Syslog Messages 602101 to 622102

This chapter contains the following sections:

Messages 602101 to 609002

This section includes messages from 602101 to 609002.

602101

Error Message `%FTD-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address , src_addr=source_address , prot=protocol`

Explanation The Secure Firewall Threat Defense device sent an ICMP destination unreachable message and fragmentation is needed.

Recommended Action Make sure that the data is sent correctly.

602103

Error Message `%FTD-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.`

Explanation The MTU of an SA was changed. When a packet is received for an IPsec tunnel, the corresponding SA is located and the MTU is updated based on the MTU suggested in the ICMP packet. If the suggested MTU is greater than 0 but less than 256, then the new MTU is set to 256. If the suggested MTU is 0, the old MTU is reduced by 256 or it is set to 256—whichever value is greater. If the suggested MTU is greater than 256, then the new MTU is set to the suggested value.

- src_addr—IP address of the PMTU sender
- rcvd_mtu—Suggested MTU received in the PMTU message
- peer_addr—IP address of the IPsec peer
- spi—IPsec Security Parameter Index
- username—Username associated with the IPsec tunnel
- old_mtu—Previous MTU associated with the IPsec tunnel

- new_mtu—New MTU associated with the IPsec tunnel

Recommended Action None required.

602104

Error Message `%FTD-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr , PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu , for SA with peer peer_addr , SPI spi , tunnel name username .`

Explanation An ICMP message was received indicating that a packet sent over an IPsec tunnel exceeded the path MTU, and the suggested MTU was greater than or equal to the current MTU. Because the MTU value is already correct, no MTU adjustment is made. This may happen when multiple PMTU messages are received from different intermediate stations, and the MTU is adjusted before the current PMTU message is processed.

- **src_addr**—IP address of the PMTU sender
- **rcvd_mtu**—Suggested MTU received in the PMTU message
- **curr_mtu**—Current MTU associated with the IPsec tunnel
- **peer_addr**—IP address of the IPsec peer
- **spi**—IPsec Security Parameter Index
- *username* —Username associated with the IPsec tunnel

Recommended Action None required.

602303

Error Message `%FTD-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been created.`

Explanation A new SA was created.

- direction—SA direction (inbound or outbound)
- tunnel_type—SA type (remote access or L2L)
- spi—IPsec Security Parameter Index
- local_IP—IP address of the tunnel local endpoint
- remote_IP—IP address of the tunnel remote endpoint
- >*username* —Username associated with the IPsec tunnel

Recommended Action None required.

602304

Error Message `%FTD-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been deleted.`

Explanation An SA was deleted.

- direction—SA direction (inbound or outbound)
- tunnel_type—SA type (remote access or L2L)
- spi—IPsec Security Parameter Index
- local_IP—IP address of the tunnel local endpoint
- remote_IP—IP address of the tunnel remote endpoint

- >*username* —Username associated with the IPsec tunnel

Recommended Action None required.

602305

Error Message `%FTD-3-602305: IPSEC: SA creation error, source source address , destination destination address , reason error string`

Explanation An error has occurred while creating an IPsec security association.

Recommended Action This is typically a transient error condition. If this message occurs consistently, contact the Cisco TAC.

602306

Error Message `%FTD-3-602306: IPSEC: SA change peer IP error, SPI: IPsec SPI, (src {original src IP address | original src port}, dest {original dest IP address| original dest port} => src {new src IP address | new src port}, dest: {new dest IP address | new dest port}), reason failure reason`

Explanation An error has occurred while updating an IPsec tunnel's peer address for Mobile IKE and the peer address could not be changed.

Recommended Action This is typically a transient error condition. If this message occurs consistently, contact the Cisco TAC.

604101

Error Message `%FTD-6-604101: DHCP client interface interface_name : Allocated ip = IP_address , mask = netmask , gw = gateway_address`

Explanation The Secure Firewall Threat Defense DHCP client successfully obtained an IP address from a DHCP server. The dhcpc command statement allows the Secure Firewall Threat Defense device to obtain an IP address and network mask for a network interface from a DHCP server, as well as a default route. The default route statement uses the gateway address as the address of the default router.

Recommended Action None required.

