Catalyst 6500 Series Switch SSL Services Module System Message Guide

Release 2.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Preface

This preface describes who should read the *Catalyst 6500 Series Switch SSL Services Module System Message Guide*, how it is organized, and its document conventions.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Only trained and qualified service personnel (as defined in IEC 60950 and AS/NZS3260) should install, replace, or service the Catalyst 6500 series switch SSL Services Module.

Organization

The major sections of this publication are as follows:

Chapter	Title	Description
1	System Message Overview	Describes how to read a system or error message.
2	System Messages	Contains system messages, explanations, and recommended actions.

Related Documentation

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

- *Release Notes for Catalyst 6500 Series SSL Services Module Software Release 2.x*
- *Catalyst 6500 Series Switch SSL Services Module Installation and Verification Note*
- *Catalyst 6500 Series Switch SSL Services Module Command Reference*
- *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 Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Site Preparation and Safety Guide*

Conventions

Screen examples use the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	`This pointer highlights an important line of text in an example.`
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

System Message Overview

This publication lists and describes the system messages for the Catalyst 6500 series switch SSL Services Module. The system software sends these messages to the console (and, optionally, to a logging server on another system) during operation. Not all system messages indicate problems with your system. Some messages are purely informational, while others may help diagnose problems with communications lines, internal hardware, or the system software.

This publication also includes system messages that appear when the system fails.

This chapter contains the following sections:

System Message Structure

System messages are structured as follows:

FACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY code

  The facility code consists of two or more uppercase letters that indicate the facility to which the message refers. In this publication, the only facility is STE.

- SEVERITY level

  The severity level is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. Table 1-1 lists the message severity levels.

Table 1-1 Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable
1 – alert	Immediate action required
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Message that appears during debugging only

- MNEMONIC code

  The MNEMONIC code uniquely identifies the error message.

- Message-text

  Message-text is a text string that describes the condition. The text string sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because variable fields change from

message to message, they are represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec]. Table 1-2 lists the variable fields in messages.

Table 1-2 Representation of Variable Fields in Messages

Representation	Type of Information
[chars] or [char]	Character string
[dec]	Decimal
[hex]	Hexadecimal integer
[int]	Integer
[num]	Number

System Message Example

The following is an example of a system message:

```
%STE-2-IPC_HEALTH_PROBE: [chars]
```

- STE is the facility code.
- 2 is the severity level.
- IPC_HEALTH_PROBE is the mnemonic code.
- [chars] is the message text.

Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. This information is very important and should be included when you report a problem to your technical support representative.

The following sample message includes traceback information:

-Process = "Exec", level = 0, pid = 17

-Traceback = 1A82 1AB4 6378 A072 1054 1860

System Messages

This chapter lists the Catalyst 6500 series switch SSL Services Module system messages by severity level. The highest severity level is 0, and the lowest severity level is 7. Each message is followed by an explanation and a recommended action.

Note The messages listed in this chapter do not include the date/time stamp designation; the date/time stamp designation is displayed only if the software is configured for system log messaging.

STE-2

Error Message `%STE-2-IPC_HEALTH_PROBE: [chars]`

Explanation The system did not receive a health probe response from the specified modules.

Recommended Action No action is required. The system resets itself automatically. If you continue to see this message after the system resets itself, contact your Cisco technical support representative.

Note This message always appears on the console or in the system log with `%STE-2-IPC_HEALTH_PROBE_HEAD` and `%STE-2-IPC_HEALTH_PROBE_TAIL`. The three messages together indicate one error condition. If you see these three messages, no action is required because the system automatically resets itself. If you continue to see these messages after the system resets itself, contact your Cisco technical support representative.

Error Message `%STE-2-IPC_HEALTH_PROBE_HEAD: The following modules failed to respond to a health probe.`

Explanation The system did not receive a health probe response from the specified modules.

Recommended Action No action is required. The system resets itself automatically. If you continue to see this message after the system resets itself, contact your Cisco technical support representative.

Error Message `%STE-2-IPC_HEALTH_PROBE_TAIL: Declaring the module dead.`

Explanation The system did not receive a health probe response from the specified modules.

