SSL Services Module with a Content Switching Module (CSM), configure health monitoring on the CSM. (CSCdy83210)
- The client (SSL) and server (HTTP) connections that were bound during data transfer show up as four connections in the TCP connection table if both connections are in TIME_WAIT state. (CSCdy69930)
- With an open TCP connection, when the associated SSL proxy service is deleted and configured again using the same name, the association between the SSL proxy service and the previous open TCP connection is lost. When you delete and create the same SSL proxy service, a new service ID for the same service name is created. (CSCdy68548)
- When you configure private VLANs, the SSL Services Module VLAN must be different from the primary or secondary VLAN on the client or server. If the SSL Services Module VLAN is the same as the primary or secondary VLAN on the client or server, the SSL interface may drop the traffic coming from the private VLAN. (CSCdy86258)

- The SSL Services Module supports only one route per VLAN. If you add multiple routes using the **ssl-proxy vlan** command, only the last route entered is added. (CSCdy44647)
- Do not use any routing protocols on the SSL Services Module. Although you can configure the Routing Information Protocol (RIP), we do not recommend it. The module supports administrative VLAN for all management (non-SSL) traffic. (CSCdz23816)
- If ARP requests are sent at wire speed to the SSL Services Module, traceback messages are displayed that warn that the module is receiving heavy traffic in its control plane, which is not a normal condition. Avoid sending wire-speed traffic to a services module. (CSCdz36033)
- Operations affecting NVRAM (such as deleting a file or exporting a trustpoint to NVRAM) displays a message regarding downgrade compatibility. This message is similar to the message displayed after you enter the **copy system:running-config nvram:startup-config** command. (CSCea69515)
- The SSL Services Module is not Federal Information Processing Standards (FIPS) certified in SSL software release 1.*x*. or 2.*x*.
- If there is more than one level of certificate authority, only the lowest level certificate authority trustpoint that is authenticated and enrolled is exported in PEM files.

  Workaround: Export the enrolled trustpoint to a PKCS12 file. All levels of CA trustpoints in the certificate chain will be automatically included in the same file. (CSCea75462)
- The **clear ssl-proxy stats ssl** command does not clear the counters in the **max handshake conns** and the **max device q len** fields. The **clear ssl-proxy stats service backend-ssl** command does not clear the counters in the **valid sessions** field. These counters are running counters and are not meant to be cleared when you enter a **clear** command. (CSCeh70549)

Caveats

These sections describe open and resolved caveats in SSL software for all 2.1(x) software releases:

Open Caveats in Release 2.1(13)

There are no open caveats in SSL Services Module, software release 2.1(13).

Resolved Caveats in Release 2.1(13)

This section describes resolved caveats in SSL Services Module, software release 2.1(13):

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- Time zone information is not properly replicated to the SSLM. This can cause client certificate authentication requests to fail and display a ‘page not found’ error.

  Workaround: Configure the correct time zone on the SSLM. (CSCek44168)
- Authenticating sub-CA certificate stops the SSLM when the sub-CA certificate does not have a valid Certificate Revocation List (CRL) distribution point and the CRL validation is active in the root trustpoint.

  Workaround: Modify the root trustpoint to perform ‘crl optional’. (CSCek76329)
- Configuring Network Time Protocol (NTP) on the SSLM or the Content Switching Module with SSL (CSM-S) SSL daughtercard (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 SSLM. The daughtercard clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)
- SSL Connections are dropped.

  Workaround: Reboot the SSLM. (CSCsl63177)
- Unnecessary spaces in debug messages at times cause failures in regressions. (CSCsl72099)

  Workaround: None.
- SSL termination breaks traffic when header insert is turned on.

  Workaround: Modify the application behavior or turn header insert off. (CSCsl76911)
- The extended validation root certificate expiry is shown incorrect. (CSCsl92290)

Workaround: None.

- The session-id inserted into the cleartext HTTP header incorrectly contains all zeros at times.

  Workaround: Disable session cache or make the timeout long enough to be tolerable. (CSCso58537)

- New connections are responded to with an RST.

  Workaround: This might be a performance limitation. However, reboot the linecard if the count remains high after the reducing the system load. (CSCso09564)

- When the SSLM receives a TLS1.1 ClientHello message, the connection is closed. (CSCso60805)

  Workaround: None.

- When an http-header insertion policy is configured, WebDav requests do not work and the TCP connection stops.

  Workaround: Remove http-header insertion policy. (CSCsq48567)

- TCP Processor crashes with prefix wild-card url-rewrite.

  Workaround: Change the rewrite rule by configuring the prefix wildcard url-rewrite policy and rewrite the URL to contain a forward slash '/' or a carriage-return '\r' in it. (CSCsq57256)

- SSLM includes a session ID in the SSL ClientHello message when the SSLM is configured for backend encryption. (CSCsu42466)

  Workaround: None.

- If the client authentication is configured on the SSLM, and multiple SSL messages span multiple packets causing the SSL message length to span two buffers, then the length field is read incorrectly. The SSLM might fail an SSL handshake with an SSL handshake failure alert for some valid client certificates. (CSCsx15053)

  Workaround: Disable client authentication.

- When a prefix wildcard url-rewrite policy is configured, the TCP processor crashes. (CSCsx37391)

  Workaround: Change the rewrite rule.

- When a TCP or SSL processor crashes, no crash information is saved after reboot. (CSCsy05771)

  Workaround: None.

