© 2018-2019 Cisco Systems, Inc. All rights reserved.
About This Guide

The following topics explain how to use this guide.

- What’s New in Each Release, on page iii
- About Firepower Threat Defense Syslog Messages, on page v
- Configure the System to Send Syslog Messages, on page viii
- Communications, Services, and Additional Information, on page viii

What’s New in Each Release

This section provides the following new or changed logging information for the Firepower Threat Defense.

<table>
<thead>
<tr>
<th>Version Introduced</th>
<th>Feature or Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>Support for file and malware events</td>
</tr>
<tr>
<td></td>
<td>For details, see Security Event Syslog Message IDs, on page 1 and File and Malware Event Field Descriptions, on page 15.</td>
</tr>
<tr>
<td>6.3</td>
<td>Event type IDs for security events:</td>
</tr>
<tr>
<td></td>
<td>Messages for connection, security intelligence, and intrusion events include an event type ID in the message header.</td>
</tr>
<tr>
<td></td>
<td>For details, see Security Event Syslog Message IDs, on page 1.</td>
</tr>
<tr>
<td>6.3</td>
<td>Omission of empty and unknown values from security event messages:</td>
</tr>
<tr>
<td></td>
<td>Fields with empty or unknown values are omitted from syslog messages for connection, security intelligence, and intrusion events.</td>
</tr>
<tr>
<td>6.3</td>
<td>Syslog Prefix Format:</td>
</tr>
<tr>
<td></td>
<td>The Firepower Threat Defense operating system was using parts of the ASA operating system, including the syslog utility. Therefore, Firepower Threat Defense syslog messages were starting with &quot;%ASA&quot; due to this shared utility. Beginning with release 6.3, the Firepower Threat Defense syslog messages will be starting with &quot;%FTD&quot;</td>
</tr>
<tr>
<td>Version Introduced</td>
<td>Feature or Change</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>6.3</td>
<td><strong>Timestamp Logging:</strong></td>
</tr>
<tr>
<td></td>
<td>Beginning with version 6.3, Firepower Threat Defense provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;166&gt;2018-06-27T12:17:46Z firepower : %FTD-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port</code></td>
</tr>
</tbody>
</table>

| 6.3                | **Documentation improvement** (functionality is not new in this release): |
|                    | Syslog field names and descriptions for connection, security intelligence, and intrusion events. |

This section provides the following new, changed, and deprecated syslog messages for the following Firepower Threat Defense releases.

- **Table 1: New, Changed, and Deprecated Syslog Message for Version 6.5**
- **Table 2: New, Changed, and Deprecated Syslog Messages for Version 6.4**

The following table lists the new, changed, and deprecated syslog messages for Version 6.4. For complete syslog message descriptions, see respective chapters.

**Table 1: New, Changed, and Deprecated Syslog Message for Version 6.5**

<table>
<thead>
<tr>
<th>New Syslog Messages</th>
<th>748011, 748012, 302311, 747042, 747043, 747044, 769007, 769009, 852001, 852002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed Syslog Messages</td>
<td></td>
</tr>
<tr>
<td>Deprecated Syslog Messages</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2: New, Changed, and Deprecated Syslog Messages for Version 6.4**

<table>
<thead>
<tr>
<th>New Syslog Messages</th>
<th>Security events: 430004, 430005 Other: 305017, 308003, 308004, 408101, 408102, 409014, 409015, 409016, 409017, 419004, 419005, 419006, 503002, 503003, 503004, 503005, 737038, 737200-737206, 737400-737407, 747042, 747043, 747044, 768003, 768004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed Syslog Messages</td>
<td>737001-737019, 737031-737036</td>
</tr>
<tr>
<td>Deprecated Syslog Messages</td>
<td></td>
</tr>
</tbody>
</table>
Information in this topic does not apply to messages related to security events.

The following table lists the message classes and the ranges of message IDs that are associated with each class. The valid range for message IDs is between 100000 and 999999.

When a number is skipped in a sequence, the message is no longer in the Firepower Threat Defense device code.

Most of the ISAKMP messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a message when available. If the object is not known at the time the message is generated, the specific `heading = value` combination will not be displayed.

The objects will be prepended as follows:

- Group = `groupname`, Username = `user`, IP = `IP_address`, ...

Where the Group identifies the tunnel group, the Username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

Typically, a traffic session displays the connection numbers/IDs for each flow in the syslog messages. However, for some of the connections, though the connection ID is incremented, the syslog messages does not display the ID. Thus, you may find missing sequence numbers in the connection IDs of the subsequent messages. For example, during a TCP traffic flow, the syslog messages display the connection IDs as 201, 202, 203, and 204 for each flow. When an ICMP flow begins, though the connection ID is internally incremented to 205 and 206, the syslog messages does not display the numbers. When another TCP flow follows, its connection numbers are now displayed as 207, 208, and so on, giving an impression of skipping sequence.

### Table 3: Syslog Message Classes and Associated Message ID Numbers

<table>
<thead>
<tr>
<th>Logging Class</th>
<th>Definition</th>
<th>Syslog Message ID Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auth</strong></td>
<td>User Authentication</td>
<td>109, 113</td>
</tr>
<tr>
<td>---</td>
<td>Access Lists</td>
<td>106</td>
</tr>
<tr>
<td>---</td>
<td>Application Firewall</td>
<td>415</td>
</tr>
<tr>
<td><strong>bridge</strong></td>
<td>Transparent Firewall</td>
<td>110, 220</td>
</tr>
<tr>
<td><strong>ca</strong></td>
<td>PKI Certification Authority</td>
<td>717</td>
</tr>
<tr>
<td><strong>citrix</strong></td>
<td>Citrix Client</td>
<td>723</td>
</tr>
<tr>
<td>---</td>
<td>Clustering</td>
<td>747</td>
</tr>
<tr>
<td>---</td>
<td>Card Management</td>
<td>323</td>
</tr>
<tr>
<td><strong>config</strong></td>
<td>Command Interface</td>
<td>111, 112, 208, 308</td>
</tr>
<tr>
<td>Logging Class</td>
<td>Definition</td>
<td>Syslog Message ID Numbers</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>csd</td>
<td>Secure Desktop</td>
<td>724</td>
</tr>
<tr>
<td>cts</td>
<td>Cisco TrustSec</td>
<td>776</td>
</tr>
<tr>
<td>dap</td>
<td>Dynamic Access Policies</td>
<td>734</td>
</tr>
<tr>
<td>eap, eapoudp</td>
<td>EAP or EAPoUDP for Network Admission Control</td>
<td>333, 334</td>
</tr>
<tr>
<td>eigrp</td>
<td>EIGRP Routing</td>
<td>336</td>
</tr>
<tr>
<td>email</td>
<td>E-mail Proxy</td>
<td>719</td>
</tr>
<tr>
<td></td>
<td>Environment Monitoring</td>
<td>735</td>
</tr>
<tr>
<td>ha</td>
<td>Failover</td>
<td>101, 102, 103, 104, 105, 210, 311, 709, 727</td>
</tr>
<tr>
<td></td>
<td>Identity-based Firewall</td>
<td>746</td>
</tr>
<tr>
<td>ids</td>
<td>Intrusion Detection System</td>
<td>400, 733</td>
</tr>
<tr>
<td></td>
<td>IKEv2 Toolkit</td>
<td>750, 751, 752</td>
</tr>
<tr>
<td>ip</td>
<td>IP Stack</td>
<td>209, 215, 313, 317, 408</td>
</tr>
<tr>
<td>ipaa</td>
<td>IP Address Assignment</td>
<td>735</td>
</tr>
<tr>
<td>ips</td>
<td>Intrusion Protection System</td>
<td>400, 401, 420</td>
</tr>
<tr>
<td></td>
<td>IPv6</td>
<td>325</td>
</tr>
<tr>
<td></td>
<td>Blacklists, Whitelists, and Graylists</td>
<td>338</td>
</tr>
<tr>
<td></td>
<td>Licensing</td>
<td>444</td>
</tr>
<tr>
<td>mdm-proxy</td>
<td>MDM Proxy</td>
<td>802</td>
</tr>
<tr>
<td>nac</td>
<td>Network Admission Control</td>
<td>731, 732</td>
</tr>
<tr>
<td>nacpolicy</td>
<td>NAC Policy</td>
<td>731</td>
</tr>
<tr>
<td>nacsettings</td>
<td>NAC Settings to apply NAC Policy</td>
<td>732</td>
</tr>
<tr>
<td></td>
<td>Network Access Point</td>
<td>713</td>
</tr>
<tr>
<td>np</td>
<td>Network Processor</td>
<td>319</td>
</tr>
<tr>
<td></td>
<td>NP SSL</td>
<td>725</td>
</tr>
<tr>
<td>ospf</td>
<td>OSPF Routing</td>
<td>318, 409, 503, 613</td>
</tr>
<tr>
<td></td>
<td>Password Encryption</td>
<td>742</td>
</tr>
<tr>
<td></td>
<td>Phone Proxy</td>
<td>337</td>
</tr>
<tr>
<td>Logging Class</td>
<td>Definition</td>
<td>Syslog Message ID Numbers</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>rip</td>
<td>RIP Routing</td>
<td>107, 312</td>
</tr>
<tr>
<td>rm</td>
<td>Resource Manager</td>
<td>321</td>
</tr>
<tr>
<td>—</td>
<td>Security events</td>
<td>430</td>
</tr>
<tr>
<td></td>
<td>(Information in this topic does not apply to these events)</td>
<td></td>
</tr>
<tr>
<td>—</td>
<td>Smart Call Home</td>
<td>120</td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP</td>
<td>212</td>
</tr>
<tr>
<td>—</td>
<td>ScanSafe</td>
<td>775</td>
</tr>
<tr>
<td>ssl</td>
<td>SSL Stack</td>
<td>725</td>
</tr>
<tr>
<td>svc</td>
<td>SSL VPN Client</td>
<td>722</td>
</tr>
<tr>
<td>—</td>
<td>Threat Detection</td>
<td>733</td>
</tr>
<tr>
<td>tre</td>
<td>Transactional Rule Engine</td>
<td>780</td>
</tr>
<tr>
<td>—</td>
<td>UC-IME</td>
<td>339</td>
</tr>
<tr>
<td>tag-switching</td>
<td>Service Tag Switching</td>
<td>779</td>
</tr>
<tr>
<td>vm</td>
<td>VLAN Mapping</td>
<td>730</td>
</tr>
<tr>
<td>vpdn</td>
<td>PPTP and L2TP Sessions</td>
<td>213, 403, 603</td>
</tr>
<tr>
<td>vpn</td>
<td>IKE and IPsec</td>
<td>316, 320, 402, 404, 501, 602, 702, 713, 714, 715</td>
</tr>
<tr>
<td>vpnc</td>
<td>VPN Client</td>
<td>611</td>
</tr>
<tr>
<td>vpnfo</td>
<td>VPN Failover</td>
<td>720</td>
</tr>
<tr>
<td>vpnlb</td>
<td>VPN Load Balancing</td>
<td>718</td>
</tr>
<tr>
<td>—</td>
<td>VXLAN</td>
<td>778</td>
</tr>
<tr>
<td>webfo</td>
<td>WebVPN Failover</td>
<td>721</td>
</tr>
<tr>
<td>webvpn</td>
<td>WebVPN and AnyConnect Client</td>
<td>716</td>
</tr>
<tr>
<td>—</td>
<td>NAT and PAT</td>
<td>305</td>
</tr>
</tbody>
</table>
Configure the System to Send Syslog Messages

For information about how to configure logging and SNMP, see the *Firepower Management Center Configuration Guide* or Firepower Threat Defense configuration guide for your release.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you’re looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

**Cisco Bug Search Tool**

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
CHAPTER 1

Security Event Syslog Messages

• Security Event Syslog Message IDs, on page 1
• Intrusion Event Field Descriptions, on page 1
• Connection and Security Intelligence Event Field Descriptions, on page 5
• File and Malware Event Field Descriptions, on page 15
• History for Security Event Syslog Messages, on page 21

Security Event Syslog Message IDs

• 430001: Intrusion event
  This ID was introduced in release 6.3.
• 430002: Connection event logged at beginning of connection
  This ID was introduced in release 6.3.
• 430003: Connection event logged at end of connection
  This ID was introduced in release 6.3.
• 430004: File events
  Syslog support for these events was introduced in release 6.4.
• 430005: File malware events
  Syslog support for these events was introduced in release 6.4.

Intrusion Event Field Descriptions

Note
Starting in release 6.3, fields with empty or unknown values are not included in syslog messages.

AccessControlRuleName
This field is included in applicable intrusion event syslog messages starting in release 6.5.
The access control rule that invoked the intrusion policy that generated the event. Default Action indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.

This field is empty (or, for syslog messages, omitted) if there is:

- No associated rule/default action: Intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the default intrusion policy.
- No associated connection event: The connection event logged for the session has been purged from the database, for example, if connection events have higher turnover than intrusion events.

**ACPolicy**

The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.

**ApplicationProtocol**

The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.

**Classification**

The classification where the rule that generated the event belongs.

**Client**

The client application, if available, which represents software running on the monitored host detected in the traffic that triggered the intrusion event.

**Connection Counter**

This field was added in release 6.4.0.4.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**Connection Instance ID**

This field was added in release 6.4.0.4.

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**DstIP**

The IP address used by the receiving host involved in the intrusion event.

**DstPort**

The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.

**EgressInterface**

The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.
**EgressZone**

The egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.

**First Packet Time (FirstPacketSecond)**

This field was added in release 6.4.0.4.

The time the system encountered the first packet.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**GID**

Generator ID; the ID of the component that generated the event.

**HTTPResponse**

The HTTP status code sent in response to a client's HTTP request over the connection that triggered the event.

**ICMPCode**

See **DstPort**.

**ICMPType**

See **SrcPort**.

**IngressInterface**

The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.

**IngressZone**

The ingress security zone or tunnel zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.

**InlineResult**

This field became available via syslog in version 6.3.

This field has:

- **Dropped** if the packet is dropped in an inline deployment
- **Would have dropped** if the packet would have been dropped if the intrusion policy had been set to drop packets in an inline deployment

In a passive deployment, the system does not drop packets, including when an inline interface is in tap mode, regardless of the rule state or the inline drop behavior of the intrusion policy.

