



## 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

