



Release Notes for Catalyst 6500 Series Switch SSL Services Module Software Release 3.x

Current Release: 3.1(4)—July 18, 2008

Previous releases: 3.1(1), 3.1(2), 3.1(3)

The SSL Services Module (SSLM) 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 3.x.



Note

For detailed installation and configuration procedures for the SSL Services Module, refer to the Cisco Services Modules documentation at this URL:

http://www.cisco.com/en/US/products/hw/modules/ps2706/tsd_products_support_series_home.html

Contents

This document consists of these sections:

- [System Requirements, page 2](#)
- [Features, page 3](#)
- [Upgrading from a Previous Software Release, page 4](#)
- [New and Changed Information, page 5](#)
- [Limitations and Restrictions, page 9](#)
- [Caveats, page 10](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation and Submitting a Service Request, page 28](#)



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

© 2005—2008 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for the Catalyst 6500 series SSL Services Module software release 3.x:

- [Hardware Requirements, page 2](#)
- [Software Requirements, page 2](#)

Hardware Requirements

The Catalyst 6500 series SSL Services Module is supported in systems with a Supervisor Engine 2 with an MSFC2, a Supervisor Engine 32 with an MSFC2A, or a Supervisor Engine 720 with an MSFC3, and any module with ports that connect server and client networks.

Software Requirements


Note

Support for the SSL Services Module is removed in Cisco IOS Software Release 12.2(33)SXH and later releases.


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 releases supported by Catalyst operating system and Cisco IOS software.

Table 1 *SSL Software Compatibility*

Product Number	Minimum SSL Software Release		Recommended SSL Software Release		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	3.1(4)	2.1(1)	12.2(17a)SX1	8.2(1)
					12.2(14)SX1	–
WS-SVC-SSL-1 with Supervisor Engine 32	3.1(1)	2.1(1)	3.1(4)	2.1(1)	12.2(18)SXF	–
WS-SVC-SSL-1 with Supervisor Engine 2	1.2(2)	1.2(1) ¹	3.1(4)	2.1(1)	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 releases and applicable ordering information for the SSL software.

Table 2 **Orderable Software Images**

Software Release	Filename	Orderable Product Number
3.1(4)	c6svc-ssl-k9y9.3-1-4.bin	SC-SVC-SSL-3.1.4-K9
3.1(3)	c6svc-ssl-k9y9.3-1-3.bin	SC-SVC-SSL-3.1.3-K9
3.1(2)	c6svc-ssl-k9y9.3-1-2.bin	SC-SVC-SSL-3.1.2-K9
3.1(1)	c6svc-ssl-k9y9.3-1-1.bin	SC-SVC-SSL-3.1.1-K9

Features

The list of features can be found in the following sections:

- [New Features in Software Release 3.1, page 3](#)
- [Features in Software Release 1.x and 2.x, page 4](#)

New Features in Software Release 3.1



Note

See the “[Upgrading from a Previous Software Release](#)” section on page 4 for information about upgrading from a previous SSL software release to SSL software release 3.x.

This section describes the new features available in SSL software release 3.1:

- Support for Supervisor Engine 32 with MSFC2A
- Virtualization with VPN routing and forwarding (VRF)
- Support for non-HTTP protocols (LDAP, IMAP, Telnet, POP)
- Online Certificate Status Protocol (OCSP)
- Nonstop forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy on the supervisor engine
- Support for additional Cipher suites:
 - SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
 - SSL_RSA_EXPORT_WITH_RC4_40_MD5
 - SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
 - SSL_RSA_EXPORT1024_WITH_RC4_56_MD5
 - SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
 - SSL_RSA_WITH_NULL_MD5
- Session renegotiation
- Protected key storage

- TCP health probe
- Support for SSHv2
- Enhancements to HTTP header insertion:

Client certificate	Adds the following fields: <ul style="list-style-type: none"> • ClientCert-X509v3-Key-Usage • ClientCert-X509v3-Subject-Alternative-Name • ClientCert-X509v3-CRL-Distribution-Points • ClientCert-X509v3-Authority-Information-Access
Client certificate in PEM format	Inserts the entire client certificate in PEM format.
Session header	Adds the following fields: <ul style="list-style-type: none"> • Session-Step-Up • Session-Initial-Cipher-Name • Session-Initial-Cipher-Key-Size • Session-Initial-Cipher-Use-Size
Header alias	Allows you to create an alias for the standard name of the header so that the same value is passed using the aliased name instead of the standard name that the SSL Services Module sends.

Features in Software Release 1.x and 2.x

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

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/1.2/release/notes/OL_3396.html

For a complete list of features for SSL software releases 2.x, refer to the *Release Notes for Catalyst 6500 Series SSL Services Module Software Release 2.x* at this URL:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/release/notes/OL_5277.html

Upgrading from a Previous Software Release



Note

SSL software release 3.1 introduces many features that require an automatic configuration conversion when upgrading from release 1.x or 2.x. Before you upgrade to SSL software release 3.1 from an earlier release, we recommend that you save your current configuration.