- SSLM does not forward XML data while using header insertion. SSLM recognizes "content-length" only when both C and L are capitalized or are in lowercase, but not a mix of uppercase and lowercase characters. (CSCsz18081)

  Workaround: Use only "content-length" or "Content-Length" in the header.

- When the TCP source port is reused by a BlueCoat proxy server directly after the connection is terminated, you are required to tune the default TIME_WAIT timer to a lower value than 16 to 32 seconds. See the "New and Changed Information" section on page 5. (CSCsy92231)

  Workaround: None.

- If the SSLM is rebooted after a processor stops due to an infinite loop in the software, the SSLM might reload unexpectedly. When it reboots, the SSLM does not provide any information about the crash in the **show ssl-proxy crash-info** log. (CSCsz97316)

  Workaround: None.

- Sometimes when the CRLs expire, a router using certificate revocation lists might restart due to a software-forced crash. (CSCsa63387)

  Workaround: None.

- For SSLM sustaining releases 3.1(4.4) and 3.1(4.5), all connections are reset by the SSLM after the configured TCP SYN timeout expires. This TCP SYN timeout defaults to 75 seconds and is configurable to any value between 05 and 75 seconds. (CSCtb63789)

  Workaround: None.

- When the chunked encoding trailer part is split across several application data records, HTTP requests using chunked encoding time out when going through the SSLM. (CSCtc45467)

  Workaround: Ensure final 0\r\n\r\n data bytes are all within the same record.

- The URL rewrite functionality does not work if the URL in the redirect is in upper case. For example, HTTP:. (CSCte19206)

  Workaround: Check for both lowercase and uppercase letters.

- In the SSLM 2.1.12(x) releases, while attempting to export a trustpoint, the following error is observed:

```
ssl-proxy(config)#crypto ca export <trustpoint_name>  pem terminal des <password>
% The specified trustpoint is not enrolled. Only enrolled trustpoints can be exported
in PEM format (<trustpoint_name>)
```

  Workaround: After reloading the SSLM using a **hw-module module** [slot] **reset**, you can export the trustpoint. (CSCtf17353)

- Cisco Content Services Switch (CSS), SSL Services Module (SSLM), and Application Control Engine (ACE) contain a vulnerability that could allow an authenticated, remote attacker to insert spoofed SSL headers into HTTP requests. See the "New and Changed Information" section on page 5.

  More details at http://tools.cisco.com/security/center/viewAlert.x?alertId=20807. (CSCti85702)

  Workaround: Cisco customers can obtain upgrades by contacting the Cisco Technical Assistance Center (TAC).

- The SSLM might randomly start failing SSL or TLS handshakes with either a handshake failure alert (SSL3) or and internal error alert (TLS1). (CSCtj13900)

- **Workaround**: Upgrade to a version of code that has the fix for this bug ID. If the problem persists, configure the **ssl-proxy device-check interval 20** command and monitor the output of the **show ssl-proxy stats ssl** command. See the "New and Changed Information" section on page 5.

Open Caveats in Release 2.1(12)

This section describes open caveats for the SSL Services Module, software release 2.1(12):

- Configuring Network Time Protocol (NTP) on the SSLM or the Content Switching Module with SSL (CSM-S) SSL daughtercard (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 SSLM. The daughtercard clock periodically synchronizes with the supervisor engine, so having NTP running on the supervisor engine is enough to keep the clock in synchronization. (CSCsg55214)

Resolved Caveats in Release 2.1(12)

This section describes resolved caveats in SSL Services Module, software release 2.1(12):

- When a URL-rewrite policy is configured with an asterisk (*), the SSLM will rewrite HTTP to HTTPS on nondefault (port 80) TCP ports. (CSCse28330)
- 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 the output display of the **show ssl-proxy stats hdr** command, the Service Errors counter is incremented when accessing a proxy service without an HTTP header policy. (CSCsd06143)
- When client certification and header insertion are enabled, and the client certificate contains UTF8-encoded non-ASCII characters, the ISSUER and SUBJECT fields are empty in the HTTP header from the SSLM to the back-end server.

  Workaround: Do not use UTF8-encoding in the client certificate. (CSCsk31737)
- 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)
- The **show ssl-proxy mac address** and **show ssl-proxy mac cpu-util** commands display incorrect results. (CSCsl28453)
- 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)

Open Caveats in Release 2.1(11)

This section describes open caveats for the SSL Services Module, software release 2.1(11):

- Configuring NTP on the SSLM or CSM-S SSL-DC may interfere with the clock synchronization. Configuring the CSM-S SSL-DC to synchronize its clock using NTP might lead to the clock going out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSLM. 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)

Resolved Caveats in Release 2.1(11)

This section describes resolved caveats in SSL Services Module, software release 2.1(11):

- After normal operation, the SSLM stops inserting the header into the clear text traffic. This problem occurs only with software release 2.1(10).

  Workaround: None. (CSCsh79045)

Open Caveats in Release 2.1(10)

This section describes open caveats for the SSL Services Module, software release 2.1(10):

- After normal operation, the SSLM stops inserting the header into the clear text traffic. This problem occurs only with SSL software release 2.1(10).

  Workaround: None.

- Configuring NTP on the SSLM or CSM-S SSL-DC may interfere with the clock synchronization. Configuring the CSM-S SSL-DC to synchronize its clock using NTP might lead to the clock going out of synchronization.