**IntrusionPolicy**

This field became available via syslog in version 6.4.

The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled. You can choose an intrusion policy as the default action for an access control policy, or you can associate an intrusion policy with an access control rule.

**MPLS_Label**

This field is new in version 6.3.
The Multiprotocol Label Switching label associated with the packet that triggered the intrusion event.

**Message**

The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule. For decoder- and preprocessor-based events, the event message is hard coded.

The Generator and Snort IDs (GID and SID) and the SID version (Revision) are appended in parentheses to the end of each message in the format of numbers separated by colons (GID:SID:version). For example (1:36330:2).

**NAPPolicy**

The network analysis policy, if any, associated with the generation of the event.

This field displays the first fifty characters of the extracted URI. You can hover your pointer over the displayed portion of an abbreviated URI to display the complete URI, up to 2048 bytes. You can also display the complete URI, up to 2048 bytes, in the packet view.

**NumIOC**

Whether the traffic that triggered the intrusion event also triggered an indication of compromise (IOC) for a host involved in the connection.

**Priority**

The event priority as determined by the Cisco Talos Intelligence Group (Talos). The priority corresponds to either the value of the `priority` keyword or the value for the `classtype` keyword. For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.

**Protocol**

The name or number of the transport protocol used in the connection as listed in [http://www.iana.org/assignments/protocol-numbers](http://www.iana.org/assignments/protocol-numbers). This is the protocol associated with the source and destination port/ICMP column.

**Revision**

The version of the signature that was used to generate the event.

**Sensor UUID**

This field was added in release 6.4.0.4.

The unique identifier of the Firepower device that generated an event.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**SID**

The signature ID (also known as the Snort ID) of the rule that generated the event.

**SSLActualAction**

The action the system applied to encrypted traffic:

**SrcIP**

The IP address used by the sending host involved in the intrusion event.
SrcPort

The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.

User

The User ID for any known user logged in to the source host.

Starting in release 6.5: If applicable, the username is preceded by <realm>.

VLAN_ID

This field is new in version 6.3.

The innermost VLAN ID associated with the packet that triggered the intrusion event.

WebApplication

The web application, which represents the content or requested URL for HTTP traffic detected in the traffic that triggered the intrusion event.

If the system detects an application protocol of HTTP but cannot detect a specific web application, the system supplies a generic web browsing designation instead.

## Connection and Security Intelligence Event Field Descriptions

Starting in release 6.3, fields with empty or unknown values are not included in syslog messages.

### AccessControlRuleAction

The action associated with the configuration that logged the connection.

For Security Intelligence-monitored connections, the action is that of the first non-Monitor access control rule triggered by the connection, or the default action. Similarly, because traffic matching a Monitor rule is always handled by a subsequent rule or by the default action, the action associated with a connection logged due to a Monitor rule is never Monitor. However, you can still trigger correlation policy violations on connections that match Monitor rules.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Connections either allowed by access control explicitly, or allowed because a user bypassed an interactive block.</td>
</tr>
</tbody>
</table>
### Action Description

**Block, Block with reset**

Blocked connections, including:
- tunnels and other connections blocked by the prefilter policy
- connections blacklisted by Security Intelligence
- encrypted connections blocked by an SSL policy
- connections where an exploit was blocked by an intrusion policy
- connections where a file (including malware) was blocked by a file policy

For connections where the system blocks an intrusion or file, system displays Block, even though you use access control Allow rules to invoke deep inspection.

<table>
<thead>
<tr>
<th>Fastpath</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-encrypted tunnels and other connections fastpathed by the prefilter policy.</td>
<td></td>
</tr>
</tbody>
</table>

| Interactive Block, Interactive Block with reset | Connections logged when the system initially blocks a user’s HTTP request using an Interactive Block rule. If the user clicks through the warning page that the system displays, additional connections logged for the session have an action of Allow. |

| Trust | Connections trusted by access control. The system logs trusted TCP connections differently depending on the device model. |

| Default Action | Connections handled by the access control policy's default action. |

### AccessControlRuleName

The access control rule or default action that handled the connection, as well as up to eight Monitor rules matched by that connection.

If the connection matched one Monitor rule, the Firepower Management Center displays the name of the rule that handled the connection, followed by the Monitor rule name. If the connection matched more than one Monitor rule, the number of matching Monitor rules is displayed, for example, Default Action + 2 Monitor Rules.

### AccessControlRuleReason

The reason or reasons the connection was logged, if available.

Connections with a Reason of IP Block, DNS Block, and URL Block have a threshold of 15 seconds per unique initiator-responder pair. After the system blocks one of those connections, it does not generate connection events for additional blocked connections between those two hosts for the next 15 seconds, regardless of port or protocol.

### AC_POLICY

The access control policy that monitored the connection.

### ApplicationProtocol

The application protocol, which represents communications between hosts, detected in the connection.

### Client

The client application detected in the connection.
If the system cannot identify the specific client used in the connection, the field displays the word "client" appended to the application protocol name to provide a generic name, for example, FTP client.

**ClientVersion**

The version of the client application detected in the connection, if available.

**Connection Counter**

This field was added in release 6.4.0.4.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**Connection Instance ID**

This field was added in release 6.4.0.4.

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**ConnectionDuration**

This field was introduced in version 6.3.

This field has a value only when logging occurs at the end of the connection. For a start-of-connection syslog message, this field is not output, as it is not known at that time.

For an end-of-connection syslog message, this field indicates the number of seconds between the first packet and the last packet, which may be zero for a short connection. For example, if the timestamp of the syslog is 12:34:56 and the ConnectionDuration is 5, then the first packet was seen at 12:34:51.

**DestinationSecurityGroup**

This field was introduced in release 6.5.

The Security Group of the destination involved in the connection.

This field and **DestinationSecurityGroupTag** are a name-value pair. This field may be unknown while the corresponding **DestinationSecurityGroupTag** field has a value.

See also the field definitions for **SourceSecurityGroup** and **SourceSecurityGroupTag**.

**DestinationSecurityGroupTag**

This field was introduced in release 6.5.

The Security Group Tag (SGT) attribute of the destination involved in the connection. The SGT specifies the privileges of a traffic destination within a trusted network.

**DestinationSecurityGroup** and this field are a name-value pair. This field may have a value even if the corresponding DestinationSecurityGroup field value is unknown.

See also **SourceSecurityGroupTag**.

**DNS_Sinkhole**

The name of the sinkhole server where the system redirected a connection.
DNS_TTL
The number of seconds a DNS server caches the DNS resource record.

DNSQuery
The DNS query submitted in a connection to the name server to look up a domain name.

DNSRecordType
The type of the DNS resource record used to resolve a DNS query submitted in a connection.

DNSResponseType
The DNS response returned in a connection to the name server when queried.

DNSSICategory
See URLSICategory.

DstIP
The IP address (and host name, if DNS resolution is enabled) of the session responder (destination IP address).

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, source and destination IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

DstPort
The port used by the session responder.

EgressInterface
The egress interface associated with the connection. If your deployment includes an asymmetric routing configuration, the ingress and egress interface may not belong to the same inline pair.

EgressZone
The egress security zone associated with the connection.
For rezoned encapsulated connections, the egress field is blank.

Endpoint Profile
The user's endpoint device type, as identified by ISE.

Event Priority
This field was added in release 6.5.
Whether or not the connection event is a high priority event. High priority events are connection events that are associated with an intrusion, Security Intelligence, file, or malware event. All other events are Low priority.

FileCount
The number of files (including malware files) detected or blocked in a connection associated with one or more file events.

First Packet Time
This field was added in release 6.4.0.4.
The time the system encountered the first packet.
The following fields collectively uniquely identify a connection event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

HTTPReferer
The HTTP referrer, which represents the referrer of a requested URL for HTTP traffic detected in the connection (such as a website that provided a link to, or imported a link from, another URL).

HTTPResponse
The HTTP status code sent in response to a client's HTTP request over a connection.

ICMPCode
The ICMP code used by the session responder.

ICMPType
The ICMP type used by the session initiator.

IngressInterface
The ingress interface associated with the connection. If your deployment includes an asymmetric routing configuration, the ingress and egress interface may not belong to the same inline pair.

IngressZone
The ingress security zone associated with the connection.
For rezoned encapsulated connections, the ingress field displays the tunnel zone you assigned, instead of the original ingress security zone.

InitiatorBytes
The total number of bytes transmitted by the session initiator.

InitiatorPackets
The total number of packets transmitted by the session initiator.

IPReputationSICategory
See URLSICategory.

IPSCount
The number of intrusion events, if any, associated with the connection.

NAPPolicy
The network analysis policy (NAP), if any, associated with the generation of the event.

NetBIOSDomain
The NetBIOS domain used in the session.

originalClientSrcIP
The original client IP address from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To populate this field, you must enable an access control rule that handles proxied traffic based on its original client.

Prefilter Policy
The prefilter policy that handled the connection.
Protocol
The transport protocol used in the connection. To search for a specific protocol, use the name or number protocol as listed in http://www.iana.org/assignments/protocol-numbers.

ReferencedHost
If the protocol in the connection is HTTP or HTTPS, this field displays the host name that the respective protocol was using.

ResponderBytes
The total number of bytes received by the session responder.

ResponderPackets
The total number of packets received by the session responder.

SeeIntMatchingIP
Which IP address matched.
Possible values: None, Destination, or Source.

Security Group
In release 6.5, this field was replaced by the SourceSecurityGroupTag field, and new fields for SourceSecurityGroup, DestinationSecurityGroupTag, and DestinationSecurityGroup were introduced.

The Security Group Tag (SGT) attribute of the packet involved in the connection. The SGT specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) applies the attribute as packets enter the network.

Sensor UUID
This field was added in release 6.4.0.4.
The unique identifier of the Firepower device that generated an event.
The following fields collectively uniquely identify a connection event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

SourceSecurityGroup
This field was added in release 6.5.
The Security Group of the source involved in the connection.
This field and SourceSecurityGroupTag are a name-value pair. This field may be unknown while the corresponding SourceSecurityGroupTag field has a value: Tags can be obtained from inline devices (no source SGT name specified) or from ISE (which specifies a source).
See also DestinationSecurityGroup and DestinationSecurityGroupTag.

SourceSecurityGroupTag
In release 6.5, this field replaced the Security Group field.
The Security Group Tag (SGT) attribute of the packet involved in the connection. The SGT specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) applies the attribute as packets enter the network.
See also DestinationSecurityGroupTag.
SrcIP

The IP address (and host name, if DNS resolution is enabled) of the session initiator (source IP address).

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, source and destination IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

SrcPort

The port used by the session initiator.

SSLActualAction

The action the system applied to encrypted traffic in the SSL policy.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block/Block with reset</td>
<td>Represents blocked encrypted connections.</td>
</tr>
<tr>
<td>Decrypt (Resign)</td>
<td>Represents an outgoing connection decrypted using a re-signed server certificate.</td>
</tr>
<tr>
<td>Decrypt (Replace Key)</td>
<td>Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.</td>
</tr>
<tr>
<td>Decrypt (Known Key)</td>
<td>Represents an incoming connection decrypted using a known private key.</td>
</tr>
<tr>
<td>Default Action</td>
<td>Indicates the connection was handled by the default action.</td>
</tr>
<tr>
<td>Do not Decrypt</td>
<td>Represents a connection the system did not decrypt.</td>
</tr>
</tbody>
</table>

SSLCertificate

The information stored on the public key certificate used to encrypt traffic, including:

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number
- Certificate Fingerprint
- Public Key Fingerprint

SSLExpectedAction

The action the system expected to apply to encrypted traffic, given the SSL rules in effect.
SSLFlowStatus

The reason the system failed to decrypt encrypted traffic:

• Unknown
• No Match
• Success
• Uncached Session
• Unknown Cipher Suite
• Unsupported Cipher Suite
• Unsupported SSL Version
• SSL Compression Used
• Session Undecryptable in Passive Mode
• Handshake Error
• Decryption Error
• Pending Server Name Category Lookup
• Pending Common Name Category Lookup
• Internal Error
• Network Parameters Unavailable
• Invalid Server Certificate Handle
• Server Certificate Fingerprint Unavailable
• Cannot Cache Subject DN
• Cannot Cache Issuer DN
• Unknown SSL Version
• External Certificate List Unavailable
• External Certificate Fingerprint Unavailable
• Internal Certificate List Invalid
• Internal Certificate List Unavailable
• Internal Certificate Unavailable
• Internal Certificate Fingerprint Unavailable
• Server Certificate Validation Unavailable
• Server Certificate Validation Failure
• Invalid Action
SSLPolicy
The SSL policy that handled the connection.

SSLRuleName
The SSL rule or default action that handled the connection, as well as the first Monitor rule matched by that connection. If the connection matched a Monitor rule, the field displays the name of the rule that handled the connection, followed by the Monitor rule name.

SSLServerCertStatus
This applies only if you configured a Certificate Status SSL rule condition. If encrypted traffic matches an SSL rule, this field displays one or more of the following server certificate status values:

- Self Signed
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- Revoked

If undecryptable traffic matches an SSL rule, this field displays Not Checked.

SSLServerName
Hostname of the server with which the client established an encrypted connection.

SSLSessionID
The hexadecimal Session ID negotiated between the client and server during the TLS/SSL handshake.

SSLTicketID
A hexadecimal hash value of the session ticket information sent during the TLS/SSL handshake.

SSLURLCategory
URL categories for the URL visited in the encrypted connection.

If the system identifies or blocks a TLS/SSL application, the requested URL is in encrypted traffic, so the system identifies the traffic based on an SSL certificate. For TLS/SSL applications, therefore, this field indicates the common name contained in the certificate.

SSLVersion
The TLS/SSL protocol version used to encrypt the connection:

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
Connection and Security Intelligence Event Field Descriptions

- TLSv1.1
- TLSv1.2

**SSSLCipherSuite**

A macro value representing a cipher suite used to encrypt the connection. See www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for cipher suite value designations.

**TCPFlags**

For connections generated from NetFlow data, the TCP flags detected in the connection.

**Tunnel or Prefilter Rule**

The tunnel rule, prefilter rule, or prefilter policy default action that handled the connection.

**URL**

The URL requested by the monitored host during the session.