Caution

If you downgrade to a 1.x or 2.x software release after you install SSL software release 3.x, you will lose your configuration. In addition, you will need to reinstall your certificates and keys.

When you upgrade from SSL software release 1.x or 2.x to SSL software release 3.x, the following conversions are made automatically to your configuration:

- The proxy service is added to a default context (Default).
After this conversion, you can configure more contexts and assign them to different enterprises.
- The SSL proxy VLAN configurations are converted to a subinterface configurations.
- The crypto CA configurations are converted to crypto PKI configurations.
- The CRL configurations are converted to revocation check configurations.

Table 3 shows the configuration changes between an SSL 2.1 configuration and an SSL 3.1 configuration.

Table 3 Configuration Changes Between Versions

SSL 2.1 Configuration	SSL 3.1 Configuration
<pre>ssl-proxy service s2 client virtual ipaddr 10.10.0.15 protocol tcp port 80 server ipaddr 10.0.207.203 protocol tcp port 443 nat client n1 authenticate verify all inservice ! crypto ca trustpoint tp1 crl optional ! crypto ca certificate chain tp1 certificate 10 nvram:ca-root#10.cer certificate ca 01 nvram:ca-root#01.cer ! ssl-proxy vlan 2 ipaddr 10.122.0.6 255.0.0.0 gateway 10.0.100.1 route 0.0.0.0 255.255.255.0 gateway 207.0.100.1 admin</pre>	<pre>ssl-proxy context Default maxconns 65536 ! service s2 client virtual ipaddr 10.10.0.15 protocol tcp port 80 server ipaddr 10.0.207.203 protocol tcp port 443 nat client n1 authenticate verify all inservice ! crypto pki trustpoint tp1 revocation-check none ! crypto pki certificate chain tp1 certificate 10 nvram:ca-root#10.cer certificate ca 01 nvram:ca-root#01.cer ! interface SSL-Proxy0.2 encapsulation dot1q 2 ip address 10.122.0.6 255.0.0.0 ! ip route 0.0.0.0 255.255.255.0 207.0.100.1</pre>

New and Changed Information

This section describes changes in configuration commands and messages.

- [Changes in Software Release 3.1\(4\), page 5](#)
- [Changes in Software Release 3.1\(3\), page 7](#)

Changes in Software Release 3.1(4)

The following changes are introduced in SSL software release 3.1(4):

- The **mac-address** interface configuration command is removed. To change the MAC address, enter the **ssl-proxy mac-address** interface configuration command. (CSCsj36550)
- Because Cisco Discovery Protocol (CDP) is not supported on this module, it is removed as a configuration option. (CSCdz24446)

- Because the SSLM receives time setting from the supervisor engine, Network Time Protocol (NTP) and module time setting are removed as configuration options. Time setting changes are configured on the supervisor engine. You can configure the time zone information on the SSLM using the **clock timezone** and **clock summer-time** commands. (CSCsg55214 and CSCek44168)
- The **subject-name** subcommand is added to the **policy http-header** command, allowing the subject name to be inserted in every HTTP request. In earlier releases, the subject name was inserted only in the first HTTP request after the SSL handshake. (CSCsl20305)

The **subject-name** option can be configured only when a **client-cert** option has been configured on the policy. We recommend that you use the **subject-name** option only if the backend server requires the client certificate subject name to be provided for every client request in the SSL session.

The **subject-name** option consumes a large amount of memory on both the SSL processor and the supervisor engine processor. We recommend that you monitor memory usage using the **show ssl-proxy memory module** command and the **show memory statistics** command. Reduce cache timeouts and cache sizes if memory usage is excessive.

- The **allow-revoked-certs** subcommand is added to the **policy http-header** command. (CSCsl67902)

The **allow-revoked-certs** command allows SSL client authentication failures due to a revoked certificate to proceed while the failure status is reported in the client certificate HTTP header insert sent to the backend server. The client authentication **valid:** field is set to a 0 upon failure, and to 1 upon success. If the client authentication is a success, the **Error:** field contains the string “none.” Otherwise, the **Error:** field contains the following string:

Cert Revoked

Cert Revoked means that the certificate was otherwise valid, but was reported as revoked by either the Online Certificate Status Protocol (OCSP) or the Certificate Revocation List (CRL). This is the only failure that is allowed to proceed by the **allow-revoked-certs** command. To allow any SSL client authentication failure, use the **allow-auth-failures** command. The **Error:** field strings have changed from SSL software release 3.1(3) to provide more descriptive error reporting for other revocation check failures. The **Error:** field contains one of the following strings:

Cert Not In CA Pool
 Internal Error
 Internal Error: No Memory
 No Cert Public Key
 No Cert Data
 No Cert Chain
 No Cert DER
 Bad Cert DER Len
 CRL Get Failure
 Cert Not Authorized
 CA Not Self-Signed Root
 Cert Date Not Valid Yet
 Cert Date Expired
 Invalid Cert
 CA Request Failure
 OCSP Response Date Out-of-Range
 Cert Revoked
 Unknown

CA Request Failure is reported if a failure occurred when querying the CRL or OCSP responder.