  Workaround: Do not configure NTP on the CSM-S SSL-DC or the SSLM. 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)

Resolved Caveats in Release 2.1(10)

This section describes resolved caveats in SSL Services Module, software release 2.1(10):

- 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 65K difference between the connection allocation counters and deallocation 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 header insert policy is used. (CSCsh30757)

Open Caveats in Release 2.1(9)

This section describes open caveats for the SSL Services Module, software release 2.1(9).

- After upgrading to SSL software release 2.1(5) or a later release, the SSL proxy service might remain in a down state with a "No Server/Next HOP MAC" reason, even though the server is reachable. This situation might occur after reload.

  Workaround: Remove the server IP addresses from the proxy service, and reconfigure the proxy service to restart the service. (CSCei12818)

- 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)

- 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.

  Workaround: Do one of the following:
  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)
- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate that belongs to one certificate authority and a router certificate that was issued by another certificate authority. (CSCea57072)
- For manual certificate enrollment, if the URL string ends with a slash (/) 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)
- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after you reboot the system, and the proxy service remains in the no cert state.

  Workaround: After you reboot the system, delete the trustpoint, and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)
- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)
- When you upgrade the image using the **copy tftp: pclc#***mod***-fs:** command, the command accepts any filename. You will not receive an image name validation when you upgrade the maintenance partition from the application partition or upgrade the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)
- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- 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)
- 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)

- 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 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message displays when a certificate is read from NVRAM when Cisco IOS software reboots, and it does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(9)

This section describes resolved caveats in SSL Services Module software release 2.1(9):

- The SSL Services Module 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. (CSCsd25820)
- If the SSL Services Module receives a misaligned TCP selective acknowledgment (SACK) option or a misaligned TCP timestamp option, the module might reload. (CSCee35357)

Open Caveats in Release 2.1(8)

This section describes open caveats for the SSL Services Module, software release 2.1(8).

- After upgrading to SSL software release 2.1(5) or a later release, the SSL proxy service might remain in a down state with a "No Server/Next HOP MAC" reason, even though the server is reachable. This situation might occur after reload.

  Workaround: Remove the server IP addresses from the proxy service, and reconfigure the proxy service to restart the service. (CSCei12818)
- 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)

- 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.

  Workaround: Do one of the following:
  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)
- 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)
- 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:
  1. Copy the "crypto ca trustpoint *trustpoint_label*" and "crypto ca certificate chain *name*" information from the running configuration.
  2. Delete the trustpoint by entering the **no crypto ca trustpoint** *trustpoint_label* command.
  3. 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate that belongs to one certificate authority and a router certificate that was issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after you reboot the system, and the proxy service remains in the no cert state.

  Workaround: After you reboot the system, delete the trustpoint, and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When you upgrade the image, the **copy tftp: pclc#*mod*-fs:** command accepts any filename. You will not receive an image name validation when you upgrade the maintenance partition from the application partition or upgrade the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)
- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- 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)
- 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)
- 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 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message displays when a certificate is read from NVRAM when Cisco IOS software reboots, and it does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(8)

This section describes resolved caveats in SSL Services Module software release 2.1(8):

- When you add HTTP header insert policies to an SSL proxy service, the SSL Services Module 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. (CSCej38531)
- When you configure a client proxy, the SSL Services Module 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. (CSCsc26099)

- If you configure the SSL Services Module 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 SSL Services Module, the buffer overflows and the SSL Services Module resets. (CSCsb77689)
- When you configure URL rewrite, the SSL Services Module scans the response from the server. Currently, the entire response (headers and data) is scanned, which leads to a drop in performance. (CSCej33386)

Open Caveats in Release 2.1(7)

This section describes open caveats for the SSL Services Module, software release 2.1(7).

- After upgrading to SSL software release 2.1(5) or a later release, the SSL proxy service might remain in a down state with a "No Server/Next HOP MAC" reason, even though the server is reachable. This situation might occur after reload.

  Workaround: Remove the server IP addresses from the proxy service, and reconfigure the proxy service to restart the service. (CSCei12818)

- 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)

- 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.

  Workaround: Do one of the following:
  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- 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.

Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)
- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate that belongs to one certificate authority and a router certificate that was issued by another certificate authority. (CSCea57072)
- For manual certificate enrollment, if the URL string ends with a slash (/) 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)
- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after you reboot the system, and the proxy service remains in the no cert state.

  Workaround: After you reboot the system, delete the trustpoint, and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)
- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)
- When you upgrade the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. You will not receive an image name validation when you upgrade the maintenance partition from the application partition or upgrade the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)
- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module; however, the CLI is available. (CSCdz24446)
- The module might take longer to boot up 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)
- 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. (CSCdz03802)

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM.
- 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. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)
- 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM when Cisco IOS software reboot, and it does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(7)

This section describes resolved caveats in SSL Services Module software release 2.1(7):

- Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  More details can be found in the security advisory which posted at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml

  This problem is resolved in SSL software release 2.1(7). (CSCee45312)
- When you configure a gateway for a VLAN on the SSL Services Module, the module incorrectly responds to PROXY ARP, even though the module is not a router for that network. Hosts on that network use the SSL Services Module to route traffic through the network. If the traffic is not intended for the SSL Services Module, the SSL Services Module drops the packet.

  Workaround: Do not configure a gateway for a network that has hosts other than the server.