**URLCategory**

The category, if available, of the URL requested by the monitored host during the session.

**URLReputation**

The reputation, if available, of the URL requested by the monitored host during the session.

**URLSICategory, DNSSICategory, IPReputationSICategory**

The name of the blacklisted object that represents or contains the blacklisted URL, domain, or IP address in the connection. The Security Intelligence category can be the name of a network object or group, a blacklist, a custom Security Intelligence list or feed, a TID category related to an observation, or one of the categories in the Intelligence Feed.

**User**

The user logged into the session initiator. If this field is populated with No Authentication, the user traffic:

- matched an access control policy without an associated identity policy
- did not match any rules in the identity policy

Starting in release 6.5: If applicable, the username is preceded by <realm>.

**UserAgent**

The user-agent string application information extracted from HTTP traffic detected in the connection.

**VLAN_ID**

This field became available in syslog in version 6.3.

The innermost VLAN ID associated with the packet that triggered the connection.

**WebApplication**

The web application, which represents the content or requested URL for HTTP traffic detected in the connection.
If the web application does not match the URL for the event, the traffic is probably referred traffic, such as advertisement traffic. If the system detects referred traffic, it stores the referring application (if available) and lists that application as the web application.

If the system cannot identify the specific web application in HTTP traffic, this field displays Web Browsing.

File and Malware Event Field Descriptions

Syslog messages for file and malware events became available in release 6.4.

Note

- Fields with empty or unknown values are not included in security event syslog messages. However, verdicts with "Unknown" or similar values are included in file and malware event messages.
- Status field values for file and malware events reflect only the initial status; these fields do not update.

ApplicationProtocol
The application protocol used by the traffic in which a managed device detected the file.

ArchiveDepth
The level (if any) at which the file was nested in an archive file.

ArchiveFileName
The name of the archive file (if any) which contained the malware file.

ArchiveFileStatus
The status of an archive being inspected. Can have the following values:
- Pending — Archive is being inspected
- Extracted — Successfully inspected without any problems
- Failed — Failed to inspect, insufficient system resources
- Depth Exceeded — Successful, but archive exceeded the nested inspection depth
- Encrypted — Partially successful, archive was or contains an archive that is encrypted
- NotInspectable — Partially successful, file is possibly malformed or corrupt

ArchiveSHA256
The SHA-256 hash value of the archive file (if any) which contains the malware file.

Client
The client application that runs on one host and relies on a server to send a file.
Connection Counter

This field was added in release 6.4.0.4.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID

This field was added in release 6.4.0.4.

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

DstIP

The IP address of the host that responded to the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is Upload, then this is the IP address of the file recipient.

If FileDirection is Download, then this is the IP address of the file sender.

See also SrcIP.

DstPort

The port used in the connection described under DstIP.

FileAction

The action associated with file policy rule that detected the file, and any associated file rule action options.

FileDirection

Whether the file was downloaded or uploaded during the connection. Possible values are:

- Download — the file was transferred from the DstIP to the SrcIP.
- Upload — the file was transferred from the SrcIP to the DstIP.

FileName

The name of the file.

FilePolicy

The file policy that detected the file.

FileSandboxStatus

Indicates whether the file was sent for dynamic analysis and if so, the status.
**FileSHA256**

The SHA-256 hash value of the file.

To have a SHA256 value, the file must have been handled by one of:

- a Detect Files file rule with **Store files** enabled
- a Block Files file rule with **Store files** enabled
- a Malware Cloud Lookup file rule
- a Block Malware file rule

**FileSize**

The size of the file, in bytes.

Note that if the system determines the file type of a file before the file is fully received, the file size may not be calculated.

**FileStorageStatus**

The storage status of the file associated with the event:

- **Stored**
  
  Returns all events where the associated file is currently stored.

- **Stored in connection**
  
  Returns all events where the system captured and stored the associated file, regardless of whether the associated file is currently stored.

- **Failed**
  
  Returns all events where the system failed to store the associated file.

Syslog fields contain only the initial status; they do not update to reflect changed status.

**FileType**

The type of file, for example, HTML or MSEXE.

**First Packet Time**

The time the system encountered the first packet.

The following fields collectively uniquely identify the connection event associated with a particular file or malware event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**FirstPacketSecond**

The time at which the file download or upload flow started.

The time the event occurred is captured in the message header timestamp.

**Protocol**

The protocol used for the connection, for example TCP or UDP.
**Sensor UUID**

This field was added in release 6.4.0.4.

The unique identifier of the Firepower device that generated an event. The following fields collectively uniquely identify the connection event associated with a particular file or malware event: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter.

**SHA_Disposition**

The file’s disposition:

- **Clean**
  - Indicates that the AMP cloud categorized the file as clean, or that a user added the file to the clean list. Clean files appear in the malware table only if they were changed to clean.

- **Custom Detection**
  - Indicates that a user added the file to the custom detection list.

- **Malware**
  - Indicates that the AMP cloud categorized the file as malware, local malware analysis identified malware, or the file’s threat score exceeded the malware threshold defined in the file policy.

- **Unavailable**
  - Indicates that the system could not query the AMP cloud. You may see a small percentage of events with this disposition; this is expected behavior.

- **Unknown**
  - Indicates that the system queried the AMP cloud, but the file has not been assigned a disposition; in other words, the AMP cloud has not categorized the file.

File dispositions appear only for files for which the system queried the AMP cloud. Syslog fields reflect only the initial disposition; they do not update to reflect retrospective verdicts.

**SperoDisposition**

Indicates whether the SPERO signature was used in file analysis. Possible values:

- Spero detection performed on file
- Spero detection not performed on file

**SrcIP**

The IP address of the host that initiated the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is **Upload**, this is the IP address of the file sender.

If FileDirection is **Download**, this is the IP address of the file recipient.

See also **DstIP**.
SrcPort
The port used in the connection described under SrcIP.

SSLActualAction
The action the system applied to encrypted traffic:

Block or Block with reset
Represents blocked encrypted connections.

Decrypt (Resign)
Represents an outgoing connection decrypted using a re-signed server certificate.

Decrypt (Replace Key)
Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.

Decrypt (Known Key)
Represents an incoming connection decrypted using a known private key.

Default Action
Indicates the connection was handled by the default action.

Do not Decrypt
Represents a connection the system did not decrypt.

SSLCertificate
The certificate fingerprint of the TLS/SSL server.

SSLFlowStatus
The reason the system failed to decrypt encrypted traffic:

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
• Pending Server Name Category Lookup
• Pending Common Name Category Lookup
• Internal Error
• Network Parameters Unavailable
• Invalid Server Certificate Handle
• Server Certificate Fingerprint Unavailable
• Cannot Cache Subject DN
• Cannot Cache Issuer DN
• Unknown SSL Version
• External Certificate List Unavailable
• External Certificate Fingerprint Unavailable
• Internal Certificate List Invalid
• Internal Certificate List Unavailable
• Internal Certificate Unavailable
• Internal Certificate Fingerprint Unavailable
• Server Certificate Validation Unavailable
• Server Certificate Validation Failure
• Invalid Action

**ThreatName**
The name of the detected malware.

**ThreatScore**
The threat score most recently associated with this file. This is a value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.

**URI**
The URI of the connection associated with the file transaction, for example, the URL from which a user downloaded the file.

**User**
The username associated with the internal host that downloaded the file.

Starting in release 6.5: If applicable, the username is preceded by `<realm>\`.

For file events and for malware events generated by AMP for Networks, this user is determined by network discovery. Because the user is associated with the destination host, users are not associated with malware events in which the internal host uploaded a malware file.
**WebApplication**

The application that represents the content or requested URL for HTTP traffic detected in the connection.

## History for Security Event Syslog Messages

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
</table>
| New connection event fields for SGT               | 6.5     | New Security Group Tag fields:  
  - SourceSecurityGroup  
  - SourceSecurityGroupTag  
  (Replaces the Security Group field.)  
  - DestinationSecurityGroup  
  - DestinationSecurityGroupTag |
| New connection event field: Event Priority        | 6.5     | The Event Priority field was introduced.                                                                                                                                                           |
| Unique identifier for connection event in syslogs | 6.4.0.4 | The following syslog fields collectively uniquely identify a connection event and also appear in syslogs for intrusion, file, and malware events: Sensor UUID, First Packet Time, Connection Instance ID, and Connection Counter. |
| Syslog support for File and Malware events        | 6.4     | File and malware event fields are now available via syslog.                                                                                                                                         |
| IntrusionPolicy field added to intrusion events field list | 6.4     | Intrusion event syslogs now specify the intrusion policy that triggered the event.                                                                                                                  |
| Improved support for connection and intrusion events | 6.3     | Connection events, security intelligence events, and intrusion events are now available as fully-qualified events and have new event-type IDs. These fields are now documented in this guide. |
Syslog Messages 101001 to 199021

This chapter contains the following sections:

- Messages 101001 to 109104, on page 23
- Messages 110002 to 113045, on page 47
- Messages 114001 to 199027, on page 63

Messages 101001 to 109104

This section includes messages from 101001 to 109104.

101001

**Error Message** %FTD-1-101001: (Primary) Failover cable OK.

**Explanation** The failover cable is present and functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

101002

**Error Message** %FTD-1-101002: (Primary) Bad failover cable.

**Explanation** The failover cable is present, but not functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Replace the failover cable.

101003, 101004

**Error Message** %FTD-1-101003: (Primary) Failover cable not connected (this unit).

**Error Message** %FTD-1-101004: (Primary) Failover cable not connected (other unit).

**Explanation** Failover mode is enabled, but the failover cable is not connected to one unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Connect the failover cable to both units of the failover pair.
101005

**Error Message** %FTD-1-101005: (Primary) Error reading failover cable status.

**Explanation** The failover cable is connected, but the primary unit is unable to determine its status.

**Recommended Action** Replace the cable.

103001

**Error Message** %FTD-1-103001: (Primary) No response from other firewall (reason code = code).

**Explanation** The primary unit is unable to communicate with the secondary unit over the failover cable. Primary can also be listed as Secondary for the secondary unit. The following table lists the reason codes and the descriptions to determine why the failover occurred.

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The local unit is not receiving the hello packet on the failover LAN interface when LAN failover occurs or on the serial failover cable when serial failover occurs, and declares that the peer is down.</td>
</tr>
<tr>
<td>2</td>
<td>An interface did not pass one of the four failover tests, which are as follows: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP, and 4) Broadcast Ping.</td>
</tr>
<tr>
<td>3</td>
<td>No proper ACK for 15+ seconds after a command was sent on the serial cable.</td>
</tr>
<tr>
<td>4</td>
<td>The failover LAN interface is down, and other data interfaces are not responding to additional interface testing. In addition, the local unit is declaring that the peer is down.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>The standby peer went down during the configuration synchronization process.</td>
</tr>
<tr>
<td>6</td>
<td>Replication is not complete; the failover unit is not synchronized.</td>
</tr>
</tbody>
</table>

**Recommended Action** Verify that the failover cable is connected correctly and both units have the same hardware, software, and configuration. If the problem persists, contact the Cisco TAC.

### 103002

**Error Message** `%FTD-1-103002: (Primary) Other firewall network interface interface_number OK.`

**Explanation** The primary unit has detected that the network interface on the secondary unit is okay. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

### 103003

**Error Message** `%FTD-1-103003: (Primary) Other firewall network interface interface_number failed.`

**Explanation** The primary unit has detected a bad network interface on the secondary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Check the network connections on the secondary unit and the network hub connection. If necessary, replace the failed network interface.

### 103004

**Error Message** `%FTD-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string`

**Explanation** The primary unit received a message from the secondary unit indicating that the primary unit has failed. Primary can also be listed as Secondary for the secondary unit. The reason can be one of the following:

- Missed poll packets on failover command interface exceeded threshold.
- LAN failover interface failed.
- Peer failed to enter Standby Ready state.
- Failed to complete configuration replication. This firewall's configuration may be out of sync.
- Failover message transmit failure and no ACK for busy condition received.

**Recommended Action** Verify the status of the primary unit.
**103005**

**Error Message** `%FTD-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure`

**Explanation** The secondary unit has reported an SSM card failure to the primary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify the status of the secondary unit.

**103006**

**Error Message** `%FTD-1-103006: (Primary|Secondary) Mate version `ver_num` is not compatible with ours `ver_num`

**Explanation** The Firepower Threat Defense device has detected a peer unit that is running a version that is different than the local unit and is not compatible with the HA Hitless Upgrade feature.

- `ver_num` — Version number.

**Recommended Action** Install the same or a compatible version image on both units.

**103007**

**Error Message** `%FTD-1-103007: (Primary|Secondary) Mate version `ver_num` is not identical with ours `ver_num`

**Explanation** The Firepower Threat Defense device has detected that the peer unit is running a version that is not identical, but supports Hitless Upgrade and is compatible with the local unit. The system performance may be degraded because the image version is not identical, and the Firepower Threat Defense device may develop a stability issue if the nonidentical image runs for an extended period.

- `ver_num` — Version number

**Recommended Action** Install the same image version on both units as soon as possible.

**103008**

**Error Message** `%FTD-1-103008: Mate hwdib index is not compatible`

**Explanation** The number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

**104001, 104002**

**Error Message** `%FTD-1-104001: (Primary) Switching to ACTIVE (cause: string )`

**Error Message** `%FTD-1-104002: (Primary) Switching to STANDBY (cause: string )`
**Explanation** You have forced the failover pair to switch roles, either by entering the `failover active` command on the standby unit, or the `no failover active` command on the active unit. Primary can also be listed as Secondary for the secondary unit. Possible values for the string variable are as follows:

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

**Recommended Action** If the message occurs because of manual intervention, no action is required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

### 104003

**Error Message** `%FTD-1-104003: (Primary) Switching to FAILED.`

**Explanation** The primary unit has failed.

**Recommended Action** Check the messages for the primary unit for an indication of the nature of the problem (see message 104001). Primary can also be listed as Secondary for the secondary unit.