Recommended Action No action is required. The system resets itself automatically. If you continue to see this message after the system resets itself, contact your Cisco technical support representative.

STE-3

Error Message `%STE-3-APP_IPC_BUFFER_ALLOC_FAILED: Module (APP) failed to get a buffer to send a IPC message.`

Explanation The Cisco IOS software needs to allocate buffers to send IPC messages. The software has failed to allocate a buffer. This condition might occur occasionally when you enter a command.

Recommended Action If this condition occurred when you entered a command, reenter the command. If this condition happens continuously, reboot the module.

Error Message `%STE-3-APP_IPC_STATUS_FAILED: Module (APP) got a response with status failed.`

Explanation The module could not process the inter-process communications (IPC) message.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, try rebooting the module to eliminate the problem.

Error Message `%STE-3-APP_URL_REWRITE_IPC_STATUS_FAILED: Module (APP) got a response with status failed and reason [chars]`

Explanation If the module can process the IPC message, the module sets the status to "OK." If it cannot handle the IPC message, the module sets the status to "failed."

Recommended Action If this condition occurred when you entered a command, reenter the command. If not, reboot the module to try to resolve the condition.

Error Message `%STE-3-CONTENT_IPC_BUFFER_ALLOC_FAILED: Module (CONTENT) failed to get a buffer to send a IPC message.`

Explanation The Cisco IOS software needs to allocate buffers to send IPC messages. It has failed to allocate a buffer. This condition might occasionally occur when you enter a command.

Recommended Action If this condition occurred when you entered a command, retry the command. If this condition happens continuously, reboot the module.

Error Message `%STE-3-CONTENT_IPC_SEND_FAILED: Module (CONTENT) failed to send a IPC message because of lack of resources`

Explanation The Cisco IOS software needs to allocate buffers to send IPC messages. It has failed to allocate a buffer. This condition might occasionally occur when you enter a command.

Recommended Action If this condition occurred when you entered a command, retry the command. If this condition happens continuously, reboot the module.

Error Message `%STE-3-CRASHINFO_MALLOC_FAILED: Module (CRASHINFO) failed to allocate memory buffer`

Explanation The module needs to allocate a memory buffer to parse and print crash information. The memory usage on the system is probably too high to allow the module to allocate such a memory buffer.

Recommended Action If this condition occurred when you entered a command and the memory usage on the system is too high, resolve the high memory usage condition and retry the command. You can also reboot the module and retry the command. Although you reboot the module, crash information is preserved because it is stored in NVRAM.

Error Message `%STE-3-CRYPTO_IPC_FAILED: Failed to send IPC message to SSL Processor: [chars] [dec]`

Explanation The cryptographic module encountered an error when sending an IPC message to one or more SSL processors.

Recommended Action Cancel and reenter the command. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `%STE-3-FDU_IPC_BUFFER_ALLOC_FAILED: Module (FDU) failed to get a buffer to send a IPC message.`

Explanation The system failed to allocate a buffer to send IPC messages.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, reboot the module.

Error Message `%STE-3-IPC_BUFFER_ALLOC_FAILED: Module (IPC) failed to get a buffer to send a IPC message.`

Explanation The module is in a transient state or a command failed.

Recommended Action If this message is related to the CLI, reenter the command. If this situation affects the functionality of the module, contact your Cisco technical support representative.

Error Message `%STE-3-IPC_INVALID_MID: IPC received a message with a invalid destination module id [dec]`

Explanation A source module ID is not registered to receive IPC messages.

Recommended Action If this situation affects the functionality of the module, contact your Cisco technical support representative.

Error Message `%STE-3-IPC_INVALID_TYPE: IPC received a message with a invalid type [dec]`

Explanation The system might have received a message that was not intended for it.

Recommended Action If this situation affects the functionality of the module, contact your Cisco technical support representative.

Error Message `%STE-3-IPC_NULL_RECEIVE_METHOD: IPC module received a message with NULL callback.`

Explanation IPC received a message that does not have a valid callback set for it.

Recommended Action If this situation affects the functionality of the module, contact your Cisco technical support representative.

Error Message `%STE-3-IPC_NULL_RECEIVE_QUEUE: IPC module received a message with method QUEUE but queue is NULL.`

Explanation IPC received a message that does not have a valid queue set for it.