  This problem is resolved in SSL software release 2.1(7). (CSCsb09471)
- The SSL Services Module might stop responding and accepting connections if you run an application such as Telnet or secure Telnet and you use the application to perform file transfer operations that generate 1 to 2 byte packets on the wire.

  Workaround: Reboot the SSL Services Module.

  This problem is resolved in SSL software release 2.1(7). (CSCei45351)

- The SSL Services Module increases the "TOS invalid" counter (as shown in the output of the **show ssl-proxy stats tcp** command) when it receives packets that are set with a DSCP bit, but the module does not drop the packets. The packets are sent to destination correctly. This issue is not seen when the TOS carry over feature is not enabled.

  This problem is resolved in SSL software release 2.1(7). (CSCsb51510)

- Clients using duplicate SRC ports through the SSL Services Module might experience delays (up to 30 seconds) when establishing a backend connection to the real server.

  This problem is resolved in SSL software release 2.1(7). (CSCei58807)

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically reestablished. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in SSL software release 2.1(7). (CSCed27956, CSCed38527

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the Centre for the Protection of Nattional Infrastructure (CPNI), based in the United Kingdom. CPNI is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/

This problem is resolved in SSL software release 2.1(7). (CSCef60659, CSCed78149)

- When session cache is enabled, the SSL Services Module uses the same session ID when communicating with the backend SSL server, even if the server responds with a new session ID.

  Workaround: Clear session cache to force a new handshake if new session is wanted.

  This problem is resolved in SSL software release 2.1(7). (CSCej02272)

- When you configure a policy with HTTP header insertion and apply the policy to an SSL proxy client service, connections to the SSL Services Module might fail. This problem only happens if the header is split across SSL records.

  This problem is resolved in SSL software release 2.1(7). (CSCei46148)

Open Caveats in Release 2.1(6)

This section describes open caveats for the SSL Services Module, software release 2.1(6).

- After upgrading to SSL software release 2.1(5) or a later release, the SSL proxy service might remain in a down state with a "No Server/Next HOP MAC" reason, even though the server is reachable. This situation might occur after reload.

  Workaround: Remove the server IP addresses from the proxy service, and reconfigure the proxy service to restart the service. (CSCei12818)

- 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)

- 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.

Workaround: Do one of the following:

- Stabilize the real server so that it is reachable.
- If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate that belongs to one certificate authority and a router certificate that was issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after you reboot the system, and the proxy service remains in the no cert state.

  Workaround: After you reboot the system, delete the trustpoint, and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When you upgrade the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. You will not receive an image name validation when you upgrade the maintenance partition from the application partition or upgrade the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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 the 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)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)
- 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM when Cisco IOS software reboot, and it does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(6)

This section describes resolved caveats in SSL Services Module software release 2.1(6):

- Client-certificate-header insertion might not function with the Internet Explorer web browser when a server certificate has a problem that requires confirmation from the end user (for example, if the site names do not match or if the certificate has expired). When this problem occurs, the browser closes the connection and the SSL Services Module flushes the received client certificate buffer. When the browser resumes the session, the SSL Services Module no longer has the client certificate information.

  Workaround: Make sure SSL Services Module server certificate has the correct content.

  This problem is resolved in SSL software release 2.1(6). (CSCeh59216)
- After some time of running load test, SSL Services Module does not close the connection with the backend (HTTP) server and keeps the server in a CWAIT state (server sent FIN) and the client side connection remains in a FWAIT2 state until the server times out (75 seconds). Current server connections increase, which leads to a drop in performance.

  This problem is resolved in SSL software release 2.1(6). (CSCeh90683)
- URL rewrite fails when the location field spans multiple packets.

  This problem is resolved in SSL software release 2.1(6). (CSCeh76350)
- You are incorrectly allowed to delete a policy while it is applied to an active SSL proxy service, for example:

  - If you delete a URL-rewrite policy that is applied to an active SSL proxy service, the policy still shows up in the proxy service. Traffic that would have matched the policy now fails.
  - If you delete an HTTP-header insertion policy that is applied to an active proxy service, all rules within the policy are deleted. The policy is still configured and applied to the proxy service. There is no warning that advises that the policy has been applied to an active proxy service.

  Once in this condition, you need to recreate the policy and then delete it. To avoid this condition, make sure you remove the policy from all proxy services prior to deleting the policy.

  This problem is resolved in SSL software release 2.1(6). (CSCeh69068)

- Client authentication fails when the CA pool contains 16 trustpoints. The 16th trustpoint is not transmitted, and the SSL hand shake fails to complete.

  Workaround 1: Remove the 16th trustpoint from the CA pool.

  Workaround 2: Reboot the client's PC.

  This problem is resolved in SSL software release 2.1(6). (CSCeh79938)

- The SSL Services Module might crash when client-certificate header insertion is enable and the client certificate has a large binary certificate field.

  This problem is resolved in SSL software release 2.1(6). (CSCeh74334)

- If you reenroll an existing trustpoint using the terminal option, both the old and the new router certificates are displayed. The router does not replace the existing certificate. The router keeps the old certificate along with new certificate. This condition causes the router to use the old certificate instead of the new certificate.

  Workaround: Refresh the private key by entering the **crypto key generate rsa** command before enrolling. If you have already imported the new certificate, you need to delete the current trustpoint and then recreate it using the new certificate. (When you delete a trustpoint, you delete the certificates associated with the trustpoint but not the private key.)