604102

Error Message `%FTD-6-604102: DHCP client interface interface_name : address released`

Explanation The Secure Firewall Threat Defense DHCP client released an allocated IP address back to the DHCP server.

Recommended Action None required.

604103

Error Message `%FTD-6-604103: DHCP daemon interface interface_name : address granted MAC_address (IP_address )`

Explanation The Secure Firewall Threat Defense DHCP server granted an IP address to an external client.

Recommended Action None required.

604104

Error Message `%FTD-6-604104: DHCP daemon interface interface_name : address released build_number (IP_address )`

Explanation An external client released an IP address back to the Secure Firewall Threat Defense DHCP server.

Recommended Action None required.

604105

Error Message `%FTD-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name . Reply exceeds options field size (options_field_size ) by number_of_octets octets.`

Explanation An administrator can configure the DHCP options to return to the DHCP client. Depending on the options that the DHCP client requests, the DHCP options for the offer could exceed the message length limits. A DHCP offer cannot be sent, because it will not fit within the message limits.

- *hardware_address* —The hardware address of the requesting client.
- *interface_name*— The interface to which server messages are being sent and received
- *options_field_size* —The maximum options field length. The default is 312 octets, which includes 4 octets to terminate.
- *number_of_octets* —The number of exceeded octets.

Recommended Action Reduce the size or number of configured DHCP options.

604201

Error Message `%FTD-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

Explanation This syslog is displayed whenever DHCPv6 PD client is received with delegated prefix from PD server as part of initial 4-way exchange. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for delegated prefixes.

Recommended Action None.

604202

Error Message `%FTD-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>.`

Explanation This syslog is displayed whenever DHCPv6 PD Client is releasing delegated prefix(s) received from PD Server upon no configuration. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.

Recommended Action None.

604203

Error Message `%FTD-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

Explanation This syslog is displayed whenever DHCPv6 PD Client initiate renewal of previously allocated delegated prefix from PD Server and upon successful. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for delegated prefixes.

Recommended Action None.

604204

Error Message `%FTD-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>.`

Explanation This syslog is displayed whenever DHCPv6 PD Client received delegated prefix is getting expired.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *delegated prefix*—The delegated prefix received from DHCPv6 PD server.

Recommended Action None.

604205

Error Message `%FTD-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds`

Explanation This syslog is displayed whenever DHCPv6 Client address is received from DHCPv6 Server as part of initial 4-way exchange and is valid. In the case of multiple addresses, the syslog is displayed for each received address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.

- *in-seconds*—Associated preferred and valid lifetime in seconds for client address.

Recommended Action None.

604207

Error Message `%FTD-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

Explanation This syslog is displayed whenever DHCPv6 client initiates renewal of previously allocated address from DHCPv6 server. In the case of multiple addresses, the syslog is displayed for each renewed address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for client address.

Recommended Action None.

604206

Error Message `%FTD-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>.`

Explanation DHCPv6 Client is releasing received client address whenever no configuration of DHCPv6 client address is performed. In the case of multiple addresses release, the syslog is displayed for each address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.

Recommended Action None.

604208

Error Message `%FTD-6-604208: DHCPv6 client address <ipv6-address> got expired on interface <client-iface>, received from DHCPv6 server <server-address>`

Explanation This syslog is displayed whenever DHCPv6 client received address is getting expired.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.

Recommended Action None.

605004

Error Message `%FTD-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username "`

Explanation The following form of the message appears when the user attempts to log in to the console:

```
Login denied from serial to console for user "username"
```

An incorrect login attempt or a failed login to the Secure Firewall Threat Defense device occurred. For all logins, three attempts are allowed per session, and the session is terminated after three incorrect attempts. For SSH and Telnet logins, this message is generated after the third failed attempt or if the TCP session is terminated after one or more failed attempts. For other types of management sessions, this message is generated after every failed attempt. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *source-address*— Source address of the login attempt
- *source-port*— Source port of the login attempt
- *interface*— Destination management interface
- *destination*— Destination IP address
- *service*— Destination service
- *username* — Destination management interface

Recommended Action If this message appears infrequently, no action is required. If this message appears frequently, it may indicate an attack. Communicate with the user to verify the username and password.

