Catalyst 6500 Series Switch SSL Services Module System Message Guide

Release 3.1

CONTENTS

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 3.x*

- *Catalyst 6500 Series SSL Services Module Installation and Verification Note*

- *Catalyst 6500 Series SSL Services Module Configuration Note*

- *Catalyst 6500 Series 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*

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

CHAPTER**1**

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-0

Error Message `%STE-0-PANIC: [chars]`

   Explanation   An unrecoverable internal panic condition has occurred.

   Recommended Action   Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

   If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the

representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

STE-1

Error Message %STE-1-ALERT: [chars]

Explanation A condition that should be corrected immediately has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

STE-2

Error Message %STE-2-CRITICAL: [chars]

Explanation A critical condition has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages,

these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

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 the %STE-2-IPC_HEALTH_PROBE_HEAD and %STE-2-IPC_HEALTH_PROBE_TAIL messages. 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.

Error Message %STE-2-SVC_DOWN_REASON: ssl-proxy service [chars] changed state to DOWN due to [chars].

Explanation The SSL proxy service has gone into a down state because of the reason given in the message text.

Recommended Action No action is required.

Error Message %STE-2-UPDOWN: ssl-proxy service [chars] changed state to [chars]

Explanation The SSL proxy service state changed.

Recommended Action No action is required.

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 occurs 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 interprocess communication (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 the module cannot process 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 has failed to allocate a buffer. The software allocates buffers to send IPC messages. 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 occurs 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 has failed to allocate a buffer. The software allocates buffers to send IPC messages. 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 occurs 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 information.

Error Message `%STE-3-ERROR: [chars]`

Explanation An error involving the WebVPN Services Module has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the

representative with the output of the **show logging** and **show tech-support**
commands and your pertinent troubleshooting logs in a nonzipped, plain-text
(.txt) format.

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-IPC_STATUS_NOT_OK: IPC module received a message with a status that was not ok.`

    Explanation An IPC module received a message with an invalid status. This condition can occur if the IPC module does not support the latest version of the operational code.

    Recommended Action No action is required.

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 trust point assigned to the specified proxy service. Correct the key type or size, and reenroll the certificate. Remove the trust point 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 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 trust point assigned for the proxy service. Correct the key type or size, and reenroll the certificate. Remove the trust point 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 the key type that was configured for the SSL proxy service.

> **Recommended Action** Regenerate a key pair of the same type that is 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 the key type that was configured for the SSL proxy service.

> **Recommended Action** Regenerate a key pair of the same type that is 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 trust point name used for the new certificate is different from the current trust point, reassign the new trust point 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.

Error Message `%STE-4-WARNING: [chars]`

Explanation   A warning-level error has occurred.

Recommended Action   Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

STE-5

Error Message %STE-5-NOTICE: [chars]

Explanation An internal error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

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 connections that have been used for a long time remain after rollover, some entries might still be used by old certificates. Clear the connections and restart the service.

STE-6

Error Message %STE-6-CONTEXT: [chars] context name: [chars]

Explanation The context configuration has been added, modified or deleted.

Recommended Action No action is required.

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. Traffic processing might be adversely affected
while the tests are being run.

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-HTTP_HEADER_INSERTION_POLICY: [chars] policy name: [chars]

   Explanation The configuration for the header insertion policy has been changed, added or deleted.

   Recommended Action No action is required.

Error Message %STE-6-INFO: [chars]

   Explanation This message provides information regarding the status or configuration of the system.

   Recommended Action This message indicates normal system operation. 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 attempts to resend the message. If you continue to see this message, contact your Cisco technical support representative.

Error Message %STE-6-KEY_CONFIG: [chars] key name: [chars], usage: [chars]

   Explanation The key configuration has been added, modified or deleted.

   Recommended Action No action is required.

Error Message %STE-6-NVRAM_DOWNGRADE_NOT_READY

Explanation The configuration is not 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 (CA) 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 and 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 (CA) certificate was installed for use by proxy services.

  Recommended Action No action is required. A record of this CA 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 and 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 trust point 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 trust point. Enter the **show ssl-proxy service** command to display information about certificates, key pairs, and trust points 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 entering the **ssl-proxy pki certificate check-expiring interval** command. 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.

Error Message   %STE-6-SBETH_TX_UNDERFLOW: A MAC TX FIFO Underflow was detected on MAC [dec].\nProcess traceback: [chars]

Explanation   A MAC Tx FIFO underflow condition has been detected.

Recommended Action   No action is required.

Error Message   %STE-6-SSL_POLICY: [chars] policy name: [chars]

Explanation   The SSL policy configuration has been added, modified or deleted.

Recommended Action   No action is required.

Error Message %STE-6-TCP_POLICY: [chars] policy name: [chars]

> **Explanation** The TCP policy configuration has been added, modified or deleted.

> **Recommended Action** No action is required.

Error Message %STE-6-TCP_PROBE_POLICY: [chars] policy name: [chars]

> **Explanation** The policy configuration for the TCP probe has been added, modified or deleted.

> **Recommended Action** No action is required.

Error Message %STE-6-TRUSTPOINT: [chars] trustpoint for service: [chars], key_type: [chars], trust_point_label: [chars]

> **Explanation** The trust point configuration has been added, modified or deleted.

> **Recommended Action** No action is required.

Error Message %STE-6-URL_REWRITE_POLICY: [chars] policy name: [chars]

> **Explanation** The policy configuration for the URL rewrite function has been added, modified or deleted.

> **Recommended Action** No action is required.

STE-7

Error Message `%STE-7-ASSERT: Assertion Failure ( [chars] @[chars]:[dec] ) : [chars]`

Explanation An assertion operation has failed.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. For resolved software issues, use the Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

If you still require assistance, open a case with the Technical Assistance Center (TAC) at http://tools.cisco.com/ServiceRequestTool/create/launch.do, or contact your Cisco technical support representative and provide the representative with the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs in a nonzipped, plain-text (.txt) format.

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.

I N D E X

T

time stamp designations

See date/time stamp designations

traceback reports **1-3**

V

variable fields

definition **1-3**

table **1-3**

W

warning-level 4 messages

See STE-4 messages