  This problem is resolved in SSL software release 2.1(6). (CSCee04732)

- Terminal enrollment does not work for usage keys.

  This problem is resolved in SSL software release 2.1(6). (CSCee82109)

- The fully qualified domain name (FQDN) of a certificate that is obtained from a certificate authorithy (CA) during enrollment may be incorrect. If the hostname or domain name changes between the time you define a CA and enroll with the CA, the certificate may incorrectly include the old hostname or domain name. Also, if a FQDN is specified in trustpoint configuration mode and the default RSA key is used for enrollment, the FQDN of the default RSA key label incorrectly overrides the one specified. The certificate incorrectly includes the FQDN of the RSA key label. When a named RSA key pair is configured, the FQDN configuration in the trustpoint is reset.

  Workaround: If the hostname or domain name is changed after creating the trustpoint, and before enrolling with the trustpoint, remove and recreate the trustpoint to include the new hostname or domain name in the certificate. There is no workaround when using the default RSA key and specifying the FQDN in trustpoint configuration mode. The resulting certificate incorrectly contains the FQDN of the default RSA key label and not the specified FQDN.

  This problem is resolved in SSL software release 2.1(6). (CSCeh08333)

- HTTP header insertion might fail if the terminating carriage return line feed (CRLF) of the last header field and the empty line following the CRLF spans two packets. This problem is seen in rare situations where the HTTP header is unusally large (around 1500 bytes) or when the client is inefficiently breaking up the requests into small packets.

  This problem is resolved in SSL software release 2.1(6). (CSCeh96314)

- The SSL Services Module does not answer to new connections. Existing connections still work.

  Workaround: Suspend the SSL Services Module and then put it back in service.

  This problem is resolved in SSL software release 2.1(6). (CSCeh46227)

- When you import a new certificate that is issued by a renewed CA, you might not be able to succesfully import a PKCS12 file if the new CA certificate has the same subject name, but a different serial number, as the old CA certificate.

  Workaround: Convert the PKCS12 file to PEM format and import the PEM file.

  This problem is resolved in SSL software release 2.1(6). (CSCeh84541)

- The proxy service might not work after you import renewed certificates and reload. This happens when the renewed CA certificate has the same subject name as the old CA certificate.

  Workaround: Unassociate the proxy service with the trustpoint (**no certificate rsa general-purpose truspoint** *trustpoint_label*), delete the trustpoint (**no crypto ca trustpoint** *trustpoint_label*), and then reimport the trustpoint (**crypto ca import** *trustpoint_label* **pem**).

  This problem is resolved in SSL software release 2.1(6). (CSCeh91197)

- If you associate an SSL proxy service with a CA pool that does not exist, the proxy service goes into a down state with a "CA pool" reason.

  Workaround: Make sure the CA pool is configured before assigning it to the proxy service.

  This problem is resolved in SSL software release 2.1(6). (CSCeg44221)

Open Caveats in Release 2.1(5)

This section describes open caveats for the SSL Services Module, software release 2.1(5).

- 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)

- The SSL Services Module with a virtual TCP policy 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.

  Workaround: Do one of the following:

  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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 the 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate that belongs to one certificate authority and a router certificate that was issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after you reboot the system, and the proxy service remains in the no cert state.

  Workaround: After you reboot the system, delete the trustpoint, and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When you upgrade the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. You will not receive an image name validation when you upgrade the maintenance partition from the application partition or upgrade the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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. (CSCdz03802)

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode, and save the certificates in the NVRAM.
- 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. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)
- 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM when Cisco IOS software reboot, and it does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(5)

This section describes resolved caveats in SSL Services Module, software release 2.1(5):

- If you configure the SSL Services Module 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 SSL Services Module, the buffer overflows, and the SSL Services Module resets.

  This problem is resolved in SSL software release 2.1(5). (CSCsa75762)

- 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). (CSCef67472)

- 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). (CSCsa57669)

- 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). (CSCeh26040, CSCeh14851)

- 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). (CSCeh19256)

- 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). (CSCeh20306)

- 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). (CSCeh21346)

Open Caveats in Release 2.1(4)

This section describes open caveats for the SSL Services Module, 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) in the request.

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

- The SSL Services Module with a virtual TCP policy 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 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.

  Workaround: Do one of the following:

  – Stabilize the real server so that it is reachable.

  – If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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 the 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- Windows 2000 certificate authorities occasionally reject certificate enrollment requests 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the no cert state.

  Workaround: After rebooting, delete the trustpoint and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When upgrading the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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 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 the 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)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)
- 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(4)

This section describes resolved caveats in SSL Services Module, software release 2.1(4):

- When you enter the **show memory** *address* command (for example, **show memory 0xb0061aa0**), the SSL module may reset.

  This problem is resolved in SSL software release 2.1(4). (CSCed60513, CSCef74600)
- When an underscore character (_) is included in the Subject Name of a certificate for an SSL Services Module, the certificate and the subsequent global configuration may not be saved properly to the NVRAM. When the SSL Services Module is reloaded under these circumstances, the certificate is lost, and parsing the subsequent global configuration by the configuration parser results in an error.

  Workaround: Avoid using the underscore character in the fully qualified domain name (FQDN) of the certificate for the SSL Services Module.

  This problem is resolved in SSL software release 2.1(4). (CSCef40048)
- If you configure the SSL Services Module 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 SSL Services Module, the buffer overflows and the SSL Services Module resets.