605005

Error Message `%FTD-6-605005: Login permitted from source-address /source-port to interface:destination /service for user "username "`

The following form of the message appears when the user logs in to the console:

```
Login permitted from serial to console for user "username"
```

Explanation A user was authenticated successfully, and a management session started.

- *source-address*— Source address of the login attempt
- *source-port*— Source port of the login attempt
- *interface*— Destination management interface
- *destination*— Destination IP address
- *service*— Destination service
- *username*— Destination management interface

Recommended Action None required.

607001

Error Message `%FTD-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message`

Explanation The **fixup sip** command preallocated a SIP connection after inspecting a SIP message . The **connection_type** is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP

- Via UDP
- Route
- RTP
- RTCP

Recommended Action None required.

607002

Error Message `%FTD-4-607002: action_class : action SIP req_resp req_resp_info from src_ifc :sip /sport to dest_ifc :dip /dport ; further_info`

Explanation A SIP classification was performed on a SIP message, and the specified criteria were satisfied. As a result, the configured action occurs.

- *action_class* —The class of the action: SIP Classification for SIP match commands or SIP Parameter for parameter commands
- *action* —The action taken: Dropped, Dropped connection for, Reset connection for, or Masked header flags for
- *req_resp* —Request or Response
- *req_resp_info* —The SIP method name if the type is Request: INVITE or CANCEL. The SIP response code if the type is Response: 100, 183, 200.
- *src_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further_info* —More information appears for SIP match and SIP parameter commands, as follows:

For SIP match commands:

matched Class **id**: **class-name**

For example:

```
matched Class 1234: my_class
```

For SIP parameter commands:

parameter-command: **descriptive-message**

For example:

```
strict-header-validation: Mandatory header field Via is missing
state-checking: Message CANCEL is not permitted to create a Dialog.
```

Recommended Action None required.

607003

Error Message `%FTD-6-607003: action_class : Received SIP req_resp req_resp_info from src_ifc :sip /sport to dest_ifc :dip /dport ; further_info`

Explanation A SIP classification was performed on a SIP message, and the specified criteria were satisfied. As a result, the standalone log action occurs.

- *action_class* —SIP classification for SIP match commands or SIP parameter for parameter commands
- *req_resp* —Request or Response
- *req_resp_info* —The SIP method name if the type is Request: INVITE or CANCEL. The SIP response code if the type is Response: 100, 183, 200.
- *src_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address.
- *dport* —The destination port.
- *further_info* —More information appears for SIP match and SIP parameter commands, as follows:

For SIP match commands:

matched Class **id**: **class-name**

For example:

```
matched Class 1234: my_class
```

For SIP parameter commands:

parameter-command: **descriptive-message**

For example:

```
strict-header-validation: Mandatory header field Via is missing
state-checking: Message CANCEL is not permitted to create a Dialog.
```

Recommended Action None required.

607004

Error Message `%FTD-4-607004: Phone Proxy: Dropping SIP message from src_if:src_ip /src_port to dest_if :dest_ip /dest_port with source MAC mac_address due to secure phone database mismatch.`

Explanation The MAC address in the SIP message is compared with the secure database entries in addition to the IP address and interface. If they do not match, then the particular message is dropped.

Recommended Action None required.

608001

Error Message `%FTD-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message`

Explanation The **inspect skinny** command preallocated a Skinny connection after inspecting a Skinny message . The **connection_type** is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP

- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

Recommended Action None required.

608002

Error Message `%FTD-4-608002: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too small`

Explanation A Skinny (SSCP) message was received with an SCCP prefix length less than the minimum length configured.

- *in_ifc* —The input interface
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *out_ifc* —The output interface
- *dest_ip* —The destination IP address of the packet
- *dest_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

Recommended Action If the SCCP message is valid, then customize the Skinny policy map to increase the minimum length value of the SSCP prefix.

608003

Error Message `%FTD-4-608003: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too large`

Explanation A Skinny (SSCP) message was received with an SCCP prefix length greater than the maximum length configured.

- *in_ifc* —The input interface
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *out_ifc* —The output interface
- *dest_ip* —The destination IP address of the packet
- *dest_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

Recommended Action If the SCCP message is valid, then customize the Skinny policy map to increase the maximum length value of the SCCP prefix.