OCSP Response Date Out-of-Range is reported if the OCSP responder responded to the query, but its values for thisTime or nextTime were out of range. This condition often indicates a clock skew between the OCSP responder host system and the SSLM.

Following is an example of the **allow-revoked-certs** command:

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssl-proxy context Default
Router(config-context)# policy http-header headerPolicy
Router(config-ctx-http-header-policy)# allow-revoked-certs
```

Changes in Software Release 3.1(3)

The following changes are introduced in SSL software release 3.1(3):

- SSL software release 3.1 adds four new fields to the HTTP header insertion when the **client-cert** option is specified, for a total of 25 fields. SSL software release 3.1(3) adds the **client-cert basic** option for HTTP header insertion, which causes the insertion of only the 21 fields that were inserted with SSL software release 2.1. (CSCsl06228)
- New CLI command **debug ssl-proxy tcp conn** is added in SSL software release 3.1(3). (CSCsj42025)

The **debug ssl-proxy tcp conn** command prints the entire contents of the TCP connection table to the debug Telnet connection at TCP port 2002. This command is used to obtain information for debugging TCP connection issues and should be run only under the direction of Cisco support personnel. Unlike other **debug ssl-proxy** commands, this command does not set a flag that remains enabled until explicitly cleared.

- New CLI command **debug ssl-proxy ssl conn** is added in SSL software release 3.1(3). (CSCsj42025)

The **debug ssl-proxy ssl conn** command prints the entire contents of the SSL connection table to the debug Telnet connection at TCP port 2003. This command is used to obtain information for debugging SSL connection issues and should be run only under the direction of Cisco support personnel. Unlike other **debug ssl-proxy** commands, this command does not set a flag that remains enabled until explicitly cleared.

- New CLI command **show ssl-proxy stats app-if** is added in SSL software release 3.1(3).

Following is an example of the **show ssl-proxy stats app-if** command:

```
Router# show ssl-proxy stats app-if
TCP-SSL Interface Statistics:
  num csm congests          : 0          num csm congest callbacks : 0
  num multi-data rec       : 0          num large buf repack      : 0
  large buf repack copies  : 0          multi-data rec buf fails  : 0
  conn reuse               : 0          sslv2 only conns         : 0
  bufs in reassembly      : 0
  error drops              : 0          ssl encrypt drops        : 0
  alloc msg sent to ssl    : 0          delete msg sent to ssl   : 0
```

- In SSL software release 3.1(3), a number of new counters have been added to the **show ssl-proxy stats** command output using no display options and using the display options **tcp**, **ssl**, and **hdr**.
- New CLI command **log-auth-failures** is added in SSL software release 3.1(3). (CSCsl42946)

The **log-auth-failures** command enables the logging of client authentication failures to the system log. To prevent filling the log file, this option is disabled by default. When enabled, the logging is rate-limited.

Following is an example of the **log-auth-failures** command:

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssl-proxy context Default
Router(config-context)# service service1
Router(config-ctx-ssl-proxy)# log-auth-failures
```

- New CLI command **allow-auth-failures** is added in SSL software release 3.1(3). (CSCs142959)
The **allow-auth-failures** command allows SSL client authentication failures to proceed while the failure status is reported in the client certificate HTTP header insert sent to the backend server. The client authentication **valid:** field is set to a 0 upon failure, and to 1 upon success. If the client authentication is a success, the **Error:** field contains the string “none.” Otherwise, the **Error:** field contains one of the following strings:

```
Cert Not In CA Pool
Cert Not Approved
Internal Error: No Memory
No Cert Public Key
No Cert Data
No Cert Chain
No Cert DER
Bad Cert DER Len
Cert Date Not Valid Yet
Invalid Cert
CRL Get Failure
Cert Not Authorized
CA Not Self-Signed Root
OCSP Get Failure
Internal Error
Cert Date Expired
Unknown
```

Following is an example of the **allow-auth-failures** command:

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssl-proxy context Default
Router(config-context)# policy http-header headerPolicy
Router(config-ctx-http-header-policy)# allow-auth-failures
```

- New CLI command **min-chain-length** is added in SSL software release 3.1(3). (CSCs142088)
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 check only at the time that the trustpoint is associated with the service. After making a change to the **min-chain-length** value, you should disassociate the trustpoint from the service, and then reassociate it.

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

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

- In SSL software release 3.1(3), a new modifier and subcommand are added to a CA trustpoint entry. (CSCsj50972)

The new options provide the capability to specify a certificate map that may be associated with a CA trustpoint in the trusted CA pool that is used for client authentication. This capability allows the separation of the functions of client certificate authentication and authorization. The trustpoint is used to authenticate the client certificate and the trusted pool to authorize the certificate. Separating these functions allows you to control which trustpoint is selected during client authentication and to restrict access to various services based on the contents of the client certificates. Note that each trustpoint must use a different certificate as there is no ability to distinguish between trustpoints using the same certificate.

The new **match map** *map-name* modifier is an option that can be added to a CA trustpoint entry in the **pool ca** *pool_name*. For a client certificate to be approved, it must follow the normal authentication process, including the requirement that the certificate chain must be signed by one of the CA trustpoints in the trusted CA pool that is associated with the proxy service. In addition, if the certificate map name is associated with the trustpoint by configuring the optional **match map** *map-name* modifier, then the client certificate must also match that map.

Following is a configuration example using the **match map** *map-name* modifier:

```
Router(config)# ssl-proxy context Default
Router(config-context)# pool ca samplePool
Router(config-ctx-ca-pool)# ca trustpoint RootCA match map MAP1
```

When the **match map** *map-name* option is configured, the new **ssl-proxy service** subcommand **cert-trim** must be configured for the service. For legacy functionality, the default **no cert-trim** should be configured. This option trims the certificate chain to the shortest chain that patches a given trustpoint during the validation process.

Following is a configuration example using the **cert-trim** subcommand:

```
Router(config)# ssl-proxy context Default
Router(config-context)# service Service1
Router(config-ctx-ssl-proxy)# cert-trim
```

Limitations and Restrictions

This section describes general limitations and restrictions:

- 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 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)
- 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. (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 certified by the Federal Information Processing Standards (FIPS).
- 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 the open and resolved caveats in SSL software for all 3.1(x) software releases:

- [Open Caveats in Release 3.1\(4\), page 10](#)
- [Resolved Caveats in Release 3.1\(4\), page 13](#)
- [Open Caveats in Release 3.1\(3\), page 15](#)
- [Resolved Caveats in Release 3.1\(3\), page 18](#)
- [Open Caveats in Release 3.1\(2\), page 20](#)
- [Resolved Caveats in Release 3.1\(2\), page 23](#)
- [Open Caveats in Release 3.1\(1\), page 24](#)
- [Resolved Caveats in Release 3.1\(1\), page 27](#)

Open Caveats in Release 3.1(4)

This section describes open caveats for the SSL Services Module software release 3.1(4).

- When client authentication is enabled and client certificate HTTP header insertion is performed, the performance may be much lower than the performance in software release 2.1. (CSCsl06228)

Workaround: In the **policy http-header** command, specify either the **client-cert pem** option or the new **client-cert basic** option. See the “New and Changed Information” section on page 5 for information about the **client-cert basic** option.

- When you enter the **show ssl-proxy stats pki** command, the counters do not indicate whether or not Online Certificate Status Protocol (OCSP) was used to verify the certificate. (CSCei92116)
- If an interface is configured with a maximum transmission unit (MTU) smaller than 150 bytes and large size requests are posted, fragmented connections fail to reassemble when there are more than six connections per second.

Workaround: Increase the MTU to 512 bytes or larger. (CSCek01245)

- 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 re-established. 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 SSLM 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 SSLM is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)
- When the SSLM 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 SSLM.

Workaround: Save the configuration, and reset the SSLM. (CSCee46096)

- The SSLM 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 SSLM continues to insert the other configured HTTP headers (other than client certificate headers) in the request.

Workaround: Save the configuration and reset the SSLM. (CSCin67360)

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