  This problem is resolved in SSL software release 2.1(4). (CSCef67907)
- When you configure the SSL Services Module for back-end encryption, the SSL Services Module does not resume SSL sessions with Microsoft Internet Information Services (IIS) servers. The IIS servers do not send SSL close_notify alerts before closing the connection. The SSL Services Module clears the session, and that session cannot be reused.

  This problem is resolved in SSL software release 2.1(4). (CSCef65980)
- The SSL Services Module might reload if you remove the TACACS+ host configuration before you remove the server configuration.

  Workaround: Remove the server configuration before you remove TACACS+ host configuration.

  This problem is resolved in SSL software release 2.1(4). (CSCef93179)

- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  The advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in SSL software release 2.1(4). (CSCef46191)

- The following error message may be displayed on the console:

```
*Mar  1 00:02:31.127: %SCHED-3-THRASHING: Process thrashing on watched boolean 'CSM
IPC Watch Bool'.
-Process= "CSM IPC I/O Process", ipl= 5, pid= 25
-Traceback= 5233E8 5234CC 5C01AC
```

  This error message results from the way that Boolean messages are processed in the loop. If the loop exits before it has processed all the messages in the queue, the message is displayed. The module reenters the loop again, and the problem fixes itself once bootup is complete.

  This problem is resolved in SSL software release 2.1(4). (CSCed10910)

- The SSL Services Module might reset if a client certificate header insertion request exceeds the size of the first buffer (1460 bytes) on the module.

  Workaround: Disable client certificate header insertion.

  This problem is resolved in SSL software release 2.1(4). (CSCeg36221)

- With header insertion enabled, the SSL Services Module might reload if a cookie larger than 8000 bytes is inserted by the server and returned by the client.

  Workaround: Disable header insertion.

  This problem is resolved in SSL software release 2.1(4). (CSCeg43173)

Open Caveats in Release 2.1(3)

This section describes open caveats for the SSL Services Module, software release 2.1(3).

- When you enter the **show memory** *address* command (for example, **show memory 0xb0061aa0**), the SSL module may reset. (CSCed60513)

- 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) in the request.

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

- The SSL Services Module with a virtual TCP policy 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 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.

  Workaround: Do one of the following:
  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- 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 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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 the 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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- Windows 2000 certificate authorities occasionally reject certificate enrollment requests 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the no cert state.

  Workaround: After rebooting, delete the trustpoint and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When upgrading the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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 reboot. (CSCdz03802)

- **Workaround**: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode and save the certificates in the NVRAM.

- 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. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)

- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)

- 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)

- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)

- 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 Release 2.1(3)

This section describes resolved caveats in SSL Services Module, software release 2.1(3):

- The output of the **show tech** command does not include system crash information or SSL proxy service information.

  This problem is resolved in SSL software release 2.1(3). (CSCed75777)

- When you configure an HTTP header policy, the SSL Services Module might truncate or corrupt HTTP POST variables in the decrypted traffic.

  Workaround: Remove the HTTP header policy from the SSL proxy service.

  This problem is resolved in SSL software release 2.1(3).(CSCef30438)

- After you successfully export a trustpoint in PEM format, no information is displayed regarding the status of the exported PEM file.

  This problem is resolved in SSL software release 2.1(3). (CSCea69469)

- The URL rewrite feature rewrites the protocol and the nondefault port (default ports are port 80 for cleartext and port 443 for SSL). However, if a server sends a location URL that specifies the default cleartext port (for example, http://www.cisco.com:80), the SSL Services Module incorrectly rewrites the protocol as https://www.cisco.com:80. Also, if a server sends a location URL that specifies the default SSL port (for example, https://www.cisco.com:443), the SSL Services Module incorrectly rewrites the protocol as http://www.cisco.com:443. Secure HTTP (https://) cannot use port 80, and HTTP (http://) cannot use port 443.

  Workaround: Specify a different (nondefault) port on the server (for example, 81 or 444).

  This problem is resolved in SSL software release 2.1(3). (CSCef45069)

- The certificate revocation list (CRL) lookup fails during certificate authentication when a peer certificate is signed by a subordinate certificate authority and when the SSL Services Module receives only a peer certificate or a partial certificate chain. The following debug message displays if you enter the **debug crypto pki transactions** command:

  ```
  CRYPTO_PKI: status = 1872: failed to verify CRL signature
  ```

  Workaround 1: When declaring the trustpoint, enter the **crl optional** command option for all relevant subordinate certificate authority and root certificate authority.

  Workaround 2: Ensure that the peer application sends the full certificate chain.

  Workaround 3: Ensure that the peer certificate is signed by the root certificate authority.

  This problem is resolved in SSL software release 2.1(3). (CSCee74850)

- An HTTP POST request from a client using a Mozilla-based browser does not contain the end-of-header marker (\r\n\r\n) in the first buffer of the request. The SSL Services Module is unable to insert the header.

  This problem is resolved in SSL software release 2.1(3). (CSCef64660)

- When you enter the **crypto ca import** command to import a certificate and a private key, and the public key in the certificate does not match the private key, the SSL Services Module allows the import process to succeed. When the public key and private key do not match, the SSL Services Module should report an error and the import process should fail.

  Workaround: Locate the matching private key and certificate. Remove the mismatched trustpoint and reimport the matching key and certificate.

  This problem is resolved in SSL software release 2.1(3). (CSCee78711)

Open Caveats in Release 2.1(2)

This section describes open caveats for the SSL Services Module, software release 2.1(2).