609001

Error Message `%FTD-7-609001: Built local-host zone-name/* :ip-address`

Explanation A network state container was reserved for host **ip-address** connected to zone *zone-name* . The zone-name/* parameter is used if the interface on which the host is created is part of a zone. The asterisk symbolizes all interfaces because hosts do not belong to any one interface.

Recommended Action None required.

609002

Error Message `%FTD-7-609002: Teardown local-host zone-name/* :ip-address duration time`

Explanation A network state container for host **ip-address** connected to zone **zone-name** was removed. The zone-name/* parameter is used if the interface on which the host is created is part of a zone. The asterisk symbolizes all interfaces because hosts do not belong to any one interface.

Recommended Action None required.

Messages 610101 to 622102

This section includes messages from 610101 to 622102.

611101

Error Message `%FTD-6-611101: User authentication succeeded: IP, IP address : Uname: user`

Explanation User authentication succeeded when accessing the Secure Firewall Threat Defense device. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *IP address* —The IP address of the client that succeeded user authentication
- *user* —The user that authenticated

Recommended Action None required.

611102

Error Message `%FTD-6-611102: User authentication failed: IP = IP address, Uname: user`

Explanation User authentication failed when attempting to access the Secure Firewall Threat Defense device. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *IP address* —The IP address of the client that failed user authentication
- *user* —The user that authenticated

Recommended Action None required.

611103

Error Message `%FTD-5-611103: User logged out: Uname: user`

Explanation The specified user logged out.

Recommended Action None required.

611104

Error Message `%FTD-5-611104: Serial console idle timeout exceeded`

Explanation The configured idle timeout for the Secure Firewall Threat Defense serial console was exceeded because of no user activity.

Recommended Action None required.

611301

Error Message `%FTD-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address`

Explanation The VPN client policy for client mode with no split tunneling was installed.

Recommended Action None required.

611302

Error Message `%FTD-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling`

Explanation The VPN client policy for network extension mode with no split tunneling was installed.

Recommended Action None required.

611303

Error Message `%FTD-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask`

Explanation The VPN client policy for client mode with split tunneling was installed.

Recommended Action None required.

611304

Error Message `%FTD-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask`

Explanation The VPN client policy for network extension mode with split tunneling was installed.

Recommended Action None required.

611305

Error Message `%FTD-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address`

Explanation The VPN client policy for DHCP was installed.

Recommended Action None required.

611306

Error Message `%FTD-6-611306: VPNClient: Perfect Forward Secrecy Policy installed`

Explanation Perfect forward secrecy was configured as part of the VPN client download policy.

Recommended Action None required.

611307

Error Message `%FTD-6-611307: VPNClient: Head end: IP_address`

Explanation The VPN client is connected to the specified headend.

Recommended Action None required.

611308

Error Message `%FTD-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string`

Explanation A split DNS policy was installed as part of the VPN client downloaded policy.

Recommended Action None required.

611309

Error Message `%FTD-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address`

Explanation A VPN client is disconnecting and uninstalling a previously installed policy.

Recommended Action None required.

611310

Error Message `%FTD-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address`

Explanation The VPN client Xauth succeeded with the specified headend.

Recommended Action None required.

611311

Error Message `%FTD-6-611311: VNPClient: XAUTH Failed: Peer: IP_address`

Explanation The VPN client Xauth failed with the specified headend.

Recommended Action None required.

611312

Error Message `%FTD-6-611312: VPNClient: Backup Server List: reason`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the Easy VPN server downloaded a list of backup servers to the Secure Firewall Threat Defense device. This list overrides any backup servers that you have configured locally. If the downloaded list is empty, then the Secure Firewall Threat Defense device uses no backup servers. The **reason** is one of the following messages:

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers

Recommended Action None required.

611313

Error Message `%FTD-3-611313: VPNClient: Backup Server List Error: reason`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, and the Easy VPN server downloads a backup server list to the Secure Firewall Threat Defense device, the list includes an invalid IP address or a hostname. The Secure Firewall Threat Defense device does not support DNS, and therefore does not support hostnames for servers, unless you manually map a name to an IP address using the **name** command.

Recommended Action On the Easy VPN server, make sure that the server IP addresses are correct, and configure the servers as IP addresses instead of hostnames. If you must use hostnames on the server, use the **name** command on the Easy VPN remote device to map the IP addresses to names.