```
Error: Module mod didn't shutdown complete within 3 min.Module resetting...
```

The supervisor engine then successfully resets the SSLM. (CSCec69592)

- 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 pki trustpoint trustpoint_label** and **crypto pki certificate chain name** command information from the running configuration.
 - b. Delete the trustpoint by entering the **no crypto pki 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 SSLM 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 SSLM 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 SSLM. 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 pki certificate** command. (CSCea50887)
- 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: pklc#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)
- 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)
- If you enter the **clear arp** command on the SSLM, all the proxy services go into a “down” state, and then go into an “up” state. (CSCdy77843)
- When you configure query mode, entering the **no crypto pki certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSLM 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 3.1(4)

This section describes resolved caveats for the SSL Services Module software release 3.1(4).

- When a URL-rewrite policy is configured with a prefix wildcard, and the URL to be rewritten does not contain a trailing slash (/) or carriage-return (\r), the module resets. (CSCsq57256)

- The failure of an Online Certificate Status Protocol (OCSP) get operation is incorrectly reported as an invalid certificate failure instead of an OCSP get failure. (CSCsq50818)
- When a handshake timeout has been configured, the SSLM may reset connections using an interval of less than the defined handshake timeout value.

Workaround: Remove the timeout handshake value. With the default value of 0, the SSLM will wait until the connection closes for the handshake to complete. (CSCsl54156)

- All SSL connections are dropped after sending continuous high-volume traffic. (CSCsl63177)
- Unnecessary spaces or blank lines appear in debug messages. (CSCsl72099)
- If the client fragments the HTTP request, header insertion might fail. (CSCsl76911)
- An incorrect expiration date is shown for the Extended Validation Root Certificate (EV-root). (CSCsl92290)
- Importing or exporting a PEM certificate fails when using SCP with SSHv2.

Workaround: Use SSHv1 instead of SSHv2. (CSCsl74825)

- The **mac-address** command appears in the SSLM configuration even if the MAC address is the burned-in address (BIA). This command should only appear if the MAC address has been changed. (CSCsj36616)

The **mac-address** interface configuration command is removed. See the [“New and Changed Information” section on page 5](#).

- Other devices will be unable to ping or communicate with the SSLM if the MAC address is reconfigured for a value other than the burned-in address (BIA). The MAC address can be changed using the **mac-address** command under the SSL-proxy0 interface.

Workaround: Change the MAC address back to the burned-in address (BIA). (CSCsj36650)

The **mac-address** interface configuration command is removed. See the [“New and Changed Information” section on page 5](#).

- Configuring NTP on the SSLM interferes with the module’s synchronization with the supervisor engine.

Workaround: Do not configure NTP on the SSLM. (CSCsg55214)

The NTP configuration option is removed. See the [“New and Changed Information” section on page 5](#).

- After a reset or reload, the SSLM does not retain a configured time setting. The module reverts to the default, Universal Time Code (UTC). (CSCek44168)

The local SSLM time setting option is removed. See the [“New and Changed Information” section on page 5](#).

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

CDP configuration is removed. See the [“New and Changed Information” section on page 5](#).

- If the OCSP server accepts the TCP connection for an OCSP status request from the SSLM, but does not respond, the SSLM will not accept any new connections until the TCP connection is dropped by rebooting the OCSP server. (CSCsl74182)

- The SSLM logs an error #788h if it receives an OCSP response with only two HTTP headers.

Workaround: Configure the OCSP server to include the Content-Transfer-Encoding header. (CSCsm32490)

- If backend encryption is configured with a Microsoft IIS backend server, the connections will fail. When this condition occurs, the **show ssl-proxy stats ssl** command shows that the **bad macs received** counter has incremented. (CSCsm84963)
- If a session times out of the session cache while a client request is being processed by the SSLM, a session ID of zero will be inserted into the HTTP header.
Workaround: Disable the session cache or increase the timeout. (CSCso58537)
- When the **show ssl-proxy buffers** command shows that the number of TCP ingress data buffers used Current has reached 40 percent of the TCP ingress buffer pool size, the SSLM will not accept any new connections. (CSCso09564)
- The SSLM responds to a TLS1.1 ClientHello message by closing the connection. It should respond with a TLS1.0 ServerHello message. (CSCso60805)
- System messages should include the context name for policies. (CSCek72381)
- The SSLM content-scanning logic does not recognize the WebDav HTTP methods identified in RFC-2518. If a header insertion policy is configured, the WebDav request will fail with no response from the SSLM. (CSCsq48567)
- When the SSL handshake fails because the client certificate is invalid, the system message should include the actual OCSP response, including whether the certificate is revoked. (CSCsl67902)
The **allow-revoked-certs** command is added. See the [“New and Changed Information” section on page 5](#).

Open Caveats in Release 3.1(3)

This section describes open caveats for the SSL Services Module software release 3.1(3).

- Importing or exporting a PEM certificate fails when using SCP with SSHv2.
Workaround: Use SSHv1 instead of SSHv2. (CSCsl74825)
- When client authentication is enabled and client certificate HTTP header insertion is performed, the performance may be much lower than the performance in software release 2.1. (CSCsl06228)
Workaround: In the **policy http-header** command, specify either the **client-cert pem** option or the new **client-cert basic** option. See the [“New and Changed Information” section on page 5](#) for information about the **client-cert basic** option.
- Other devices will be unable to ping or communicate with the SSLM if the MAC address is reconfigured for a value other than the burned-in address (BIA). The MAC address can be changed using the **mac-address** command under the SSL-proxy0 interface.
Workaround: Change the MAC address back to the burned-in address (BIA). (CSCsj36550)
- The **mac-address** command appears in the SSLM configuration even if the MAC address is the burned-in address (BIA). This command should only appear if the MAC address has been changed. (CSCsj36616)
- If the OCSP server accepts the TCP connection for an OCSP status request from the SSLM, but does not respond, the SSLM will not accept any new connections until the TCP connection is dropped by rebooting the OCSP server. (CSCsl74182)
- When you enter the **show ssl-proxy stats pki** command, the counters do not indicate whether or not Online Certificate Status Protocol (OCSP) was used to verify the certificate. (CSCei92116)

- If an interface is configured with a maximum transmission unit (MTU) smaller than 150 bytes and large size requests are posted, fragmented connections fail to reassemble when there are more than six connections per second.

Workaround: Increase the MTU to 512 bytes or larger. (CSCek01245)

- 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 re-established. 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 SSLM 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 SSLM is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)

- When the SSLM 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 SSLM.

Workaround: Save the configuration, and reset the SSLM. (CSCee46096)

- The SSLM 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 SSLM continues to insert the other configured HTTP headers (other than client certificate headers) in the request.

Workaround: Save the configuration and reset the SSLM. (CSCin67360)

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