### 104004

**Error Message** `%FTD-1-104004: (Primary) Switching to OK.`

**Explanation** A previously failed unit reports that it is operating again. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

### 105001

**Error Message** `%FTD-1-105001: (Primary) Disabling failover.`

**Explanation** In version 7.x and later, this message may indicate the following: failover has been automatically disabled because of a mode mismatch (single or multiple), a license mismatch (encryption or context), or a hardware difference (one unit has an IPS SSM installed, and its peer has a CSC SSM installed). Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

### 105002

**Error Message** `%FTD-1-105002: (Primary) Enabling failover.`

**Explanation** You have used the `failover` command with no arguments on the console, after having previously disabled failover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.
105003

**Error Message** %FTD-1-105003: (Primary) Monitoring on interface interface_name waiting

**Explanation** The Firepower Threat Defense device is testing the specified network interface with the other unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required. The Firepower Threat Defense device monitors its network interfaces frequently during normal operation.

105004

**Error Message** %FTD-1-105004: (Primary) Monitoring on interface interface_name normal

**Explanation** The test of the specified network interface was successful. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

105005

**Error Message** %FTD-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.

**Explanation** One unit of the failover pair can no longer communicate with the other unit of the pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify that the network connected to the specified interface is functioning correctly.

105006, 105007

**Error Message** %FTD-1-105006: (Primary) Link status Up on interface interface_name.

**Error Message** %FTD-1-105007: (Primary) Link status Down on interface interface_name.

**Explanation** The results of monitoring the link status of the specified interface have been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** If the link status is down, verify that the network connected to the specified interface is operating correctly.

105008

**Error Message** %FTD-1-105008: (Primary) Testing interface interface_name.

**Explanation** Testing of a specified network interface has occurred. This testing is performed only if the Firepower Threat Defense device fails to receive a message from the standby unit on that interface after the expected interval. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.
105009

**Error Message** `%FTD-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}`.

**Explanation** The result (either Passed or Failed) of a previous interface test has been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required if the result is Passed. If the result is Failed, you should check the network cable connection to both failover units, that the network itself is functioning correctly, and verify the status of the standby unit.

105010

**Error Message** `%FTD-3-105010: (Primary) Failover message block alloc failed`.

**Explanation** Block memory was depleted. This is a transient message and the Firepower Threat Defense device should recover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Use the show blocks command to monitor the current block memory.

105011

**Error Message** `%FTD-1-105011: (Primary) Failover cable communication failure`.

**Explanation** The failover cable is not permitting communication between the primary and secondary units. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Ensure that the cable is connected correctly.

105020

**Error Message** `%FTD-1-105020: (Primary) Incomplete/slow config replication`.

**Explanation** When a failover occurs, the active Firepower Threat Defense device detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** After the Firepower Threat Defense device detects the failover, the Firepower Threat Defense device automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Firepower Threat Defense device. If failovers occur continuously, check the failover configuration and make sure that both Firepower Threat Defense devices can communicate with each other.

105021

**Error Message** `%FTD-1-105021: (failover_unit ) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name`.

**Explanation** During configuration synchronization, a standby unit will reload itself if some other process locks the configuration for more than five minutes, which prevents the failover process from applying the new configuration. This can occur when an administrator pages through a running configuration on the standby unit while configuration synchronization is in process. See also the show running-config command in privileged EXEC mode and the pager lines num command in global configuration mode in the Command Reference Guides.
**Recommended Action** Avoid viewing or modifying the configuration on the standby unit when it first boots up and is in the process of establishing a failover connection with the active unit.

**105031**

**Error Message** `%FTD-1-105031: Failover LAN interface is up`  
**Explanation** The LAN failover interface link is up.  
**Recommended Action** None required.

**105032**

**Error Message** `%FTD-1-105032: LAN Failover interface is down`  
**Explanation** The LAN failover interface link is down.  
**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed or duplex setting is correct.

**105033**

**Error Message** `%FTD-1-105033: LAN FO cmd Iface down and up again`  
**Explanation** LAN interface of failover gone down.  
**Recommended Action** Verify the failover link, might be a communication problem.

**105034**

**Error Message** `%FTD-1-105034: Receive a LAN_FAILOVER_UP message from peer.`  
**Explanation** The peer has just booted and sent the initial contact message.  
**Recommended Action** None required.

**105035**

**Error Message** `%FTD-1-105035: Receive a LAN failover interface down msg from peer.`  
**Explanation** The peer LAN failover interface link is down. The unit switches to active mode if it is in standby mode.  
**Recommended Action** Check the connectivity of the peer LAN failover interface.

**105036**

**Error Message** `%FTD-1-105036: dropped a LAN Failover command message.`  
**Explanation** The Firepower Threat Defense device dropped an unacknowledged LAN failover command message, indicating a connectivity problem exists on the LAN failover interface.  
**Recommended Action** Check that the LAN interface cable is connected.
105037

**Error Message** `%FTD-1-105037`: The primary and standby units are switching back and forth as the active unit.

**Explanation** The primary and standby units are switching back and forth as the active unit, indicating a LAN failover connectivity problem or software bug exists.

**Recommended Action** Make sure that the LAN interface cable is connected.

105038

**Error Message** `%FTD-1-105038`: (Primary) Interface count mismatch

**Explanation** When a failover occurs, the active Firepower Threat Defense device detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Once the failover is detected by the Firepower Threat Defense device, the Firepower Threat Defense device automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Firepower Threat Defense device. If failovers occur continuously, check the failover configuration and make sure that both Firepower Threat Defense devices can communicate with each other.

105039

**Error Message** `%FTD-1-105039`: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.

**Explanation** Failover initially verifies that the number of interfaces configured on the primary and secondary Firepower Threat Defense devices are the same. This message indicates that the primary Firepower Threat Defense device is not able to verify the number of interfaces configured on the secondary Firepower Threat Defense device. This message indicates that the primary Firepower Threat Defense device is not able to communicate with the secondary Firepower Threat Defense device over the failover interface. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify the failover LAN, interface configuration, and status on the primary and secondary Firepower Threat Defense devices. Make sure that the secondary Firepower Threat Defense device is running the Firepower Threat Defense device application and that failover is enabled.

105040

**Error Message** `%FTD-1-105040`: (Primary) Mate failover version is not compatible.

**Explanation** The primary and secondary Firepower Threat Defense devices should run the same failover software version to act as a failover pair. This message indicates that the secondary Firepower Threat Defense device failover software version is not compatible with the primary Firepower Threat Defense device. Failover is disabled on the primary Firepower Threat Defense device. Primary can also be listed as Secondary for the secondary Firepower Threat Defense device.

**Recommended Action** Maintain consistent software versions between the primary and secondary Firepower Threat Defense devices to enable failover.
105041

**Error Message** %FTD-1-105041: cmd failed during sync

**Explanation** Replication of the nameif command failed, because the number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

105042

**Error Message** %FTD-1-105042: (Primary) Failover interface OK

**Explanation** The LAN failover interface link is up.

The interface used to send failover messages to the secondary Firepower Threat Defense device is functioning. Primary can also be listed as Secondary for the secondary Firepower Threat Defense device.

**Recommended Action** None required.

105043

**Error Message** %FTD-1-105043: (Primary) Failover interface failed

**Explanation** The LAN failover interface link is down.

**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed or duplex setting is correct.

105044

**Error Message** %FTD-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.

**Explanation** When the operational mode (single or multiple) does not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same operational mode, and then reenable failover.

105045

**Error Message** %FTD-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).

**Explanation** When the feature licenses do not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same feature license, and then reenable failover.
105046

**Error Message**  %FTD-1-105046: (Primary|Secondary) Mate has a different chassis

**Explanation** Two failover units have a different type of chassis. For example, one has a three-slot chassis; the other has a six-slot chassis.

**Recommended Action** Make sure that the two failover units are the same.

---

105047

**Error Message**  %FTD-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2

**Explanation** The two failover units have different types of cards in their respective slots.

**Recommended Action** Make sure that the card configurations for the failover units are the same.

---

105048

**Error Message**  %FTD-1-105048: (unit) Mate’s service module (application) is different from mine (application)

**Explanation** The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

- **unit**—Primary or secondary
- **application**—The name of the application, such as InterScan Security Card

**Recommended Action** Make sure that both units have identical service modules before trying to reenable failover.

---

105050

**Error Message**  %FTD-3-105050: ASAv ethernet interface mismatch

**Explanation** Number of Ethernet interfaces on standby unit is less than that on active unit.

**Recommended Action** Firepower Threat Defense device with same number of interfaces should be paired up with each other. Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

---

106001

**Error Message**  %FTD-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name

**Explanation** An attempt was made to connect to an inside address is denied by the security policy that is defined for the specified traffic type. The IP address displayed is the real IP address instead of the IP address that appears through NAT. Possible tcp_flags values correspond to the flags in the TCP header that were present when the connection was denied. For example, a TCP packet arrived for which no connection state
exists in the Firepower Threat Defense device, and it was dropped. The tcp_flags in this packet are FIN and ACK.

The tcp_flags are as follows:

- **ACK**—The acknowledgment number was received
- **FIN**—Data was sent
- **PSH**—The receiver passed data to the application
- **RST**—The connection was reset
- **SYN**—Sequence numbers were synchronized to start a connection
- **URG**—The urgent pointer was declared valid

**Recommended Action** None required.

106002

**Error Message**  
%FTD-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address

**Explanation** The specified connection failed because of an outbound deny command. The protocol variable can be ICMP, TCP, or UDP.

**Recommended Action** Use the show outbound command to check outbound lists.

106006

**Error Message**  
%FTD-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.

**Explanation** An inbound UDP packet was denied by the security policy that is defined for the specified traffic type.

**Recommended Action** None required.

106007

**Error Message**  
%FTD-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.

**Explanation** A UDP packet containing a DNS query or response was denied.

**Recommended Action** If the inside port number is 53, the inside host probably is set up as a caching name server. Add an access-list command statement to permit traffic on UDP port 53 and a translation entry for the inside host. If the outside port number is 53, a DNS server was probably too slow to respond, and the query was answered by another server.

106010

**Error Message**  
%FTD-3-106010: Deny inbound protocol src [interface_name : source_address/source_port ] [{idfw_user | FQDN_string }, sg_info ] dst [interface_name : dest_address /dest_port ] [{idfw_user | FQDN_string }, sg_info ]

**Explanation** An inbound connection was denied by your security policy.
**Recommended Action** Modify the security policy if traffic should be permitted. If the message occurs at regular intervals, contact the remote peer administrator.

### 106011

**Error Message** %FTD-3-106011: Deny inbound (No xlate) string

**Explanation** The message appears under normal traffic conditions if there are internal users that are accessing the Internet through a web browser. Any time a connection is reset, when the host at the end of the connection sends a packet after the Firepower Threat Defense device receives the connection reset, this message appears. It can typically be ignored.

**Recommended Action** Prevent this message from getting logged to the syslog server by entering the `no logging message 106011` command.

### 106012

**Error Message** %FTD-6-106012: Deny IP from IP_address to IP_address, IP options hex.

**Explanation** An IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

**Recommended Action** Contact the remote host system administrator to determine the problem. Check the local site for loose source routing or strict source routing.

### 106013

**Error Message** %FTD-2-106013: Dropping echo request from IP_address to PAT address IP_address

**Explanation** The Firepower Threat Defense device discarded an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. The inbound packet is discarded because it cannot specify which PAT host should receive the packet.

**Recommended Action** None required.

### 106014

**Error Message** %FTD-3-106014: Deny inbound icmp src interface_name : IP_address [[(idfw_user | FQDN_string ), sg_info ] ] dst interface_name : IP_address [[(idfw_user | FQDN_string ), sg_info ] ] (type dec , code dec )

**Explanation** The Firepower Threat Defense device denied any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically allowed.

**Recommended Action** None required.

### 106015

**Error Message** %FTD-6-106015: Deny TCP (no connection) from IP_address /port to IP_address /port flags tcp_flags on interface interface_name.

**Explanation** The Firepower Threat Defense device discarded a TCP packet that has no associated connection in the Firepower Threat Defense connection table. The Firepower Threat Defense device looks for a SYN
flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the Firepower Threat Defense device discards the packet.

**Recommended Action** None required unless the Firepower Threat Defense device receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.

### 106016

**Error Message** %FTD-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.

**Explanation** A packet arrived at the Firepower Threat Defense interface that has a destination IP address of 0.0.0.0 and a destination MAC address of the Firepower Threat Defense interface. In addition, this message is generated when the Firepower Threat Defense device discarded a packet with an invalid source address, which may include one of the following or some other invalid address:

- Loopback network (127.0.0.0)
- Broadcast (limited, net-directed, subnet-directed, and all-subnets-directed)
- The destination host (land.c)

To further enhance spoof packet detection, use the `icmp` command to configure the Firepower Threat Defense device to discard packets with source addresses belonging to the internal network, because the `access-list` command has been deprecated and is no longer guaranteed to work correctly.

**Recommended Action** Determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

### 106017

**Error Message** %FTD-2-106017: Deny IP due to Land Attack from IP_address to IP_address

**Explanation** The Firepower Threat Defense device received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet that is designed to attack systems. This attack is referred to as a Land Attack.

**Recommended Action** If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

### 106018

**Error Message** %FTD-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address

**Explanation** The outgoing ICMP packet with the specified ICMP from local host (inside_address) to the foreign host (outside_address) was denied by the outbound ACL list.

**Recommended Action** None required.

### 106020

**Error Message** %FTD-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
**Explanation** The Firepower Threat Defense device discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the Firepower Threat Defense device or an Intrusion Detection System.

**Recommended Action** Contact the remote peer administrator or escalate this issue according to your security policy.

**106021**

**Error Message** %FTD-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name

**Explanation** An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. Unicast RPF, also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes that it is part of an attack on your Firepower Threat Defense device.

This message appears when you have enabled Unicast RPF with the ip verify reverse-path command. This feature works on packets input to an interface; if it is configured on the outside, then the Firepower Threat Defense device checks packets arriving from the outside.

The Firepower Threat Defense device looks up a route based on the source_address. If an entry is not found and a route is not defined, then this message appears and the connection is dropped.

If there is a route, the Firepower Threat Defense device checks which interface it corresponds to. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The Firepower Threat Defense device does not support asymmetric routing.

If the Firepower Threat Defense device is configured on an internal interface, it checks static route command statements or RIP, and if the source_address is not found, then an internal user is spoofing their address.