611314

Error Message `%FTD-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the director server of the load balancing group redirected the Secure Firewall Threat Defense device to connect to a particular server.

Recommended Action None required.

611315

Error Message `%FTD-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, it disconnected from a load balancing cluster server.

Recommended Action None required.

611316

Error Message `%FTD-6-611316: VPNClient: Secure Unit Authentication Enabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy enabled SUA.

Recommended Action None required.

611317

Error Message `%FTD-6-611317: VPNClient: Secure Unit Authentication Disabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy disabled SUA.

Recommended Action None required.

611318

Error Message `%FTD-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy enabled IUA for users on the Secure Firewall Threat Defense device inside network.

- **IP_address**—The server IP address to which the Secure Firewall Threat Defense device sends authentication requests.
- **port**—The server port to which the Secure Firewall Threat Defense device sends authentication requests
- **time**—The idle timeout value for authentication credentials

Recommended Action None required.

611319

Error Message `%FTD-6-611319: VPNClient: User Authentication Disabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy disabled IUA for users on the Secure Firewall Threat Defense inside network.

Recommended Action None required.

611320

Error Message `%FTD-6-611320: VPNClient: Device Pass Thru Enabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy enabled device pass-through. The device pass-through feature allows devices that cannot perform authentication (such as an IP phone) to be exempt from authentication when IUA is enabled. If the Easy VPN server enabled this feature, you can specify the devices that should be exempt from authentication (IUA) using the **vpnclient mac-exempt** command on the Secure Firewall Threat Defense device.

Recommended Action None required.

611321

Error Message `%FTD-6-611321: VPNClient: Device Pass Thru Disabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy disabled device pass-through.

Recommended Action None required.

611322

Error Message `%FTD-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device and the downloaded VPN policy disabled SUA, the Easy VPN server uses two-factor/SecurID/cryptocard-based authentication mechansims to authenticate the Secure Firewall Threat Defense device using XAUTH.

Recommended Action If you want the Easy VPN remote device to be authenticated using two-factor/SecureID/cryptocard-based authentication mechanisms, enable SUA on the server.

611323

Error Message `%FTD-6-611323: VPNClient: Duplicate split nw entry`

Explanation When the Secure Firewall Threat Defense device is an Easy VPN remote device, the downloaded VPN policy included duplicate split network entries. An entry is considered a duplicate if it matches both the network address and the network mask.

Recommended Action Remove duplicate split network entries from the VPN policy on the Easy VPN server.

612001

Error Message `%FTD-5-612001: Auto Update succeeded:`*`filename`*` , version:`*`number`*

Explanation An update from an Auto Update server was successful. The **filename** variable is image, ASDM file, or configuration. The **version number** variable is the version number of the update.

Recommended Action None required.

612002

Error Message `%FTD-4-612002: Auto Update failed:`*`filename`*` , version:`*`number`*` , reason:`*`reason`*

Explanation An update from an Auto Update server failed.

- **filename**—Either an image file, an ASDM file, or a configuration file.
- **number**—The version number of the update.
- **reason**—The failure reason, which may be one of the following:

- Failover module failed to open stream buffer

- Failover module failed to write data to stream buffer

- Failover module failed to perform control operation on stream buffer

- Failover module failed to open flash file

- Failover module failed to write data to flash

- Failover module operation timeout

- Failover command link is down

- Failover resource is not available

- Invalid failover state on mate

- Failover module encountered file transfer data corruption

- Failover active state change

- Failover command EXEC failed

- The image cannot run on current system

- Unsupported file type

Recommended Action Check the configuration of the Auto Update server. Check to see if the standby unit is in the failed state. If the Auto Update server is configured correctly, and the standby unit is not in the failed state, contact the Cisco TAC.

612003

Error Message `%FTD-4-612003:Auto Update failed to contact:`*`url`* `, reason:`*`reason`*

Explanation The Auto Update daemon was unable to contact the specified URL **url**, which can be the URL of the Auto Update server or one of the file server URLs returned by the Auto Update server. The **reason** field describes why the contact failed. Possible reasons for the failure include no response from the server, authentication failed, or a file was not found.

Recommended Action Check the configuration of the Auto Update server.