```
Error: Module mod didn't shutdown complete within 3 min.Module resetting...
```

The supervisor engine then successfully resets the SSLM. (CSCec69592)

- 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 pki trustpoint trustpoint_label** and **crypto pki certificate chain name** command information from the running configuration.
 - b. Delete the trustpoint by entering the **no crypto pki 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 SSLM 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 SSLM 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 SSLM. 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 pki certificate** command. (CSCea50887)

- 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: pcle#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 SSLM, 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)
- If you enter the **clear arp** command on the SSLM, all the proxy services go into a “down” state, and then go into an “up” state. (CSCdy77843)
- When you configure query mode, entering the **no crypto pki certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSLM 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 3.1(3)

This section describes resolved caveats for the SSL Services Module software release 3.1(3).

- The SSLM receives HTTPS traffic containing a POST, but does not forward the decrypted traffic to the server if the Content-Length field in the POST header is split across buffers. (CSCsi43394)
- Proxy services will fail when the server IP address is configured as the next-hop IP address and a route exists with the same next-hop IP address. The SSLM issues no warning for this situation. (CSCek25162)
- The SSLM will generate a self-signed certificate having a serial number of 00. (CSCse84368)

- When a URL-rewrite policy is configured with an asterisk (*), the SSLM will rewrite HTTP to HTTPS even on non-default (port 80) TCP ports. (CSCse28330)
- A certificate renewal fails when the original trustpoint was created using the **crypto ca import name pem terminal password** command. (CSCsj89254)
- Certificates with common names longer than 64 characters will not be processed. (CSCef34358)
- The SSLM does not provide the value of the cspScConnComplete MIB item to an SNMP request. (CSCsj49374)
- The SSLM rejects certificates with RFC3280 reasonFlags. (CSCef45734)
- On an SNMP request, PKI_GetCertAttributesOID only returns the first item of the given attribute rather than all items. (CSCsb79501)
- After a software upgrade from software release 2.1, HTTP-Header Policy insertion strings now incorrectly contain quotation marks. (CSCsj13234)
- If the CA certificate is used in multiple trustpoints, the revocation check configured for the trustpoint may be ignored. Certificate maps and any actions associated with those certificate maps may also be ignored. (CSCsj50972)
- When client authentication is enabled on a service and the associated trusted CA trustpoint has revocation-check oosp configured, the SSLM may crash when the client certificate is authenticated. (CSCsk58505)
- When enrolling certificates between Cisco IOS 12.3.3 and the Microsoft certificate authority (CA), three %SYS-3-CPUHOG messages are seen. (CSCec76781)
- When an OCSP revocation check fails, a memory leak is observed in the SSLM. (CSCef20779)
- The SSLM connection resources may become depleted, which causes connections to be rejected. (CSCsk25132)
- The SSLM may reload unexpectedly when session renegotiation is enabled. (CSCsj42025)
- During a CRL check, the wrong counter is incremented for expired certificates. (CSCek30466)
- The SSL termination engine may respond to an SSL client Hello with a TCP FIN, leading to an SSL handshake failure. (CSCsj40125)
- The commands **show ssl-proxy mac address** and **show ssl-proxy mac cpu-util** display incorrect results. (CSCsl28453)
- Custom header insertion fails for consecutive POSTs in a TCP connection. (CSCsl35144)
- When a self certificate is linked to a service, the service goes down with a “No Certificate” message. (CSCsl32019)
- SSL handshake failures due to invalid client certificates are not logged to the system log. (CSCsl42946)
- Need an option to allow the SSLM to complete a transaction with an invalid client certificate, and to report the client authentication status to the backend server. (CSCsl42959)
- Need an option to allow the SSLM to associate partial certificate chains (that do not contain the root CA) to an SSL proxy service. (CSCsl42088)
- When the SSLM supports a service that requires a client certificate and another service that does not require it, a client can connect to the nonauthenticated service, and then resume that SSL session on the authenticated service. (CSCsk36744)

Open Caveats in Release 3.1(2)

This section describes open caveats for the SSLM software release 3.1(2).

- Importing or exporting a PEM certificate fails when using SCP with SSHv2.
Workaround: Use SSHv1 instead of SSHv2. (CSCs174825)
- When client authentication is enabled and client-cert http-header insertion is performed, performance is poor relative to software release 2.1. (CSCs106228)
Workaround: In the **policy http-header** command, specify either the **client-cert pem** option or the new **client-cert basic** option. See the “New and Changed Information” section on page 5 for information about the **client-cert basic** option.
- Other devices will be unable to ping or communicate with the SSLM if the MAC address is reconfigured for a value other than the burned-in address (BIA). The MAC address can be changed using the **mac-address** command under the SSL-proxy0 interface.
Workaround: Change the MAC address back to the burned-in address (BIA). (CSCsj36550)
- The **mac-address** command appears in the SSLM configuration even if the MAC address is the burned-in address (BIA). This command should only appear if the MAC address has been changed. (CSCsj36616)
- If the OCSP server accepts the TCP connection for an OCSP status request from the SSLM, but does not respond, the SSLM will not accept any new connections until the TCP connection is dropped by rebooting the OCSP server. (CSCs174182)
- The SSLM receives HTTPS traffic containing a POST, but does not forward the decrypted traffic to the server. (CSCsi43394)
- When you enter the **show ssl-proxy stats pki** command, the counters do not indicate whether or not Online Certificate Status Protocol (OCSP) was used to verify the certificate. (CSCei92116)
- If an interface is configured with a maximum transmission unit (MTU) smaller than 150 bytes and large size requests are posted, fragmented connections fail to reassemble when there are more than six connections per second.
Workaround: Increase the MTU to 512 bytes or larger. (CSCek01245)
- 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 re-established. 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 SSLM 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 SSLM is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)
- When the SSLM 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 SSLM.

Workaround: Save the configuration, and reset the SSLM. (CSCee46096)

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