**Recommended Action** Even though an attack is in progress, if this feature is enabled, no user action is required. The Firepower Threat Defense device repels the attack.

**106022**

**Error Message** %FTD-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name

**Explanation** A packet matching a connection arrived on a different interface from the interface on which the connection began. In addition, the ip verify reverse-path command is not configured.

For example, if a user starts a connection on the inside interface, but the Firepower Threat Defense device detects the same connection arriving on a perimeter interface, the Firepower Threat Defense device has more than one path to a destination. This is known as asymmetric routing and is not supported on the Firepower Threat Defense device.

An attacker also might be attempting to append packets from one connection to another as a way to break into the Firepower Threat Defense device. In either case, the Firepower Threat Defense device shows this message and drops the connection.

**Recommended Action** Check that the routing is not asymmetric.
106023

**Error Message** %FTD-4-106023: Deny protocol src [interface_name :source_address /source_port ] [(idfw_user |FQDN_string |, sg_info )] dst interface_name :dest_address /dest_port [(idfw_user |FQDN_string |, sg_info )] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]

**Explanation** A real IP packet was denied by the ACL. This message appears even if you do not have the log option enabled for an ACL. The IP address is the real IP address instead of the values that display through NAT. Both user identity information and FQDN information is provided for the IP addresses if a matched one is found. The Firepower Threat Defense device logs either identity information (domain\user) or FQDN (if the username is not available). If the identity information or FQDN is available, the Firepower Threat Defense device logs this information for both the source and destination.

**Recommended Action** If messages persist from the same source address, a footprinting or port scanning attempt might be occurring. Contact the remote host administrator.

106024

**Error Message** %FTD-2-106024: Access rules memory exhausted

**Explanation** The access list compilation process has run out of memory. All configuration information that has been added since the last successful access list was removed from the Firepower Threat Defense device, and the most recently compiled set of access lists will continue to be used.

**Recommended Action** Access lists, AAA, ICMP, SSH, Telnet, and other rule types are stored and compiled as access list rule types. Remove some of these rule types so that others can be added.

106025, 106026

**Error Message** %FTD-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol

**Error Message** %FTD-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol

**Explanation** The security context of the packet in multiple context mode cannot be determined. Both messages can be generated for IP packets being dropped in either router and transparent mode.

**Recommended Action** None required.

106027

**Error Message** %FTD-4-106027:acl_ID: Deny src [source address] dst [destination address] by access-group “access-list name”

**Explanation** An non IP packet was denied by the ACL. This message is displayed even if you do not have the log option enabled for an extended ACL.

**Recommended Action** If messages persist from the same source address, it might indicate a foot-printing or port-scanning attempt. Contact the remote host administrator.
 ErrorMessage
%FTD-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name /source_address (source_port) (idfw_user, sg_info) interface_name /dest_address (dest_port) (idfw_user, sg_info) hit-cnt number {first hit | number -second interval} hash codes

Explanation
The initial occurrence or the total number of occurrences during an interval are listed. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level.

When an access-list line has the log argument, it is expected that this message ID might be triggered because of a nonsynchronized packet reaching the Firepower Threat Defense device and being evaluated by the access list. For example, if an ACK packet is received on the Firepower Threat Defense device (for which no TCP connection exists in the connection table), the Firepower Threat Defense device might generate message 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.

The following list describes the message values:

- permitted | denied | est-allowed—These values specify if the packet was permitted or denied by the ACL. If the value is est-allowed, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to access the Internet, and responding packets that would normally be denied by the ACL are accepted).
- protocol — TCP, UDP, ICMP, or an IP protocol number.
- interface_name — The interface name for the source or destination of the logged flow. The VLAN interfaces are supported.
- source_address — The source IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- dest_address — The destination IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- source_port — The source port of the logged flow (TCP or UDP). For ICMP, the number after the source port is the message type.
- idfw_user— The user identity username, including the domain name that is added to the existing syslog when the Firepower Threat Defense device can find the username for the IP address.
- sg_info— The security group tag that is added to the syslog when the Firepower Threat Defense device can find a security group tag for the IP address. The security group name is displayed with the security group tag, if available.
- dest_port — The destination port of the logged flow (TCP or UDP). For ICMP, the number after the destination port is the ICMP message code, which is available for some message types. For type 8, it is always 0. For a list of ICMP message types, see the following URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt number — The number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value is 1 when the Firepower Threat Defense device generates the first message for this flow.
- first hit—The first message generated for this flow.
- number -second interval—The interval in which the hit count is accumulated. Set this interval using the access-list command with the interval option.
- hash codes—Two are always printed for the object group ACE and the constituent regular ACE. Values are determined on which ACE that the packet hit. To display these hash codes, enter the show-access list command.
**Recommended Action** None required.

### 106101

**Error Message** %FTD-1-106101 Number of cached deny-flows for ACL log has reached limit (number).

**Explanation** If you configured the log option for an ACL deny statement (access-list id deny command), and a traffic flow matches the ACL statement, the Firepower Threat Defense device caches the flow information. This message indicates that the number of matching flows that are cached on the Firepower Threat Defense device exceeds the user-configured limit (using the access-list deny-flow-max command). This message might be generated as a result of a DoS attack.

- **number** – The limit configured using the access-list deny-flow-max command

**Recommended Action** None required.

### 106102

**Error Message** %FTD-6-106102: access-list acl_ID {permitted|denied} protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number {first hit|number -second interval} hash codes

**Explanation** A packet was either permitted or denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message 106100.

**Recommended Action** None required.

### 106103

**Error Message** %FTD-4-106103: access-list acl_ID denied protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number first hit hash codes

**Explanation** A packet was denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message 106023.

**Recommended Action** None required.

### 107001

**Error Message** %FTD-1-107001: RIP auth failed from IP_address : version-number, type-string, mode-string, sequence-number on interface interface_name

**Explanation** The Firepower Threat Defense device received a RIP reply message with bad authentication. This message might be caused by a misconfiguration on the router or the Firepower Threat Defense device or by an unsuccessful attempt to attack the routing table of the Firepower Threat Defense device.

**Recommended Action** This message indicates a possible attack and should be monitored. If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An attacker might be trying to determine the existing keys.
109011

**Error Message** %FTD-2-109011: Authen Session Start: user 'user ', sid number

**Explanation** An authentication session started between the host and the Firepower Threat Defense device and has not yet completed.

**Recommended Action** None required.

109012

**Error Message** %FTD-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds

**Explanation** The authentication cache has timed out. Users must reauthenticate on their next connection. You can change the duration of this timer with the timeout uauth command.

**Recommended Action** None required.

109013

**Error Message** %FTD-3-109013: User must authenticate before using this service

**Explanation** The user must be authenticated before using the service.

**Recommended Action** Authenticate using FTP, Telnet, or HTTP before using the service.

109016

**Error Message** %FTD-3-109016: Can't find authorization ACL acl_ID for user 'user '

**Explanation** The specified on the AAA server for this user does not exist on the Firepower Threat Defense device. This error can occur if you configure the AAA server before you configure the Firepower Threat Defense device. The Vendor-Specific Attribute (VSA) on your AAA server might be one of the following values:

- acl=acl_ID
- shell:acl=acl_ID
- ACS:CiscoSecured-Defined-ACL=acl_ID

**Recommended Action** Add the ACL to the Firepower Threat Defense device, making sure to use the same name specified on the AAA server.

109018

**Error Message** %FTD-3-109018: Downloaded ACL acl_ID is empty

**Explanation** The downloaded authorization has no ACEs. This situation might be caused by misspelling the attribute string ip:inacl# or omitting the access-list command.

`junk:junk# 1=permit tcp any any eq junk ip:inacl#1="`

**Recommended Action** Correct the ACL components that have the indicated error on the AAA server.
109019

**Error Message**  %FTD-3-109019: Downloaded ACL acl_ID has parsing error; ACE string

**Explanation** An error occurred during parsing the sequence number NNN in the attribute string ip:inacl#NNN= of a downloaded authorization. The reasons include: - missing = - contains nonnumeric, nonpace characters between # and = - NNN is greater than 999999999.

```plaintext
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 100000000=permit tcp any any
```

**Recommended Action** Correct the ACL element that has the indicated error on the AAA server.

109020

**Error Message**  %FTD-3-109020: Downloaded ACL has config error; ACE

**Explanation** One of the components of the downloaded authorization has a configuration error. The entire text of the element is included in the message. This message is usually caused by an invalid access-list command statement.

**Recommended Action** Correct the ACL component that has the indicated error on the AAA server.

109026

**Error Message**  %FTD-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be generated during transactions with RADIUS or TACACS+ servers.

Verify that the server key, configured using the `aaa-server` command, is correct.

109027

**Error Message**  %FTD-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be displayed during transactions with RADIUS or TACACS+ servers. The server_IP_address is the IP address of the relevant AAA server. The user is the user name associated with the connection.

**Recommended Action** Verify that the server key, configured using the `aaa-server` command, is correct.

109029

**Error Message**  %FTD-5-109029: Parsing downloaded ACL: string

**Explanation** A syntax error occurred while parsing an access list that was downloaded from a RADIUS server during user authentication.

• `string` — An error message detailing the syntax error that prevented the access list from parsing correctly
**Recommended Action** Use the information presented in this message to identify and correct the syntax error in the access list definition within the RADIUS server configuration.

**109030**

**Error Message** %FTD-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.

**Explanation** A dynamic ACL that is configured on a RADIUS server is not converted by the mechanism for automatically detecting wildcard netmasks. The problem occurs because this mechanism cannot determine if the netmask is a wildcard or a normal netmask.

- **access_list**—The access list that cannot be converted
- **source**—The source IP address
- **dest**—The destination IP address
- **netmask**—The subnet mask for the destination or source address in dotted-decimal notation

**Recommended Action** Check the access list netmask on the RADIUS server for the wildcard configuration. If the netmask is supposed to be a wildcard, and if all access list netmasks on that server are wildcards, then use the wildcard setting for `acl-netmask-convert` for the AAA server. Otherwise, change the netmask to a normal netmask or to a wildcard netmask that does not contain holes (that is, where the netmask presents consecutive binary 1s. For example, 00000000.00000000.00011111.11111111 or hex 0.0.31.255). If the mask is supposed to be normal and all access list netmasks on that server are normal, then use the normal setting for `acl-netmask-convert` for the AAA server.

**109032**

**Error Message** %FTD-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.

**Explanation** The Firepower Threat Defense device received an access control list from a RADIUS server to apply to a user connection, but an entry in the list contains a syntax error. The use of a list containing an error could result in the violation of a security policy, so the Firepower Threat Defense device failed to authenticate the user.

- **access_list**—The name assigned to the dynamic access list as it would appear in the output of the `show access-list` command
- **username**—The name of the user whose connection will be subject to this access list
- **ace**—The access list entry that was being processed when the error was detected

**Recommended Action** Correct the access list definition in the RADIUS server configuration.

**109033**

**Error Message** %FTD-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol connections.

**Explanation** AAA challenge processing was triggered during authentication of an administrative connection, but the Firepower Threat Defense device cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- **user**—The name of the user being authenticated
- **src_IP**—The IP address of the client host
• **protocol** —The client connection protocol (SSH v1 or administrative HTTP)

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

---

**109034**

**Error Message** `%FTD-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port. Interactive challenge processing is not supported for protocol connections`

**Explanation** AAA challenge processing was triggered during authentication of a network connection, but the Firepower Threat Defense device cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

---

**109035**

**Error Message** `%FTD-3-109035: Exceeded maximum number (<max_num>) of DAP attribute instances for user <user>`

**Explanation** This log is generated when the number of DAP attributes received from the RADIUS server exceeds the maximum number allowed when authenticating a connection for the specified user.

**Recommended Action** Modify the DAP attribute configuration to reduce the number of DAP attributes below the maximum number allowed as specified in the log so that the specified user can connect.

---

**109036**

**Error Message** `%FTD-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username .`

**Explanation** The LDAP response message contains an attribute that has more than 1000 values.

**Recommended Action** None required.

---

**109037**

**Error Message** `%FTD-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username .`
Explaination  The Firepower Threat Defense device supports multiple values of the same attribute received from a AAA server. If the AAA server sends a response containing more than 5000 values for the same attribute, then the Firepower Threat Defense device treats this response message as being malformed and rejects the authentication. This condition has only been seen in lab environments using specialized test tools. It is unlikely that the condition would occur in a real-world production network.

- **attribute_name** — The LDAP attribute name
- **username** — The username at login

Recommended Action  Capture the authentication traffic between the Firepower Threat Defense device and AAA server using a protocol sniffer (such as WireShark), then forward the trace file to the Cisco TAC for analysis.

109038

**Error Message**  %FTD-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name

Explanation  The AAA subsystem tried to parse an attribute from the AAA server into an internal representation and failed.

- **string-from-server** — String received from the AAA server, truncated to 40 characters.
- **type** — The type of the specified attribute

Recommended Action  Verify that the attribute is being generated correctly on the AAA server. For additional information, use the `debug ldap` and `debug radius` commands.

109039

**Error Message**  %FTD-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc :laddr to fifc :faddr

Explanation  A packet containing IPv6 addresses or IPv4 addresses translated to IPv6 addresses by NAT requires AAA authentication or authorization. AAA authentication and authorization do not support IPv6 addresses. The packet is dropped.

- **lifc** — The ingress interface
- **laddr** — The source IP address
- **fifc** — The egress interface
- **faddr** — The destination IP address after NAT translation, if any

Recommended Action  None required.

109100

**Error Message**  %FTD-6-109100: Received CoA update from coa-source-ip for user username , with session ID: audit-session-id , changing authorization attributes

Explanation  The Firepower Threat Defense device has successfully processed the CoA policy update request from coa-source-ip for user username with session id audit-session-id. This syslog message is generated after a change of authorization policy update has been received by the Firepower Threat Defense device,
validated and applied. In a non-error case, this is the only syslog message that is generated when a change of authorization is received and processed.

- **coa-source-ip** — Originating IP address of the change of authorization request
- **username** — User whose session is being changed
- **audit-session-id** — The global ID of the session being modified

**Recommended Action** None required.

### 109101

**Error Message** %FTD-6-109101: Received CoA disconnect request from coa-source-ip for user username, with audit-session-id: audit-session-id

**Explanation** The Firepower Threat Defense device has received a correctly formatted Disconnect-Request for an active VPN session and has successfully terminated the connection.