Recommended Action If this situation affects the functionality of the module, contact your Cisco technical support representative.

Error Message `%STE-3-IPC_SEND_FOR_DATE_FAILED: Module (IPC) failed to send a IPC message to get date and time.`

Explanation The daughter card is unable to synchronize with the clock on the supervisor engine because of a failure in the control channel. This situation sometimes occurs during bootup.

Recommended Action Set the clock manually by entering the **set clock** command.

Error Message `%STE-3-PKI_CERT_CACHE_INIT_FAILED: Failed to reinitialize peer certificate cache with size [dec] and timeout [dec] minutes.`

Explanation Because of an internal error, the peer certificate cache with the new parameter values did not reinitialize.

Recommended Action Contact your technical support representative.

Error Message `%STE-3-PKI_CERT_INSTALL_FAILED: Failed to install a certificate chain, trustpoint: [chars], proxy service: [chars], index: [dec]`

Explanation The public key infrastructure (PKI) module failed to install a certificate chain for the specified proxy service. This error might be due to an unsupported key type or size.

Recommended Action Check the configuration and state of the key pair associated with the trustpoint assigned to the specified proxy service. Correct the key type or size, and reenroll the certificate. Remove the trustpoint assigned to the proxy service, and reassign it. If this message recurs, copy the

error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `%STE-3-PKI_CERT_ROLLOVER_FAILED: The process of rolling over the certificate without the sudden loss of services has failed for the proxy service [chars], trustpoint [chars]`

Explanation The rollover process cannot be completed because of an error that was encountered when installing the new certificate. This error might be due to an unsupported key type or size.

Recommended Action Check the current configuration and state of the key pair associated with the trustpoint assigned for the proxy service. Correct the key type or size, and reenroll the certificate. Remove the trustpoint assigned to the service, and reassign it. Enter the **show ssl-proxy service** command to display information about keys and certificates associated with the proxy service.

Error Message `%STE-3-PKI_INVALID_IPC_MSG: Invalid PKI IPC messages: [chars]`

Explanation The public key infrastructure module received an invalid IPC message.

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the message information.

Error Message `%STE-3-PKI_IPC_FAILED: Failed to send IPC message to SSL Processor: [chars] [chars] [dec]`

Explanation The public key infrastructure module encountered an error when the module sent an IPC message to one or more SSL processors.

Recommended Action Remove the certificate that is assigned to the proxy services. Reassign the certificate to trigger IPC again. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the message information.

Error Message `%STE-3-PKI_KEY_INSTALL_FAILED: Failed to install a key pair: [chars], trustpoint: [chars], proxy service: [chars], index: [dec]`

Explanation The public key infrastructure module failed to install a key pair for the specified proxy service.

Recommended Action Check that the key pair of the trust point assigned to the proxy service is in the Cisco IOS key chain by entering the **show crypto key mypub rsa** command. Remove the certificate that was assigned to the proxy service. Reassign the certificate to reinstall it. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the message information

Error Message `%STE-3-PKI_MISCONFIGURED_KEY_TYPE: Trustpoint [chars] key type [chars] does not match type for SSL proxy service.`

Explanation The key type of the trust point must be the same as what was configured for the SSL proxy service.

Recommended Action Regenerate a key pair of the same type configured for the SSL proxy service. Enroll for a new certificate.

Error Message `%STE-3-PKI_MISMATCHED_CERT_KEY_TYPE: Certificate key type [chars] does not match type for SSL proxy service [chars].`

Explanation The specified key type of the certificate must be the same as what was configured for the SSL proxy service.

Recommended Action Regenerate a key pair of the same type configured for the SSL proxy service. Enroll for a new certificate.

Error Message `%STE-3-PKI_OP_FAILURE: [chars] [chars] [dec]`

Explanation A public key infrastructure operation failed. The failure might have occurred because of a lack of resources.

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the message information.

Error Message `%STE-3-PKI_UNSUPPORTED_KEY_ALGORITHM: Algorithm of key pair [chars] is unsupported.`

Explanation The key algorithm is unsupported. The supported key type is RSA.

Recommended Action Regenerate a key pair of the supported type.