- When you enter the **show memory** *address* command (for example, **show memory 0xb0061aa0**), the SSL module may reset. (CSCed60513)
- The certificate revocation list (CRL) lookup fails during certificate authentication when a peer certificate is signed by a subordinate certificate authority and when the SSL Services Module receives only a peer certificate or a partial certificate chain. The following debug message displays if you enter the **debug crypto pki transactions** command:

  ```
  CRYPTO_PKI: status = 1872: failed to verify CRL signature
  ```

  Workaround 1: When declaring the trustpoint, enter the **crl optional** command option for all relevant subordinate certificate authority and root certificate authority.

  Workaround 2: Ensure that the peer application sends the full certificate chain.

  Workaround 3: Ensure that the peer certificate is signed by the root certificate authority.

  (CSCee74850)
- 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) in the request.

  Workaround: Save the configuration and reset the SSL Services Module. (CSCin67360)
- The SSL Services Module with a virtual TCP policy 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 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.

  Workaround: Do one of the following:
  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)
- 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 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

  Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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 could 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. (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)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- Windows 2000 certificate authorities occasionally reject certificate enrollment requests 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the no cert state. (CSCdz20220)

  Workaround: After rebooting, delete the trustpoint and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate.

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When upgrading the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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 reboot. (CSCdz03802)

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

- 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. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)
- 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)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)
- 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 Release 2.1(2)

This section describes resolved caveats in SSL Services Module, software release 2.1(2):

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically reestablished. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml,

  and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in SSL software release 2.1(2). (CSCee35285)
- When an SSL proxy service is configured to offload mail applications, some of the mail connections might fail. The SSL Services Module drops the initial greeting sent by the mail server, which causes the client mail application to fail. This problem does not apply to HTTP applications.

  This problem is resolved in SSL software release 2.1(2). (CSCee56105)
- The SSL Services Module resets during the SSL handshake phase when the size of the server certificate or certificate chain is a multiple of 1568 bytes (for example, 1568, 3136, 4704, etc.).

  Workaround: Change the certificate size by altering some fields in the certificate.

This problem is resolved in SSL software release 2.1(2). (CSCee50197)

- Before copying the application partition (AP) or maintenance partition (MP) image, the **copy** command checks to see if there is enough space in the root file system of the destination device for the image. However, the root file system is not the actual destination directory. If the file being copied is larger than the amount of space available in the root file system, the check fails and the image is not copied.

  This problem is resolved in SSL software release 2.1(2). (CSCee29521)

- 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.

  This problem is resolved in SSL software release 2.1(2). (CSCin67360)

- Some client certificate headers contain a null character at the end of the header. This character is accepted by some HTTP servers, such as the Apache server, but not others, such as the Microsoft IIS.

  Workaround: If the HTTP server rejects the HTTP Get request, disable the client certificate header insertion configuration.

  This problem is resolved in SSL software release 2.1(2). (CSCee42149)

- The TCP stack on the SSL Services Module does not support selective acknowledgement (SACK). If the module receives a packet that has the SACK option bit set in the ESTABLISHED state, the module resets.

  This problem is resolved in SSL software release 2.1(2). (CSCee37232)

- Under the following conditions, the SSL Services Module might be unable to complete back-end SSL connections:

  a. A server sends Server Hello and Certificate in the same TCP segment.

  b. The certificate is large enough that it spans multiple TCP segments.

  The problem occurs while establishing the SSL connection, when the server responds to the Client Hello from the SSL Services Module.

  This problem is resolved in SSL software release 2.1(2). (CSCee10836)

- The SSL Services Module might stop sending traffic. There is no software reset. The output from the **show ssl-proxy crash-info** command shows high values for "TCP data buffers used." These values do not decrease.

  Workaround: Reset the SSL Services Module to release the TCP buffers.

  This problem is resolved in SSL software release 2.1(2). (CSCee00803)

- When the SSL Services Module interacts with TCP clients, the module might not correctly parse TCP options that involve NOP (no operation), which can cause the module to reset.

  This problem is resolved in SSL software release 2.1(2). (CSCed77870)

- The SSL Services Module discards client and server traffic if the IP address validation check fails after the module applies a local subnet mask to the destination IP address of the received packet.

  Workaround: Configure the SSL proxy VLAN with the lowest subnet mask to receive traffic, or configure the SSL proxy VLAN where traffic is received to the lowest subnet mask.

This problem is resolved in SSL software release 2.1(2). (CSCed77583)

- When the SSL Services Module configuration contains an expired certificate authority certificate, the module resets after downloading the certificate revocation list (CRL).

  Workaround: Remove expired certificate authority certificates from the configuration.

  This problem is resolved in SSL software release 2.1(2). (CSCin70309)

- When redundant SSL Services Modules share similar configurations in a system with a Content Switching Module, connectivity issues occur with Internet Explorer.

  Workaround 1: Remove the SSL proxy MAC address information from the running configuration on both SSL Services Modules, and then save the configuration and reload.

  Workaround 2: Configure a unique MAC address on each SSL Services Module.

  This problem is resolved in SSL software release 2.1(2). (CSCee11932)

- The SSL Services Module might reset when high traffic loads are sent to SSL client proxies only. The module does not reset when traffic is sent to both client proxies and server proxies.