- **coa-source-ip** — Originating IP address of the change of authorization request
- **username** — User whose session is being changed
- **audit-session-id** — The global ID of the session being modified

**Recommended Action** None required.

### 109102

**Error Message** %FTD-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id

**Explanation** The Firepower Threat Defense device has received a valid change of authorization request, but the session ID specified in the request does not match any active sessions on the Firepower Threat Defense device. This could be the result of the change of authorization server attempting to issue a change of authorization on a session that has already been closed by the user.

- **action-type** — The requested change of authorization action (update or disconnect)
- **coa-source-ip** — Originating IP address of the change of authorization request
- **audit-session-id** — The global ID of the session being modified

**Recommended Action** None required.

### 109103

**Error Message** %FTD-3-109103: CoA action-type from coa-source-ip failed for user username, with session ID: audit-session-id.

**Explanation** The Firepower Threat Defense device has received a correctly formatted change of authorization request, but was unable to process it successfully.

- **action-type** — The requested change of authorization action (update or disconnect)
- **coa-source-ip** — Originating IP address of the change of authorization request
- **username** — User whose session is being changed
- **audit-session-id** — The global ID of the session being modified

**Recommended Action** Investigate the relevant VPN subsystem logs to determine why the updated attributes could not be applied or why the session could not be terminated.
109104

**Error Message** %FTD-3-109104: CoA action-type from coa-source-ip failed for user username, session ID: audit-session-id. Action not supported.

**Explanation** The Firepower Threat Defense device has received a correctly formatted change of authorization request, but did not process it because the indicated action is not supported by the Firepower Threat Defense device.

- **action-type** — The requested change of authorization action (update or disconnect)
- **coa-source-ip** — Originating IP address of the change of authorization request
- **username** — User whose session is being changed
- **audit-session-id** — The global ID of the session being modified

**Recommended Action** None required.

109105

**Error Message** %FTD-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>.

**Explanation** It is necessary for Firepower Threat Defense device to log a syslog if no routes are present when the interface is BVI. Apparently, if default route is present and it does not route packet to the correct interface then it becomes impossible to track it. In case of Firepower Threat Defense, management routes are looked first following the data interface. So if default route is routing packets to different destination, then it is difficult to track it.

**Recommended Action** It is highly recommended to add default route for correct destination or add static routes.

Messages 110002 to 113045

This section includes messages from 110002 to 113045.

110002

**Error Message** %FTD-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port

**Explanation** An error occurred when the Firepower Threat Defense device tried to find the interface through which to send the packet.

- **protocol** — The protocol of the packet
- **src interface** — The interface from which the packet was received
- **src IP** — The source IP address of the packet
- **src port** — The source port number
- **dest IP** — The destination IP address of the packet
- **dest port** — The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.
110003

**Error Message** %FTD-6-110003: Routing failed to locate next-hop for protocol from src interface : src IP/src port to dest interface : dest IP/dest port

**Explanation** An error occurred when the Firepower Threat Defense device tried to find the next hop on an interface routing table.

- **protocol** — The protocol of the packet
- **src interface** — The interface from which the packet was received
- **src IP** — The source IP address of the packet
- **src port** — The source port number
- **dest IP** — The destination IP address of the packet
- **dest port** — The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC. During debugging, use the `show asp table routing` command to view the routing table details.

110004

**Error Message** %FTD-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone /parent_outside_ifc :outside_addr /outside_port (mapped_addr /mapped_port ) to inside_zone /parent_inside_ifc :inside_addr /inside_port (mapped_addr /mapped_port )

**Explanation** A flow changed on the egress interface.

**Recommended Action** None required.

111001

**Error Message** %FTD-5-111001: Begin configuration: IP_address writing to device

**Explanation** You have entered the `write` command to store your configuration on a device (either floppy, flash memory, TFTP, the failover standby unit, or the console terminal). The **IP_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.

111002

**Error Message** %FTD-5-111002: Begin configuration: IP_address reading from device

**Explanation** You have entered the `read` command to read your configuration from a device (either floppy disk, flash memory, TFTP, the failover standby unit, or the console terminal). The **IP_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.
111003

**Error Message** %FTD-5-111003: IP_address Erase configuration

**Explanation** You have erased the contents of flash memory by entering the `write erase` command at the console. The IP_address value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** After erasing the configuration, reconfigure the Firepower Threat Defense device and save the new configuration. Alternatively, you can restore information from a configuration that was previously saved, either on a floppy disk or on a TFTP server elsewhere on the network.

111004

**Error Message** %FTD-5-111004: IP_address end configuration: {FAILED|OK}

**Explanation** You have entered the `config floppy/memory/ network` command or the `write floppy/memory/network/standby` command. The IP_address value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required if the message ends with OK. If the message indicates a failure, try to fix the problem. For example, if writing to a floppy disk, ensure that the floppy disk is not write protected; if writing to a TFTP server, ensure that the server is up.

111005

**Error Message** %FTD-5-111005: IP_address end configuration: OK

**Explanation** You have exited the configuration mode. The IP_address value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

111007

**Error Message** %FTD-5-111007: Begin configuration: IP_address reading from device.

**Explanation** You have entered the `reload` or `configure` command to read in a configuration. The device text can be floppy, memory, net, standby, or terminal. The IP_address value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

111008

**Error Message** %FTD-5-111008: User user executed the command `string`

**Explanation** The user entered any command, with the exception of a `show` command.

**Recommended Action** None required.
111009

Error Message %FTD-7-111009: User user executed cmd: string

Explanation The user entered a command that does not modify the configuration. This message appears only for show commands.

Recommended Action None required.

111010

Error Message %FTD-5-111010: User username, running application-name from IP ip addr, executed cmd

Explanation A user made a configuration change.

- username — The user making the configuration change
- application-name — The application that the user is running
- ip addr — The IP address of the management station
- cmd — The command that the user has executed

Recommended Action None required.

111111

Error Message % FTD-1-111111 error_message

Explanation A system or infrastructure error has occurred.

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

112001

Error Message %FTD-2-112001: (string :dec ) Clear complete.

Explanation A request to clear the module configuration was completed. The source file and line number are identified.

Recommended Action None required.

113001

Error Message %FTD-3-113001: Unable to open AAA session. Session limit [limit ] reached.

Explanation The AAA operation on an IPsec tunnel or WebVPN connection cannot be performed because of the unavailability of AAA resources. The limit value indicates the maximum number of concurrent AAA transactions.

Recommended Action Reduce the demand for AAA resources, if possible.

113003

Error Message %FTD-6-113003: AAA group policy for user user is being set to policy_name.
Explanation The group policy that is associated with the tunnel group is being overridden with a user-specific policy, policy_name. The policy_name is specified using the username command when LOCAL authentication is configured or is returned in the RADIUS CLASS attribute when RADIUS authentication is configured.

Recommended Action None required.

113004

Error Message %FTD-6-113004: AAA user aaa_type Successful: server = server_IP_address , User = user

Explanation The AAA operation on an IPsec or WebVPN connection has been completed successfully. The AAA types are authentication, authorization, or accounting. The server_IP_address is the IP address of the relevant AAA server. The user is the username associated with the connection.

Recommended Action None required.

113005

Error Message %FTD-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr

Explanation The AAA authentication on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the no logging hide username command has been configured.

Recommended Action Retry the authentication.

113006

Error Message %FTD-6-113006: User user locked out on exceeding number successive failed authentication attempts

Explanation A locally configured user is being locked out. This happens when a configured number of consecutive authentication failures have occurred for this user and indicates that all future authentication attempts by this user will be rejected until an administrator unlocks the user using the clear aaa local user lockout command. The user is the user that is now locked, and the number is the consecutive failure threshold configured using the aaa local authentication attempts max-fail command.

Recommended Action Try unlocking the user using the clear aaa local user lockout command or adjusting the maximum number of consecutive authentication failures that are tolerated.
113007

Error Message  %FTD-6-113007: User user unlocked by administrator

Explanation A locally configured user that was locked out after exceeding the maximum number of consecutive authentication failures set by using the `aaa local authentication attempts max-fail` command has been unlocked by the indicated administrator.

Recommended Action None required.

113008

Error Message  %FTD-6-113008: AAA transaction status ACCEPT: user = user

Explanation The AAA transaction for a user associated with an IPsec or WebVPN connection was completed successfully. The user is the username associated with the connection.

Recommended Action None required.

113009

Error Message  %FTD-6-113009: AAA retrieved default group policy policy for user user

Explanation The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that were specified with the `tunnel-group` or `webvpn` commands have been retrieved.

Recommended Action None required.

113010

Error Message  %FTD-6-113010: AAA challenge received for user user from server server_IP_address

Explanation The authentication of an IPsec connection has occurred with a SecurID server. The user will be prompted to provide further information before being authenticated.

- `user`—The username associated with the connection
- `server_IP_address`—The IP address of the relevant AAA server

Recommended Action None required.

113011

Error Message  %FTD-6-113011: AAA retrieved user specific group policy policy for user user

Explanation The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that was specified with the `tunnel-group` or `webvpn` commands have been retrieved.

Recommended Action None required.
113012

**Error Message**  %FTD-6-113012: AAA user authentication Successful: local database: user = user

**Explanation** The user associated with an IPsec or WebVPN connection has been successfully authenticated to the local user database.

- user—The username associated with the connection

**Recommended Action** None required.

113013

**Error Message**  %FTD-6-113013: AAA unable to complete the request Error: reason = reason : user = user

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or has been rejected because of a policy violation.

- reason—The reason details
- user—The username associated with the connection

**Recommended Action** None required.

113014

**Error Message**  %FTD-6-113014: AAA authentication server not accessible: server = server_IP_address : user = user

**Explanation** The device was unable to communicate with the configured AAA server during the AAA transaction associated with an IPsec or WebVPN connection. This may or may not result in a failure of the user connection attempt depending on the backup servers configured in the **aaa-server** group and the availability of those servers. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Verify connectivity with the configured AAA servers.

113015

**Error Message**  %FTD-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user: user IP = xxx.xxx.xxx.xxx

**Explanation** A request for authentication to the local user database for a user associated with an IPsec or WebVPN connection has been rejected. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- reason—The details of why the request was rejected
- user—The username associated with the connection
- user_ip—The IP address of the user who initiated the authentication or authorization request<915CLI>

**Recommended Action** None required.
113016

**Error Message** %FTD-6-113016: AAA credentials rejected: reason = reason : server = server_IP_address : user = user<915CLI> : user IP = xxx.xxx.xxx.xxx

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected due to a policy violation. The username is hidden when invalid or unknown, but appears when valid or the `no logging hide username` command has been configured.

- **reason**—The details of why the request was rejected
- **server_IP_address**—The IP address of the relevant AAA server
- **user**—The username associated with the connection
- **<915CLI>user_ip**—The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

113017

**Error Message** %FTD-6-113017: AAA credentials rejected: reason = reason : local database: user = user : user IP = xxx.xxx.xxx.xxx

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected because of a policy violation. This event only appears when the AAA transaction is with the local user database rather than with an external AAA server.

- **reason**—The details of why the request was rejected
- **user**—The username associated with the connection
- **user_ip**—The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

113018

**Error Message** %FTD-3-113018: User: user , Unsupported downloaded ACL Entry: ACL_entry , Action: action

**Explanation** An ACL entry in unsupported format was downloaded from the authentication server. The following list describes the message values:

- **user**—User trying to log in
- **ACL_entry**—Unsupported ACL entry downloaded from the authentication server
- **action**—Action taken when encountering the unsupported ACL entry

**Recommended Action** The ACL entry on the authentication server has to be changed by the administrator to conform to the supported ACL entry formats.

113019

**Error Message** %FTD-4-113019: Group = group , Username = username , IP = peer_address , Session disconnected. Session Type: type , Duration: duration , Bytes xmt: count , Bytes rcv: count , Reason: reason

**Explanation** An indication of when and why the longest idle user is disconnected.
- **group**—Group name
- **username**—Username
- **IP**—Peer address
- **Session Type**—Session type (for example, IPsec or UDP)
- **duration**—Connection duration in hours, minutes, and seconds
- **Bytes xmt**—Number of bytes transmitted
- **Bytes rcv**—Number of bytes received
- **reason**—Reason for disconnection

User Requested
Lost Carrier
Lost Service
Idle Timeout
Max time exceeded
Administrator Reset
Administrator Reboot
Administrator Shutdown
Port Error
NAS Error
NAS Request
NAS Reboot
Port unneeded

Connection preempted. Indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.

Port Suspended
Service Unavailable
Callback
User error
Host Requested
SA Expired
IKE Delete
Bandwidth Management Error
Certificate Expired
Phase 2 Mismatch
Firewall Mismatch
Peer Address Changed
ACL Parse Error
Phase 2 Error
Configuration Error
Peer Reconnected
Internal Error
Crypto map policy not found
L2TP initiated
VLAN Mapping Error
NAC-Policy Error
Dynamic Access Policy terminate
Client type not supported
Unknown

**Recommended Action** Unless the reason indicates a problem, then no action is required.

**113020**

**Error Message** `%FTD-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds`

**Explanation** Authentication for an IPsec or WebVPN user through a Kerberos server has failed because the clocks on the Firepower Threat Defense device and the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

- **ip_address** —The IP address of the Kerberos server

**Recommended Action** Synchronize the clocks on the Firepower Threat Defense device and the Kerberos server.

**113021**

**Error Message** `%FTD-3-113021: Attempted console login failed. User username did NOT have appropriate Admin Rights.`

**Explanation** A user has tried to access the management console and was denied.

- **username** —The username entered by the user

**Recommended Action** If the user is a newly added admin rights user, check that the service type (LOCAL or RADIUS authentication server) for that user is set to allow access:

- **nas-prompt**—Allows login to the console and exec privileges at the required level, but not enable (configuration modification) access
- **admin**—Allows all access and can be further constrained by command privileges

Otherwise, the user is inappropriately trying to access the management console; the action to be taken should be consistent with company policy for these matters.
### 113022

**Error Message** %FTD-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED

**Explanation** The Firepower Threat Defense device has tried an authentication, authorization, or accounting request to the AAA server and did not receive a response within the configured timeout window. The AAA server will be marked as failed and has been removed from service.