Error Message `%STE-3-PKI_UNSUPPORTED_KEY_SIZE: Trustpoint [chars] key size is not supported. Supported sizes are: 512, 678, 1024, 1536, 2048-bit`

Explanation The trust point key size is not supported.

Recommended Action Regenerate a key pair of supported size for the trust point. Enroll for a new certificate.

Error Message `%STE-3-PKI_UNSUPPORTED_KEY_TYPE: Trustpoint [chars] key type [chars] is unsupported.`

Explanation The specified key type is unsupported. Supported key types are RSA key pairs and general purpose key pairs.

Recommended Action Regenerate a key pair of a supported type for the trust point. Enroll for a new certificate.

Error Message `%STE-3-SSL_IPC_BUFFER_ALLOC_FAILED: Module (SSL) failed to get a buffer to send a IPC message.`

Explanation The system failed to allocate a buffer to send IPC messages.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, try rebooting the module to eliminate the problem.

Error Message `%STE-3-SSL_IPC_SEND_FAILED: Module (SSL) failed to send a IPC message because of a lack of resources`

Explanation The system failed to allocate a buffer to send IPC messages.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, try rebooting the module to eliminate the problem.

Error Message `%STE-3-TCP_IPC_BUFFER_ALLOC_FAILED: Module (TCP) failed to get a buffer to send a IPC message.`

Explanation The system failed to allocate a buffer to send IPC messages.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, try rebooting the module to eliminate the problem.

Error Message `%STE-3-TCP_IPC_STATUS_FAILED: Module (TCP) got a response with status failed.`

Explanation The module could not process the IPC message.

Recommended Action If you see this message when entering a command, reenter the command. If you do not see this message when entering a command, try rebooting the module to eliminate the problem.

STE-4

Error Message `%STE-4-PKI_CA_POOL_CERT_EXPIRING: A CA certificate in a CA pool is going to expire or has expired at this time: [chars], CA pool: [chars], trustpoint: [chars].`

Explanation A CA certificate that has been assigned to a CA pool that is used for SSL proxy services is going to expire or has expired.

Recommended Action Import a new CA certificate.

Error Message `%STE-4-PKI_PROXY_SERVICE_CA_CERT_EXPIRING: A CA certificate is going to expire or has expired at this time: [chars], subject name: [chars], serial number: [chars].`

Explanation The certificate of a CA that has issued certificates for one or more SSL proxy services is going to expire or has expired.

Recommended Action Renew the CA certificate, and request the CA to issue new certificates for the proxy services.

Error Message `%STE-4-PKI_PROXY_SERVICE_CERT_EXPIRING: A proxy service certificate is going to expire or has expired at this time: [chars], proxy service: [chars], trustpoint: [chars].`

Explanation A proxy service certificate is going to expire or has expired.

Recommended Action Regenerate the key pair if necessary and renew the certificate. If the trustpoint name used for the new certificate is different from the current trustpoint, reassign the new trustpoint to the proxy services.

Error Message `%STE-4-PKI_WEAK_KEY: Trustpoint [chars] key size is weak. Recommended sizes are: 1024, 1536 and 2048-bit`

Explanation The key size is either 512 bits or 768 bits. We recommend stronger keys.

Recommended Action Regenerate a stronger key pair for the trust point and enroll for a new certificate.

STE-5

Error Message `%STE-5-PKI_NO_ENTRY: No free key and certificate table entries. [dec] entries in use.`

Explanation All entries in the proxy service key and certificate table are now in use. New proxy services cannot be supported.

Recommended Action Enter the **show ssl-proxy stats pki** command to display the counters. If long-lived connections still remain after rollover, some entries might still be used by old certificates. Clear the connections and restart the service.

Error Message `%STE-5-UPDOWN:ssl-proxy service [chars] changed state to [chars]`

Explanation The SSL proxy service state changed.

Recommended Action No action is required.

STE-6

Error Message `%STE-6-CRYPTO_SELFTEST_RUNNING: Cryptographic self-tests have started to run on the SSL Processor(s).`

Explanation The cryptographic algorithm test cases are running in the background with a time interval of 1 to 8 seconds. These self-tests are run on each cryptographic device in turn. Data traffic performance might be impacted.