613001

Error Message `%FTD-6-613001: Checksum Failure in database in area` *`string`* `Link State Id` *`IP_address`* `Old Checksum` *`number`* `New Checksum` *`number`*

Explanation OSPF has detected a checksum error in the database because of memory corruption.

Recommended Action Restart the OSPF process.

613002

Error Message `%FTD-6-613002: interface` *`interface_name`* `has zero bandwidth`

Explanation The interface reported its bandwidth as zero.

Recommended Action Copy the message exactly as it appears, and report it to the Cisco TAC.

613003

Error Message `%FTD-6-613003:` *`IP_address netmask`* `changed from area` *`string`* `to area` *`string`*

Explanation An OSPF configuration change has caused a network range to change areas.

Recommended Action Reconfigure OSPF with the correct network range.

613004

Error Message `%FTD-3-613004: Internal error: memory allocation failure`

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears, and report it to Cisco TAC.

613005

Error Message `%FTD-3-613005: Flagged as being an ABR without a backbone area`

Explanation The router was flagged as an Area Border Router (ABR) without a backbone area in the router.

Recommended Action Restart the OSPF process.

613006

Error Message `%FTD-3-613006: Reached unknown state in neighbor state machine`

Explanation An internal software error in this router has resulted in an invalid neighbor state during database exchange.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

613007

Error Message `%FTD-3-613007: area string lsid IP_address mask netmask type number`

Explanation OSPF is trying to add an existing LSA to the database.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

613008

Error Message `%FTD-3-613008: if inside if_state number`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

613011

Error Message `%FTD-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id`

Explanation An OSPF process is being reset, and it is going to select a new router ID. This action brings down all virtual links. To make them work again, the virtual link configuration needs to be changed on all virtual link neighbors.

Recommended Action Change the virtual link configuration on all the virtual link neighbors to reflect the new router ID.

613013

Error Message `%FTD-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address/mask type number has no corresponding LSA`

Explanation OSPF found inconsistency between its database and the IP routing table.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613014

Error Message `%FTD-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string`

Explanation OSPF interfaces attached to MTR-compatible OSPF areas require the base topology to be enabled.

Recommended Action None.

613015

Error Message `%FTD-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask`

Explanation A router is extensively re-originating or flushing the LSA reported by this error message.

Recommended Action If this router is flushing the network LSA, it means the router received a network LSA whose LSA ID conflicts with the IP address of one of the router's interfaces and flushed the LSA out of the network. For OSPF to function correctly, the IP addresses of transit networks must be unique. Conflicting routers are the router reporting this error message and the router with the OSPF router ID reported as adv-rtr in this message. If this router is re-originating an LSA, it is highly probable that some other router is flushing this LSA out of the network. Find that router and avoid the conflict. The conflict for a Type-2 LSA may be due to a duplicate LSA ID. For a Type-5 LSA, it may be a duplicate router ID on the router reporting this error message and on the routers connected to a different area. In an unstable network, this message may also warn of extensive re-origination of the LSA for some other reason. Contact Cisco TAC to investigate this type of case.

613016

Error Message `%FTD-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.`

Explanation The router tried to build a router-LSA that is larger than the huge system buffer size or the OSPF protocol imposed maximum.

Recommended Action If the reported total length (LSA size plus overhead) is larger than the huge system buffer size but less than 65535 bytes (the OSPF protocol imposed maximum), you may increase the huge system buffer size. If the reported total length is greater than 65535, you need to decrease the number of OSPF interfaces in the reported area.

613017

Error Message `%FTD-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address`

Explanation The router received an LSA with an invalid LSA mask because of an incorrect configuration from the LSA originator. As a result, this route is not installed in the routing table.

Recommended Action Find the originating router of the LSA with the bad mask, then correct any misconfiguration of this LSA's network. For further debugging, call Cisco TAC for assistance.

613018

Error Message `%FTD-4-613018: Maximum number of non self-generated LSA has been exceeded "OSPF number" - number LSAs`

Explanation The maximum number of non self-generated LSAs has been exceeded.

Recommended Action Check whether or not a router in the network is generating a large number of LSAs as a result of a misconfiguration.

613019

Error Message `%FTD-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs`

Explanation The threshold for the maximum number of non self-generated LSAs has been reached.