- *protocol* — The type of authentication protocol, which can be one of the following:
  - RADIUS
  - TACACS+
  - NT
  - RSA SecurID
  - Kerberos
  - LDAP

- *ip-addr* — The IP address of the AAA server
- *tag* — The server group name

**Recommended Action** Verify that the AAA server is online and is accessible from the Firepower Threat Defense device.

### 113023

**Error Message** %FTD-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE

**Explanation** The Firepower Threat Defense device has reactivated the AAA server that was previously marked as failed. The AAA server is now available to service AAA requests.

- *protocol* — The type of authentication protocol, which can be one of the following:
  - RADIUS
  - TACACS+
  - NT
  - RSA SecurID
  - Kerberos
  - LDAP

- *ip-addr* — The IP address of the AAA server
- *tag* — The server group name

**Recommended Action** None required.

### 113024

**Error Message** %FTD-5-113024: Group tg : Authenticating type connection from ip with username, user_name , from client certificate
Explanation The prefill username feature overrides the username with one derived from the client certificate for use in AAA.

- *tg* — The tunnel group
- *type* — The type of connection (ssl-client or clientless)
- *ip* — The IP address of the connecting user
- *user_name* — The name extracted from the client certificate for use in AAA

Recommended Action None required.

113025

Error Message  %FTD-5-113025: Group tg : fields  Could not authenticate connection type connection from ip

Explanation A username cannot be successfully extracted from the certificate.

- *tg* — The tunnel group
- *fields* — The DN fields being searched for
- *connection type* — The type of connection (SSL client or clientless)
- *ip* — The IP address of the connecting user

Recommended Action The administrator should check that the authentication aaa certificate, ssl certificate-authentication, and authorization-dn-attributes keywords have been set correctly.

113026

Error Message  %FTD-4-113026: Error error while executing Lua script for group tunnel group

Explanation An error occurred while extracting a username from the client certificate for use in AAA. This message is only generated when the username-from-certificate use-script option is enabled.

- *error* — Error string returned from the Lua environment
- *tunnel group* — The tunnel group attempting to extract a username from a certificate

Recommended Action Examine the script being used by the username-from-certificate use-script option for errors.

113027

Error Message  %FTD-2-113027: Error activating tunnel-group scripts

Explanation The script file cannot be loaded successfully. No tunnel groups using the username-from-certificate use-script option work correctly.

Recommended Action The administrator should check the script file for errors using ASDM. Use the debug aaa command to obtain a more detailed error message that may be useful.

113028

Error Message  %FTD-7-113028: Extraction of username from VPN client certificate has string. [Request num ]
**Explanation** The processing request of a username from a certificate is running or has finished.

- `num` — The ID of the request (the value of the pointer to the fiber), which is a monotonically increasing number.
- `string` — The status message, which can one of the following:
  - been requested
  - started
  - finished with error
  - finished successfully
  - completed

**Recommended Action** None required.

---

**113029**

**Error Message** `%FTD-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached`

**Explanation** The user session cannot be established because the current number of sessions exceeds the maximum session load.

**Recommended Action** Increase the configured limit, if possible, to create a load-balanced cluster.

---

**113030**

**Error Message** `%FTD-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.`

**Explanation** The specified ACL was not found on the Firepower Threat Defense device.

- `group` — The name of the group
- `user` — The name of the user
- `ipaddr` — The IP address
- `acl` — The name of the ACL

**Recommended Action** Modify the configuration to add the specified ACL or to correct the ACL name.

---

**113031**

**Error Message** `%FTD-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.`

**Explanation** The type of ACL to be applied is incorrect. An IPv6 ACL has been configured as an IPv4 ACL through the `vpn-filter` command.

- `group` — The group policy name of the user
- `user` — The username
- `ipaddr` — The public (not assigned) IP address of the user
- `filter` — The name of the VPN filter
**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Firepower Threat Defense device, and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

---

**113032**

**Error Message** `%FTD-4-113032`: Group `group` User `user` IP `ipaddr` AnyConnect `ipv6-vpn-filter` filter is an IPv4 ACL; ACL not applied.

**Explanation** The type of ACL to be applied is incorrect. An IPv4 ACL has been configured as an IPv6 ACL through the `ipv6-vpn-filter` command.

- `group` — The group policy name of the user
- `user` — The username
- `ipaddr` — The public (not assigned) IP address of the user
- `filter` — The name of the VPN filter

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Firepower Threat Defense device and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

---

**113033**

**Error Message** `%FTD-6-113033`: Group `group` User `user` IP `ipaddr` AnyConnect session not allowed. ACL parse error.

**Explanation** The WebVPN session for the specified user in this group is not allowed because the associated ACL did not parse. The user will not be allowed to log in via WebVPN until this error has been corrected.

- `group` — The group policy name of the user
- `user` — The username
- `ipaddr` — The public (not assigned) IP address of the user

**Recommended Action** Correct the WebVPN ACL.

---

**113034**

**Error Message** `%FTD-4-113034`: Group `group` User `user` IP `ipaddr` User ACL `acl` from AAA ignored, AV-PAIR ACL used instead.

**Explanation** The specified ACL was not used because a Cisco AV-PAIR ACL was used.

- `group` — The name of the group
- `user` — The name of the user
- `ipaddr` — The IP address
- `acl` — The name of the ACL

**Recommended Action** Determine the correct ACL to use and correct the configuration.
113035

Error Message %FTD-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.

Explanation The user logged in via the AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The session connection has been terminated.

- group — The name of the group policy with which the user is trying to connect
- user — The name of the user who is trying to connect
- ipaddr — The IP address of the user who is trying to connect

Recommended Action Enable the SVC globally using the svc-enable command. Validate the integrity and versions of the SVC images by reloading new images using the svc image command.

113036

Error Message %FTD-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.

Explanation The given parameter has a bad value. The value is not shown because it might be very long.

- group — The name of the group
- user — The name of the user
- ipaddr — The IP address
- name — The name of the parameter

Recommended Action Modify the configuration to correct the indicated parameter.

113037

Error Message %FTD-6-113037: Reboot pending, new sessions disabled. Denied user login.

Explanation A user was unable to log in to WebVPN because the Firepower Threat Defense device is in the process of rebooting.

Recommended Action None required.

113038

Error Message %FTD-4-113038: Group group User user IP ipaddr Unable to create AnyConnect parent session.

Explanation The AnyConnect session was not created for the user in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

- group — The name of the group
- user — The name of the user
- ipaddr — The IP address

Recommended Action None required.
113039

Error Message  %FTD-6-113039: Group group User user IP ipaddr AnyConnect parent session started.

Explanation The AnyConnect session has started for the user in this group at the specified IP address. When the user logs in via the AnyConnect login page, the AnyConnect session starts.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address

Recommended Action None required.

113040

Error Message  %FTD-4-113040: Terminating the VPN connection attempt from attempted group .

Reason: This connection is group locked to locked group.

Explanation The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- **attempted group** —The tunnel group over which the connection came in
- **locked group** —The tunnel group for which the connection is locked or restricted

Recommended Action Check the group-lock value in the group policy or the user attributes.

113041

Error Message  %FTD-4-113041: Redirect ACL configured for assigned IP does not exist on the device.

Explanation An error occurred when the redirect URL was installed and the ACL was received from the ISE, but the redirect ACL does not exist on the Firepower Threat Defense device.

- **assigned IP** —The IP address that is assigned to the client

Recommended Action Configure the redirect ACL on the Firepower Threat Defense device.

113042

Error Message  %FTD-4-113042: CoA: Non-HTTP connection from src_if :src_ip /src_port to dest_if :dest_ip /dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.

Explanation For the CoA feature, the redirect ACL filter drops the matching non-HTTP traffic during the redirect processing and provides information about the terminated traffic flow.

- **src_if**, **src_ip**, **src_port** —The source interface, IP address, and port of the flow
- **dest_if**, **dest_ip**, **dest_port** —The destination interface, IP address, and port of the flow
- **username** —The name of the user
- **client_IP** —The IP address of the client
**Recommended Action** Validate the redirect ACL configuration on the Firepower Threat Defense device. Make sure that the correct filter is used to match the traffic to redirect and does not block the flow that is intended to be allowed through.

**Messages 114001 to 199027**

This section includes messages from 114001 to 199027.

**114001**

<table>
<thead>
<tr>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%FTD-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).</td>
</tr>
</tbody>
</table>

**Explanation** The system failed to initialize a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

**114002**

<table>
<thead>
<tr>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%FTD-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).</td>
</tr>
</tbody>
</table>

**Explanation** The system failed to initialize an SFP connector in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
Recommended Action

Perform the following steps:
1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

Error Message

%FTD-1-114003: Failed to run cached commands in 4GE SSM I/O card (error_string).

Explanation

The system failed to run cached commands in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORTED
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action

Perform the following steps:
1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

Error Message

%FTD-6-114004: 4GE SSM I/O Initialization start.
Explanation The user has been notified that a 4GE SSM I/O initialization is starting.

• >syslog_id — Message identifier

Recommended Action None required.

114005

Error Message %FTD-6-114005: 4GE SSM I/O Initialization end.

Explanation The user has been notified that an 4GE SSM I/O initialization is finished.

• >syslog_id — Message identifier

Recommended Action None required.

114006

Error Message %FTD-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).

Explanation The Firepower Threat Defense device failed to obtain port statistics in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

• >syslog_id — Message identifier
• >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  • I2C_BUS_TRANSACTION_ERROR
  • I2C_CHKSUM_ERROR
  • I2C_TIMEOUT_ERROR
  • I2C_BUS_COLLISION_ERROR
  • I2C_HOST_BUSY_ERROR
  • I2C_UNPOPULATED_ERROR
  • I2C_SMBUS_UNSUPPORT
  • I2C_BYTE_COUNT_ERROR
  • I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:
1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114007

Error Message %FTD-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).

Explanation The Firepower Threat Defense device failed to obtain the current module status register information in a 4GE SSM I/O card because of an I2C error or a switch initialization error.
Error Message: %FTD-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.

Explanation: The Firepower Threat Defense device failed to enable a port after the link transition to Up state is detected in a 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

Recommended Action: Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.
114009

**Error Message** %FTD-3-114009: Failed to set multicast address in 4GE SSM I/O card (error \textit{error_string}).

**Explanation** The Firepower Threat Defense device failed to set the multicast address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- \textit{syslog_id} — Message identifier
- \textit{error_string} — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - \texttt{I2C\_BUS\_TRANSACTION\_ERROR}
  - \texttt{I2C\_CHKSUM\_ERROR}
  - \texttt{I2C\_TIMEOUT\_ERROR}
  - \texttt{I2C\_BUS\_COLLISION\_ERROR}
  - \texttt{I2C\_HOST\_BUSY\_ERROR}
  - \texttt{I2C\_UNPOPULATED\_ERROR}
  - \texttt{I2C\_SMBUS\_UNSUPPORT}
  - \texttt{I2C\_BYTE\_COUNT\_ERROR}
  - \texttt{I2C\_DATA\_PTR\_ERROR}

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114010

**Error Message** %FTD-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error \textit{error_string}).

**Explanation** The Firepower Threat Defense device failed to set the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- \textit{syslog_id} — Message identifier
- \textit{error_string} — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - \texttt{I2C\_BUS\_TRANSACTION\_ERROR}
  - \texttt{I2C\_CHKSUM\_ERROR}
  - \texttt{I2C\_TIMEOUT\_ERROR}
  - \texttt{I2C\_BUS\_COLLISION\_ERROR}
  - \texttt{I2C\_HOST\_BUSY\_ERROR}
  - \texttt{I2C\_UNPOPULATED\_ERROR}
  - \texttt{I2C\_SMBUS\_UNSUPPORT}
  - \texttt{I2C\_BYTE\_COUNT\_ERROR}
  - \texttt{I2C\_DATA\_PTR\_ERROR}
• I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114011

Error Message %FTD-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).

Explanation The Firepower Threat Defense device failed to delete the multicast address in a 4GE SSM I/O card because of either an I2C error or a switch initialization error.

• >syslog_id —Message identifier
• >error_string —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  • I2C_BUS_TRANSACTION_ERROR
  • I2C_CHKSUM_ERROR
  • I2C_TIMEOUT_ERROR
  • I2C_BUS_COLLISION_ERROR
  • I2C_HOST_BUSY_ERROR
  • I2C_UNPOPULATED_ERROR
  • I2C_SMBUS_UNSUPPORT
  • I2C_BYTE_COUNT_ERROR
  • I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114012

Error Message %FTD-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).

Explanation The Firepower Threat Defense device failed to delete the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

• >syslog_id —Message identifier
• >error_string —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114013

Error Message %FTD-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).

Explanation The Firepower Threat Defense device failed to set the MAC address table in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2CCHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.
**114014**

**Error Message** \%FTD-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).

**Explanation** The Firepower Threat Defense device failed to set the MAC address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

**114015**

**Error Message** \%FTD-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).

**Explanation** The Firepower Threat Defense device failed to set individual or promiscuous mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR
Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

**Error Message**%FTD-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).

**Explanation** The Firepower Threat Defense device failed to set the multicast mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

**Error Message**%FTD-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).
**Explanation** The Firepower Threat Defense device failed to obtain link status in a 4GE SSM I/O card because of an I2C serial bus access error or a switch access error.

- **syslog_id** — Message identifier
- **error_string** — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Notify the system administrator.
2. Log and review the messages and the errors associated with the event.
3. Reboot the software running on the Firepower Threat Defense device.
4. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
5. If the problem persists, contact the Cisco TAC.