Recommended Action Enter the **show ssl-proxy status crypto** command to display test results. These tests are for troubleshooting purposes only. You do not need to continually run these tests in the background.

Error Message `%STE-6-CRYPTO_SELFTEST_STATS_CLEARED: Cryptographic self-tests statistics have been cleared.`

Explanation Statistics for the cryptographic self-tests have been cleared.

Recommended Action No action is required.

Error Message `%STE-6-CRYPTO_SELFTEST_STOPPED: Cryptographic self-tests have stopped to run on the SSL Processor(s).`

Explanation The cryptographic algorithm tests are no longer running on the SSL processor.

Recommended Action No action is required.

Error Message `%STE-6-IPC_UNSUPPORTED_VERSION: Unsupported IPC Version number [dec]`

Explanation The system received an IPC message with an invalid version number. Only IPC version 1.0 is supported.

Recommended Action No action is required. IPC retries sending the message. If you continue to see this message, contact your Cisco technical support representative.

Error Message `%STE-6-NVRAM_DOWNGRADE_NOT_READY`

Explanation The configuration will not be saved when you downgrade the SSL module software to an earlier version.

Recommended Action If you plan to downgrade the SSL module software to an earlier version, enter the **copy running-config startup-config** command one more time. This action will prepare the configuration for the image downgrade. If you do not plan to downgrade the image, no action is required.

Error Message `%STE-6-NVRAM_DOWNGRADE_READY`

Explanation The configuration is saved when you downgrade the SSL module software to an earlier version.

Recommended Action No action is required.

Error Message `%STE-6-PKI_CERT_CACHE_INIT: Peer certificate cache has been reinitialized. Cache size is set to [dec] entries, and timeout is set to [dec] minutes`

Explanation Peer certificate cache configuration has been modified. The cache size and timeout values are set to the new values.

Recommended Action No action is required.

Error Message `%STE-6-PKI_CA_CERT_DELETE: [chars], Subject Name: [chars], Serial#: [chars], Index: [dec]`

Explanation A certificate authority certificate was deleted because no proxy services use it.

Recommended Action No action is required. A record of this deletion can be archived for reference or auditing.

Error Message `%STE-6-PKI_CERT_EXP_WARN_DISABLED: Checking of certificate expiration has been disabled.`

Explanation The expiration time interval has been reset to 0. No checking and logging will be performed. No SNMP traps will be sent. The internal memory of past logging will be erased. The next time that the time interval is set to a positive value, the checking, logging, and SNMP traps will be restarted.

Recommended Action No action is required.

Error Message `%STE-6-PKI_CERT_EXP_WARN_ENABLED: Proxy service certificate expiration warning has been enabled. Time interval is set to [dec] hours.`

Explanation Proxy service certificates, issuer CA certificates, and trusted CA certificates are periodically checked for expiration, which might occur within the configured time interval. Warning messages are logged once for each

certificate that has expired or is expiring. One SNMP trap also is generated for each of these proxy service certificates if the certificate expiration trap is enabled.

Explanation Renew all expired and expiring certificates.

Error Message `%STE-6-PKI_CA_CERT_INSTALL: [chars], Subject Name: [chars], Serial#: [chars], Index: [dec]`

Explanation A certificate authority certificate was installed for use by proxy services.

Recommended Action No action is required. A record of this certificate authority certificate can be archived for reference or auditing.

Error Message `%STE-6-PKI_CERT_HIST_CLEARED: [dec] certificate history records have been cleared from memory.`

Explanation The specified number of certificate history records were cleared from the system memory.

Recommended Action No action is required.

Error Message `%STE-6-PKI_CERT_HIST_DISABLED: Certificate history of proxy services has been disabled.`

Explanation The proxy service certificate history function was disabled. Certificate installation and deletion records will be cleared from memory. No new history records will be written into memory.

Recommended Action No action is required.

Error Message `%STE-6-PKI_CERT_HIST_ENABLED: Proxy Service Certificate History has been enabled.`

Explanation The proxy service certificate history function was enabled. Certificate installation and deletion records will be written into memory.