Recommended Action Check whether or not a router in the network is generating a large number of LSAs as a result of a misconfiguration.

613021

Error Message `%FTD-4-613021: Packet not written to the output queue`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613022

Error Message `%FTD-4-613022: Doubly linked list linkage is NULL`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613023

Error Message `%FTD-4-613023: Doubly linked list prev linkage is NULL number`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613024

Error Message `%FTD-4-613024: Unrecognized timer number in OSPF string`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613025

Error Message `%FTD-4-613025: Invalid build flag number for LSA IP_address, type number`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613026

Error Message `%FTD-4-613026: Can not allocate memory for area structure`

Explanation An internal error occurred.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613027

Error Message `%FTD-6-613027: OSPF process number removed from interface interface_name`

Explanation The OSPF process was removed from the interface because of an IP VRF.

Recommended Action None.

613028

Error Message `%FTD-6-613028: Unrecognized virtual interface intetface_name. Treat it as loopback stub route`

Explanation The virtual interface type was not recognized by OSPF, so it is treated as a loopback interface stub route.

Recommended Action None.

613029

Error Message `%FTD-3-613029: Router-ID IP_address is in use by ospf process number`

Explanation The Secure Firewall Threat Defense device attempted to assign a router ID that is in use by another process.

Recommended Action Configure another router ID for one of the processes.

613030

Error Message `%FTD-4-613030: Router is currently an ASBR while having only one area which is a stub area`

Explanation An ASBR must be attached to an area that can carry AS external or NSSA LSAs.

Recommended Action Make the area to which the router is attached into an NSSA or regular area.

613031

Error Message `%FTD-4-613031: No IP address for interface inside`

Explanation The interface is not point-to-point and is unnumbered.

Recommended Action Change the interface type or give the interface an IP address.

613032

Error Message `%FTD-3-613032: Init failed for interface inside, area is being deleted. Try again.`

Explanation The interface initialization failed. The possible reasons include the following:

- The area to which the interface is being attached is being deleted.
- It was not possible to create a neighbor datablock for the local router.

Recommended Action Remove the configuration command that covers the interface and then try it again.

613033

Error Message `%FTD-3-613033: Interface inside is attached to more than one area`

Explanation The interface is on the interface list for an area other than the one to which the interface links.

Recommended Action Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

613034

Error Message `%FTD-3-613034: Neighbor IP_address not configured`

Explanation The configured neighbor options are not valid.

Recommended Action Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

613035

Error Message `%FTD-3-613035: Could not allocate or find neighbor IP_address`

Explanation An internal error occurred.

Recommended Action Copy the error message exactly as it appears, and report it to Cisco TAC.

613036

Error Message `%FTD-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network`

Explanation The configured neighbor was found on an NBMA network and either the cost or database-filter option was configured. These options are only allowed on point-to-multipoint type networks.

Recommended Action Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

613037

Error Message `%FTD-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

Explanation The configured neighbor was found on a point-to-multipoint network and either the poll or priority option was configured. These options are only allowed on NBMA-type networks.

Recommended Action Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

613038

Error Message `%FTD-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network`

Explanation The configured neighbor was found on a point-to-multipoint broadcast network. Either the **cost** or **database-filter** option needs to be configured.

Recommended Action Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

613039

Error Message `%FTD-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks`

Explanation The configured neighbor was found on a network for which the network type was neither NBMA nor point-to-multipoint.

Recommended Action None.

613040

Error Message `%FTD-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number`

Explanation The router indicated in this message has originated an LSA with an invalid metric. If this is a router LSA and the link metric is zero, a risk of routing loops and traffic loss in the network exists.

Recommended Action Configure a valid metric for the given LSA type and link type on the router originating on the reported LSA.

613041

Error Message `%FTD-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge`

Explanation An internal error has corrected itself. There is no operational effect related to this error message.

Recommended Action Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support ospf** commands.

613042

Error Message `%FTD-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared`

Explanation There is no viable forwarding address in the NSSA area. As a result, the P-bit must be cleared and the Type 7 LSA is not translated into a Type 5 LSA by the NSSA translator. See RFC 3101.

Recommended Action Configure at least one interface in the NSSA with an advertised IP address. A loopback is preferable because an advertisement does not depend on the underlying layer 2 state.