  This problem is resolved in SSL software release 2.1(2). (CSCee12382)

Open Caveats in Release 2.1(1)

This section describes open caveats for the SSL Services Module, software release 2.1(1).

- When you enter the **show memory** *address* command (for example, **show memory 0xb0061aa0**), the SSL module may reset. (CSCed60513)

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically reestablished. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml,

  and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml. (CSCee35285)

- The SSL Services Module with a virtual TCP policy 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 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.

  Workaround: Do one of the following:

  - Stabilize the real server so that it is reachable.
  - If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- When the SSL Services Module configuration contains an expired certificate authority certificate, the module resets after downloading the certificate revocation list (CRL).

  Workaround: Remove expired certificate authority certificates from the configuration. (CSCin70309)

- 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 certificate revocation list (CRL) lookup fails during certificate authentication when a peer certificate is signed by a subordinate certificate authority and when the SSL Services Module receives only a peer certificate or a partial certificate chain. The following debug message displays if you enter the **debug crypto pki transactions** command:

  ```
  CRYPTO_PKI: status = 1872: failed to verify CRL signature
  ```

  Workaround 1: When declaring the trustpoint, enter the **crl optional** command option for all relevant subordinate certificate authority and root certificate authority.

  Workaround 2: Ensure that the peer application sends the full certificate chain.

  Workaround 3: Ensure that the peer certificate is signed by the root certificate authority.

  (CSCee74850)

- 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. (CSCin67360)

- On systems that are running Catalyst operating software on the supervisor engine and are configured with high availability, if you reset the SSL Services Module after a switch over, 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 add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

  ```
  GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
  ```

  The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

Workaround: Do not enter a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint. (CSCed33492)

- 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*" 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 could 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 you renew all the 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 the certificate has the correct extension (for example, basic constraint) before importing it to the module. (CSCed14070)

- Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system. (CSCea48145)

- Windows 2000 certificate authorities occasionally reject certificate enrollment requests 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.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)

- 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 authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a slash (/) 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)

- If you import a key pair and a self-signed certificate from a PKCS12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the no cert state. (CSCdz20220)

  Workaround: After rebooting, delete the trustpoint and import the PKCS12 file again. The proxy service automatically reinstalls the self-signed certificate.

- Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.

  Workaround: Copy the configuration file to the running configuration, or import the certificate with the key pair using a PKCS12 file. (CSCdz63758)

- When upgrading the image, the **copy tftp: pclc#***mod***-fs:** command accepts any filename. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

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

- The module might take longer to boot up 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)

- 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 reboot. (CSCdz03802)

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

- 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. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)

- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a "down" state and then go into an "up" state. (CSCdy77843)

- 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)

- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)

- 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 switch over (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 Release 2.1(1)

This section describes resolved caveats in SSL Services Module, software release 2.1(1):

- TACACS authentication is not supported in SSL Services Module.

  This problem is resolved in SSL software release 2.1(1). (CSCea76618)

- On systems running Catalyst operating software on the supervisor engine, you might not be able to session to the SSL module, and the module might not recover from a software reset.

  This problem is resolved in SSL software release 2.1(1). (CSCeb17020)

- Making a Telnet connection from supervisor engine console to the administration VLAN IP address on the SSL module does not work. This problem exists in SSL software 1.1(1) and 1.2(1).

  Workaround 1: Enter the **session slot** *slot-number* **proc 1** command to session from the supervisor engine console to the SSL module.

  Workaround 2: On the MSFC, enter the **ip telnet tos 0** command. You can then make a Telnet connection to the SSL Services Module.

  This problem is resolved in SSL software release 2.1(1). (CSCdy81460)

- The output from the **show ssl-proxy stats ssl** command shows the overload drops counter incrementing even though the SSL module is not overloaded. The SSL module then rejects all connections. This situation occurs if the SSL record header spans across multiple TCP segments.

  This problem is resolved in SSL software release 2.1(1). (CSCeb83024)

- When you run the cryptographic self-test, run-time performance is impacted. Run the self-test to troubleshoot persistent failures in cryptographic operations. When you finish troubleshooting, stop the test. If you run the cryptographic self-test continuously for more than three days, the system could exhaust memory and fail to set up new connections or forward traffic under heavy loads.

  Workaround: Reboot the system to regain the memory.

  This problem is resolved in SSL software release 2.1(1). (CSCed39184)

Documentation Updates

This section describes updates to the product documentation. These changes will be included in the next update to the documentation.

Changes

The [**no**] **nagle** subcommand was added to the **ssl-proxy policy tcp** command in SSL software release 2.1(8). Refer to the *Catalyst 6500 Series SSL Services Module Configuration Note, 2.1* and the *Catalyst 6500 Series SSL Services Module Command Reference, 2.1* for details regarding the use of this subcommand.

The **tls-rollback** [**current** | **any**] and **cert-req empty** subcommands were added to the **ssl-proxy policy ssl** command in SSL software release 2.1(5). Refer to the *Catalyst 6500 Series SSL Services Module Configuration Note, 2.1*, and the *Catalyst 6500 Series SSL Services Module Command Reference, 2.1*, for details regarding the use of these subcommands.

The **tos carryover** subcommand was added to the **ssl-proxy policy tcp** command in SSL software release 2.1(4) . Refer to the *Catalyst 6500 Series SSL Services Module Configuration Note, 2.1*, and the *Catalyst 6500 Series SSL Services Module Command Reference, 2.1*, for details regarding the use of this subcommand.

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.