Recommended Action Enter the **show ssl-proxy certificate-history** command to display certificate history records. Save the output of this command to a file for archiving.

Error Message `%STE-6-PKI_CERT_HIST_RECORD_THRESHOLD: [dec] certificate history records have been logged to memory\n. Maximum of [dec] can be logged before the oldest ones are overwritten.`

Explanation There is a maximum number of certificate history records that can be saved to memory. The maximum number will be reached soon. Older records will be overwritten.

Recommended Action Enter the **show ssl-proxy certificate-history** command to display certificate history records. To prevent the loss of older records, save the output of this command to a file for archiving.

Error Message `%STE-6-PKI_CERT_ROLLOVER_BEGIN: The process of rolling over the certificate without the sudden loss of services has begun for the proxy service: [chars], trustpoint: [chars]`

Explanation The key pair, the certificate, or the trustpoint assigned to the specified proxy service has been modified. Until the new certificate is received, the old certificate will be used.

Recommended Action Finish the rollover process by enrolling or importing the modified trustpoint. Enter the **show ssl-proxy service** command to display information about certificates, key pairs, and trustpoints associated with the specified proxy service.

Error Message `%STE-6-PKI_CERT_ROLLOVER_END: The process of rolling over the certificate without the sudden loss of services has ended for the proxy service: [chars], trustpoint: [chars]`

Explanation A new certificate has been received for the specified proxy service. The old certificate will be deleted when all connections using it are finished.

Recommended Action No action is required. Enter the **show ssl-proxy service** command to display more information about new and old certificates.

Error Message `%STE-6-PKI_SERVICE_CERT_DELETE: Proxy: [chars], Trustpoint [chars], Key [chars], Serial#: [chars], Index: [dec]`

Explanation A certificate was deleted for a proxy service.

Recommended Action No action is required. A record of this deletion can be archived for reference or auditing.

Error Message `%STE-6-PKI_SERVICE_CERT_INSTALL: Proxy: [chars], Trustpoint: [chars], Key: [chars], Serial#: [chars], Index: [dec]`

Explanation A certificate was installed for a proxy service.

Recommended Action No action is required. A record of this certificate can be archived for reference or auditing.

Error Message `%STE-6-PKI_TEST_CERT_INSTALL: Test key and certificate was installed into NVRAM in a PKCS#12 file.`

Explanation A PKCS12 file, containing a key pair and a certificate chain that can be used for testing purposes, was copied from memory into the NVRAM device.

Recommended Action No action is required.

Error Message `%STE-6-PROXY_CERT_EXPIRING_TRAP_DISABLED: SNMP trap for proxy service certificate expiration warning has been disabled.`

Explanation No SNMP traps will be issued when a proxy service certificate is going to expire or has expired.

Recommended Action No action is required.

Error Message `%STE-6-PROXY_CERT_EXPIRING_TRAP_ENABLED: SNMP trap for proxy service certificate expiration warning has been enabled.`

Explanation When the certificate of a proxy service is going to expire or has expired within a time interval, an SNMP trap is issued. This time interval can be configured by the command **ssl-proxy pki certificate check-expiring interval**. If this time interval is set to zero, no SNMP traps are issued, and the internal memory for which traps have been sent also is cleared. The next time that the interval is set to a positive value, the proxy service certificates are periodically checked every 30 minutes for expiration, and SNMP traps are issued.

Recommended Action No action is required.

Error Message `%STE-6-PROXY_OPER_STATUS_TRAP_DISABLED: SNMP trap for proxy service operational status change has been disabled.`

Explanation When the operational status of a proxy service is changed, a SNMP trap will not be issued.

Recommended Action No action is required.

Error Message `%STE-6-PROXY_OPER_STATUS_TRAP_ENABLED: SNMP trap for proxy service operational status change has been enabled.`

Explanation When the operational status of a proxy service is changed, a SNMP trap will be issued.

Recommended Action No action is required.

STE-7

Error Message `%STE-7-IPC_REQUEST_RESPONSE_MISMATCH: IPC module received a message where the request and response do not match.`

Explanation IPC received a message that does not have a corresponding valid request.

Recommended Action If this situation is affecting the functionality of the module, contact your Cisco technical support representative

N

R

S

T

V