```
Error: Module mod didn't shutdown complete within 3 min.Module resetting...
```

The supervisor engine then successfully resets the SSLM. (CSCec69592)

- 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:

- Copy the **crypto pki trustpoint** *trustpoint_label* and **crypto pki certificate chain name** command information from the running configuration.
 - Delete the trustpoint by entering the **no crypto pki trustpoint** *trustpoint_label* command.
 - 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 SSLM 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 SSLM 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 SSLM. 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 pki certificate** command. (CSCea50887)
- 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: pklc#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 SSLM, 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)
- If you enter the **clear arp** command on the SSLM, all the proxy services go into a “down” state, and then go into an “up” state. (CSCdy77843)
- When you configure query mode, entering the **no crypto pki certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)

- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSLM 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 3.1(2)

This section describes resolved caveats for the SSLM software release 3.1(2).

- The SSLM stops accepting new SSL connections because of a depletion of connection IDs on the FDU processor. When this happens, a large difference between the conn alloc counters and conn dealloc counters under FDU is displayed when you enter the **show ssl-proxy stats fdu** command. (CSCsh14823)

- The SSLM reboots every 2 to 6 hours in the URL rewrite process.

Workaround: Disable URL rewrite. (CSCsd25820)

- When HTTPS service is configured on the SSLM, some browsers will return Error Code -12243. (CSCsd88210)

- You may receive a CDP duplex mismatch error from the SSLM.

Workaround: Disable CDP on the SSLM using the **no cdp run** command. (CSCse02001)

- The SSLM stops accepting new SSL connections because of a depletion of connection IDs on the TCP processor. The condition can occur when there is a difference of approximately 65K between the conn alloc counters and conn dealloc counters under TCP as seen using the **show ssl-proxy stats** command. When all connection IDs are exhausted, the module is unable to initiate any more connections to the backend servers.

Workaround: Reload the SSLM. (CSCek50983)

- When header insert is configured in the SSL-Proxy service, the SSLM fails to pass the entire POST from the client to the server. This error is seen with a POST that has a large payload, spanning two packets.

Workaround: Do not configure the SSL-Proxy service for header insert. (CSCse31785)

- The URL rewrite process is erroneously triggered by a URL match beyond the host name portion of the location string. (CSCsg65505)

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

When the SSL-Proxy service is configured under certain non-default contexts, cspServCertExpiring traps are sent with varbinds that have the value NO_SUCH_INSTANCE_EXCEPTION.

Workaround: If virtualization is not required (for example, if VRF is not configured), move all services under the default context. (CSCsh52152)

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

Workaround: Reload the SSLM. (CSCsh79045)

- When displayed by the **show ssl-proxy status** command, the SNMPWALK cspCpuProcessUtilIn5Sec output for SSL CPU figures does not match the CLI. (CSCsi06451)

- When you configure two proxy services with the same TCP health probe name and remove the TCP health probe from one of the proxy services, a traceback error occurs. (CSCek26614)

- When you upgrade an SSLM that is configured with the default configuration to software release 3.1(1) and boot up the module for the first time, the console displays a “Would you like to enter the initial configuration dialogue?” message. If you do not reply to the message, or if you reply “yes” to the message but do not complete the initial configuration, the module might reboot after a few minutes.

Workaround: Complete the initial configuration, or reply no to the message. (CSCek39233)

Open Caveats in Release 3.1(1)

This section describes open caveats for the SSLM software release 3.1(1).

- Importing or exporting a PEM certificate fails when using SCP with SSHv2.

Workaround: Use SSHv1 instead of SSHv2. (CSCsl74825)

- When client authentication is enabled and client-cert http-header insertion is performed, performance is poor relative to software release 2.1. (CSCsl06228)

Workaround: In the **policy http-header** command, specify either the **client-cert pem** option or the new **client-cert basic** option. See the “[New and Changed Information](#)” section on page 5 for information about the **client-cert basic** option.

- Other devices will be unable to ping or communicate with the SSLM if the MAC address is reconfigured for a value other than the burned-in address (BIA). The MAC address can be changed using the **mac-address** command under the SSL-proxy0 interface.

Workaround: Change the MAC address back to the burned-in address (BIA). (CSCsj36550)

- The **mac-address** command appears in the SSLM configuration even if the MAC address is the burned-in address (BIA). This command should only appear if the MAC address has been changed. (CSCsj36616)
- If the OCSP server accepts the TCP connection for an OCSP status request from the SSLM, but does not respond, the SSLM will not accept any new connections until the TCP connection is dropped by rebooting the OCSP server. (CSCsl74182)
- When you configure two proxy services with the same TCP health probe name and remove the TCP health probe from one of the proxy services, a traceback error occurs. (CSCek26614)
- When you enter the **show ssl-proxy stats pki** command, the counters do not indicate whether or not Online Certificate Status Protocol (OCSP) was used to verify the certificate. (CSCei92116)
- If an interface is configured with a maximum transmission unit (MTU) smaller than 150 bytes and large size requests are posted, fragmented connections fail to reassemble when there are more than six connections per second.

Workaround: Increase the MTU to 512 bytes or larger. (CSCek01245)

- 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 re-established. 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 SSLM 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 SSLM is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM. (CSCed53976)
- When you upgrade an SSLM that is configured with the default configuration to software release 3.1(1) and boot up the module for the first time, the console displays a “Would you like to enter the initial configuration dialogue?” message. If you do not reply to the message, or if you reply “yes” to the message but do not complete the initial configuration, the module might reboot after a few minutes.

Workaround: Complete the initial configuration, or reply no to the message. (CSCek39233)

- When the SSLM 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 SSLM.

Workaround: Save the configuration, and reset the SSLM. (CSCee46096)

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