613043

Error Message `%FTD-6-613043:`

Explanation A negative database reference count occurred.

Recommended Action Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support ospf** commands.

613101

Error Message `%FTD-6-613101: Checksum Failure in database in area` *`s`* `Link State Id` *`i`* `Old Checksum` *`#x`* `New Checksum` *`#x`*

Explanation OSPF has detected a checksum error in the database because of memory corruption.

Recommended Action Restart the OSPF process.

613102

Error Message `%FTD-6-613102: interface s has zero bandwidth`

Explanation The interface reports its bandwidth as zero.

Recommended Action None required.

613103

Error Message `%FTD-6-613103: i m changed from area AREA_ID_STR to area AREA_ID_STR`

Explanation An OSPF configuration change has caused a network range to change areas.

Recommended Action None required.

613104

Error Message `%FTD-6-613104: Unrecognized virtual interface IF_NAME .`

Explanation The virtual interface type was not recognized by OSPFv3, so it is treated as a loopback interface stub route.

Recommended Action None required.

614001

Error Message `%FTD-6-614001: Split DNS: request patched from server: IP_address to server: IP_address`

Explanation Split DNS is redirecting DNS queries from the original destination server to the primary enterprise DNS server.

Recommended Action None required.

614002

Error Message `%FTD-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address`

Explanation Split DNS is redirecting DNS queries from the enterprise DNS server to the original destination server.

Recommended Action None required.

615001

Error Message `%FTD-6-615001: vlan number not available for firewall interface`

Explanation The switch removed the VLAN from the Secure Firewall Threat Defense device.

Recommended Action None required.

615002

Error Message `%FTD-6-615002: vlan number available for firewall interface`

Explanation The switch added the VLAN to the Secure Firewall Threat Defense device.

Recommended Action None required.

621001

Error Message `%FTD-6-621001: Interface` *interface_name* does not support multicast, not enabled

Explanation An attempt was made to enable PIM on an interface that does not support multicast.

Recommended Action If the problem persists, contact the Cisco TAC.

621002

Error Message `%FTD-6-621002: Interface` *interface_name* does not support multicast, not enabled

Explanation An attempt was made to enable IGMP on an interface that does not support multicast.

Recommended Action If the problem persists, contact the Cisco TAC.

621003

Error Message `%FTD-6-621003: The event queue size has exceeded` *number*

Explanation The number of event managers created has exceeded the expected amount.

Recommended Action If the problem persists, contact the Cisco TAC.

621006

Error Message `%FTD-6-621006: Mrib disconnected`, (*IP_address* ,*IP_address*) event cancelled

Explanation A packet triggering a data-driven event was received, but the connection to the MRIB was down. The notification was canceled.

Recommended Action If the problem persists, contact the Cisco TAC.

621007

Error Message `%FTD-6-621007: Bad register from` *interface_name* :*IP_address* to *IP_address* for (*IP_address* , *IP_address*)

Explanation A PIM router configured as a rendezvous point or with NAT has received a PIM register packet from another PIM router. The data encapsulated in this packet is invalid.

Recommended Action The sending router is erroneously sending non-RFC registers. Upgrade the sending router.

622001

Error Message `%FTD-6-622001:` *string* tracked route *network mask address* , distance *number* , table *string* , on interface *interface-name*

Explanation A tracked route has been added to or removed from a routing table, which means that the state of the tracked object has changed from up or down.

- *string* —Adding or Removing
- *network* —The network address
- *mask* —The network mask
- *address* —The gateway address
- *number* —The route administrative distance
- *string* —The routing table name
- *interface-name* —The interface name as specified by the **nameif** command

Recommended Action None required.

622101

Error Message `%FTD-6-622101:` Starting regex table compilation for *match_command* ; table entries = *regex_num* entries

Explanation Information on the background activities of regex compilation appear.

- *match_command* —The match command to which the regex table is associated
- *regex_num* —The number of regex entries to be compiled

Recommended Action None required.

622102

Error Message `%FTD-6-622102:` Completed regex table compilation for *match_command* ; table size = *num* bytes

Explanation Information on the background activities of the regex compilation appear.

- *match_command* —The match command to which the regex table is associated
- *num* —The size, in bytes, of the compiled table

Recommended Action None required.