```
Error: Module mod didn't shutdown complete within 3 min.Module resetting...
```

The supervisor engine then successfully resets the SSLM. (CSCec69592)

- If you add a trailing slash (/) to the *url* value in the **enrollment url** *url* command for a trustpoint, the SSLM 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)

- 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:

- Copy the **crypto pki trustpoint** *trustpoint_label* and **crypto pki certificate chain name** command information from the running configuration.
 - Delete the trustpoint by entering the **no crypto pki trustpoint** *trustpoint_label* command.
 - 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 SSLM 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 SSLM 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 SSLM. 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 pki certificate** command. (CSCea50887)
- 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: pklc#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 SSLM, 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)
- If you enter the **clear arp** command on the SSLM, all the proxy services go into a “down” state, and then go into an “up” state. (CSCdy77843)
- When you configure query mode, entering the **no crypto pki certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- On systems that are running Cisco IOS software and are configured with route processor redundancy plus (RPR+) or stateful switchover (SSO), if you shut down the SSLM 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 3.1(1)

There are no resolved caveats in SSL Services Module software release 3.1(1).

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Content Switching Module Configuration Note*
- *Catalyst 6500 Series Content Switching Module Command Reference*
- *Catalyst 6500 Series Content Switching Module Installation and Verification Note*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*

- For information about MIBs, refer to this URL:
<http://www.cisco.com/go/mibs>

Cisco IOS Software Documentation Set

Cisco IOS Configuration Guides and Command References—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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.

© 2005–2008, Cisco Systems, Inc.
All rights reserved.