**Error Message** `FTD-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string ).`

**Explanation** The Firepower Threat Defense device failed to set the port speed in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- **syslog_id** — Message identifier
- **error_string** — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR
- I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

### 114019

**Error Message** `%FTD-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).`

**Explanation** The Firepower Threat Defense device failed to set the media type in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >syslog_id — Message identifier
- >error_string — An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

### 114020

**Error Message** `%FTD-3-114020: Port link speed is unknown in 4GE SSM I/O card.`

**Explanation** The Firepower Threat Defense device cannot detect the port link speed in a 4GE SSM I/O card.

**Recommended Action** Perform the following steps:

1. Log and review the messages associated with the event.
2. Reset the 4GE SSM I/O card and observe whether or not the software automatically recovers from the event.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

**Error Message** 
%FTD-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.

**Explanation** The Firepower Threat Defense device failed to set the multicast address table in the 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

- **error**—A switch access error (a decimal error code) or an I2C serial bus error. Possible I2C serial bus errors include:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:
1. Log and review the messages associated with the event.
2. Try to reboot the Firepower Threat Defense device.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

**Error Message** 
%FTD-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string.

**Explanation** The Firepower Threat Defense device failed to pass broadcast traffic in the 4GE SSM I/O card because of a switch access error.

- **error_string**—A switch access error, which will be a decimal error code

**Recommended Action** Perform the following steps:
1. Log the message and errors surrounding the event.
2. Retrieve the ssm4ge_dump file from the compact flash, and send it to Cisco TAC.
3. Contact Cisco TAC with the information collected in Steps 1 and 2.
The 4GE SSM will be automatically reset and recover.

114023

**Error Message** %FTD-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to *error_string*.

**Explanation** A failure to cache or flush the MAC table in a 4GE SSM I/O card occurred because of an I2C serial bus access error or a switch access error. This message rarely occurs.

- *error_string*— Either an I2C serial bus error (see the second bullet for possible values) or a switch access error (which is a decimal error code).
- I2C serial bus errors are as follows:
  - I2C_BUS_TRANSACTION_ERROR
  - I2CCHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log the syslog message and the errors surrounding the event.
2. Try to software reboot the Firepower Threat Defense device.
3. Power cycle the Firepower Threat Defense device.

When you turn off the power, make sure that you wait several seconds before powering on again. After you complete steps 1-3, if the problem persists, contact the Cisco TAC and provide the information described in step 1. You may need to RMA the Firepower Threat Defense device.

115000

**Error Message** %FTD-2-115000: Critical assertion in process: *process name* fiber: *fiber name*, component: *component name*, subcomponent: *subcomponent name*, file: *filename*, line: *line number*, cond: *condition*

**Explanation** The critical assertion has gone off and is used during development in checked builds only, but never in production builds.

- *process name*— The name of the process
115001

**Error Message** %FTD-3-115001: Error in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition

**Explanation** An error assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- **fiber name**—The name of the fiber
- **component name**—The name of the specified component
- **subcomponent name**—The name of the specified subcomponent
- **filename**—The name of the specified file
- **line number**—The line number for the specified line
- **condition**—The specified condition

**Recommended Action** A high priority defect should be filed, the reason for the assertion should be investigated, and the problem corrected.

115002

**Error Message** %FTD-4-115002: Warning in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition

**Explanation** A warning assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- **fiber name**—The name of the fiber
- **component name**—The name of the specified component
- **subcomponent name**—The name of the specified subcomponent
- **filename**—The name of the specified file
- **line number**—The line number for the specified line
- **condition**—The specified condition

**Recommended Action** The reason for the assertion should be investigated and if a problem is found, a defect should be filed, and the problem corrected.
199001

**Error Message** %FTD-5-199001: Reload command executed from Telnet (remote IP_address).

**Explanation** The address of the host that is initiating an Firepower Threat Defense device reboot with the reload command has been recorded.

**Recommended Action** None required.

199002

**Error Message** %FTD-6-199002: startup completed. Beginning operation.

**Explanation** The Firepower Threat Defense device finished its initial boot and the flash memory reading sequence, and is ready to begin operating normally.

**Note** You cannot block this message by using the no logging message command.

**Recommended Action** None required.

199003

**Error Message** %FTD-6-199003: Reducing link MTU dec.

**Explanation** The Firepower Threat Defense device received a packet from the outside network that uses a larger MTU than the inside network. The Firepower Threat Defense device then sent an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the sequence number of the ICMP message.

**Recommended Action** None required.

199005

**Error Message** %FTD-6-199005: Startup begin

**Explanation** The Firepower Threat Defense device started.

**Recommended Action** None required.

199010

**Error Message** %FTD-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0

**Explanation** The system has recovered from a serious error.

**Recommended Action** Contact the Cisco TAC.
199011

**Error Message**  %FTD-2-199011: Close on bad channel in process/fiber process/fiber, channel ID p, channel state s process/fiber name of the process/fiber that caused the bad channel close operation.

**Explanation** An unexpected channel close condition has been detected.

- p—The channel ID
- process/fiber—The name of the process/fiber that caused the bad channel close operation
- s—The channel state

**Recommended Action** Contact the Cisco TAC and attach a log file.

199012

**Error Message**  %FTD-1-199012: Stack smash during new_stack_call in process/fiber process/fiber, call target f, stack size s, process/fiber name of the process/fiber that caused the stack smash

**Explanation** A stack smash condition has been detected.

- f—The target of the new_stack_call
- process/fiber—The name of the process/fiber that caused the stack smash
- s—The new stack size specified in new_stack_call

**Recommended Action** Contact the Cisco TAC and attach a log file.

199013

**Error Message**  %FTD-1-199013: syslog

**Explanation** A variable syslog was generated by an assistive process.

- syslog—The alert syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

199014

**Error Message**  %FTD-2-199014: syslog

**Explanation** A variable syslog was generated by an assistive process.

- syslog—The critical syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

199015

**Error Message**  %FTD-3-199015: syslog

**Explanation** A variable syslog was generated by an assistive process.

- syslog—The error syslog passed verbatim from an external process
Recommended Action Contact the Cisco TAC.

199016

Error Message %FTD-4-199016: syslog
Explanation A variable syslog was generated by an assistive process.
  • syslog—The warning syslog passed verbatim from an external process
Recommended Action Contact the Cisco TAC.

199017

Error Message %FTD-5-199017: syslog
Explanation A variable syslog was generated by an assistive process.
  • syslog—The notification syslog passed verbatim from an external process
Recommended Action None required.

199018

Error Message %FTD-6-199018: syslog
Explanation A variable syslog was generated by an assistive process.
  • syslog—The informational syslog passed verbatim from an external process
Recommended Action None required.

199019

Error Message %FTD-7-199019: syslog
Explanation A variable syslog was generated by an assistive process.
  • syslog—The debugging syslog passed verbatim from an external process
Recommended Action None required.

199020

Error Message %FTD-2-199020: System memory utilization has reached X %. System will reload if memory usage reaches the configured trigger level of Y %.
Explanation The system memory utilization has reached 80% of the system memory watchdog facility's configured value.
Recommended Action Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.
**Error Message** %FTD-1-199021: System memory utilization has reached the configured watchdog trigger level of 100%. System will now reload.

**Explanation** The system memory utilization has reached 100% of the system memory watchdog facility's configured value. The system will automatically reload.

**Recommended Action** Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.
Syslog Messages 201002 to 219002

This chapter contains the following sections:

- Messages 201002 to 210022, on page 81
- Messages 211001 to 219002, on page 88

Messages 201002 to 210022

This chapter includes messages from 201002 to 210022.

**201002**

**Error Message**  
%FTD-3-201002: Too many TCP connections on {static|xlate} global_address ! econns nconns

**Explanation**  
The maximum number of TCP connections to the specified global address was exceeded.

- econns—The maximum number of embryonic connections
- nconns—The maximum number of connections permitted for the static or xlate global address

**Recommended Action**  
Use the show static or show nat command to check the limit imposed on connections to a static address. The limit is configurable.

**201003**

**Error Message**  
%FTD-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address ) inside_address /inside_port on interface interface_name

**Explanation**  
The number of embryonic connections from the specified foreign address with the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the Firepower Threat Defense device is reached, the Firepower Threat Defense device attempts to accept them anyway, but puts a time limit on the connections. This situation allows some connections to succeed even if the Firepower Threat Defense device is very busy. This message indicates a more serious overload than message 201002, which can be caused by a SYN attack, or by a very heavy load of legitimate traffic.

- nconns—The maximum number of embryonic connections received
- elimit —The maximum number of embryonic connections specified in the static or nat command
**Recommended Action** Use the show static command to check the limit imposed on embryonic connections to a static address.

**201004**

**Error Message** %FTD-3-201004: Too many UDP connections on \{static\|xlate\} global_address!udp connections limit

**Explanation** The maximum number of UDP connections to the specified global address was exceeded.

- udp conn limit—The maximum number of UDP connections permitted for the static address or translation

**Recommended Action** Use the show static or show nat command to check the limit imposed on connections to a static address. You can configure the limit.

**201005**

**Error Message** %FTD-3-201005: FTP data connection failed for IP_address

**Explanation** The Firepower Threat Defense device cannot allocate a structure to track the data connection for FTP because of insufficient memory.

**Recommended Action** Reduce the amount of memory usage or purchase additional memory.

**201006**

**Error Message** %FTD-3-201006: RCMD backconnection failed for IP_address/port.

**Explanation** The Firepower Threat Defense device cannot preallocate connections for inbound standard output for rsh commands because of insufficient memory.

**Recommended Action** Check the rsh client version; the Firepower Threat Defense device only supports the Berkeley rsh client version. You can also reduce the amount of memory usage, or purchase additional memory.

**201008**

**Error Message** %FTD-3-201008: Disallowing new connections.

**Explanation** You have enabled TCP system log messaging and the syslog server cannot be reached.

**Recommended Action** Disable TCP syslog messaging. Also, make sure that the syslog server is up and you can ping the host from the Firepower Threat Defense console. Then restart TCP system message logging to allow traffic.

**201009**

**Error Message** %FTD-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded

**Explanation** The maximum number of connections to the specified static address was exceeded.

- number—The maximum of connections permitted for the host
- IP_address—The host IP address
• interface_name—The name of the interface to which the host is connected

**Recommended Action** Use the show static and show nat commands to check the limit imposed on connections to an address. The limit is configurable.

---

**201010**

**Error Message** %FTD-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name

**Explanation** An attempt to establish a TCP connection failed because of an exceeded embryonic connection limit, which was configured with the set connection embryonic-conn-max MPC command for a traffic class.

- econns—The current count of embryonic connections associated to the configured traffic class
- limit—The configured embryonic connection limit for the traffic class
- dir—input: The first packet that initiates the connection is an input packet on the interface interface_name
  output: The first packet that initiates the connection is an output packet on the interface interface_name
- source_address/source_port —The source real IP address and the source port of the packet initiating the connection
- dest_address/dest_port —The destination real IP address and the destination port of the packet initiating the connection
- interface_name—The name of the interface on which the policy limit is enforced

**Recommended Action** None required.

---

**201011**

**Error Message** %FTD-3-201011: Connection limit exceeded cnt /limit for dir packet from sip /sport to dip /dport on interface if_name.

**Explanation** A new connection through the Firepower Threat Defense device resulted in exceeding at least one of the configured maximum connection limits. This message applies both to connection limits configured using a static command, or to those configured using Cisco Modular Policy Framework. The new connection will not be allowed through the Firepower Threat Defense device until one of the existing connections is torn down, which brings the current connection count below the configured maximum.

- cnt—Current connection count
- limit—Configured connection limit
- dir—Direction of traffic, inbound or outbound
- sip—Source real IP address
- sport—Source port
- dip—Destination real IP address
- dport—Destination port
- if_name—Name of the interface on which the traffic was received

**Recommended Action** None required.

---

**201012**

**Error Message** %FTD-6-201012: Per-client embryonic connection limit exceeded curr num /limit for [input|output] packet from IP_address / port to ip /port on interface interface_name
**Explanation** An attempt to establish a TCP connection failed because the per-client embryonic connection limit was exceeded. By default, this message is rate limited to 1 message every 10 seconds.

- **curr num**—The current number
- **limit**—The configured limit
- [input/output]—Input or output packet on interface **interface_name**
- **IP_address**—Real IP address
- **port**—TCP or UDP port
- **interface_name**—The name of the interface on which the policy is applied

**Recommended Action** When the limit is reached, any new connection request will be proxied by the Firepower Threat Defense device to prevent a SYN flood attack. The Firepower Threat Defense device will only connect to the server if the client is able to finish the three-way handshake. This usually does not affect the end user or the application. However, if this creates a problem for any application that has a legitimate need for a higher number of embryonic connections, you can adjust the setting by entering the `set connection per-client-embryonic-max` command.

### 201013

**Error Message** %FTD-3-201013: Per-client connection limit exceeded curr num /limit for [input/output] packet from ip /port to ip /port on interface **interface_name**

**Explanation** A connection was rejected because the per-client connection limit was exceeded.

- **curr num**—The current number
- **limit**—The configured limit
- [input/output]—The input or output packet on interface **interface_name**
- **ip**—The real IP address
- **port**—The TCP or UDP port
- **interface_name**—The name of the interface on which the policy is applied

**Recommended Action** When the limit is reached, any new connection request will be silently dropped. Normally an application will retry the connection, which will cause a delay or even a timeout if all retries also fail. If an application has a legitimate need for a higher number of concurrent connections, you can adjust the setting by entering the `set connection per-client-max` command.

### 202010

**Error Message** %FTD-3-202010: {NAT | PAT} pool exhausted for **pool-name**, port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface :src-ip /src-port to out-interface :dst-ip /dst-port

**Explanation**

- **pool-name**—The name of the NAT or PAT pool
- **protocol**—The protocol used to create the connection
- **in-interface**—The ingress interface
- **src-ip**—The source IP address
- **src-port**—The source port
- **out-interface**—The egress interface
- **dest-ip**—The destination IP address
• **dst-port** — The destination port

The Firepower Threat Defense device has no more address translation pools available.

**Recommended Action** Use the `show nat pool` and `show nat detail` commands to determine why all addresses and ports in the pool are used up. If this occurs under normal conditions, then add additional IP addresses to the NAT/PAT pool.

### 202016

**Error Message** %FTD-3-202016: "%d: Unable to pre-allocate SIP %s secondary channel for message" "from %s:%A/%d to %s:%A/%d with PAT and missing port information."

**Explanation**

When SIP application generates an SDP payload with Media port set to 0, you cannot allocate a PAT xlate for such invalid port request and drop the packet with this syslog.

**Recommended Action** None. This is an application specific issue.

### 208005

**Error Message** %FTD-3-208005: (function;line_num) clear command return code

**Explanation**

The Firepower Threat Defense device received a nonzero value (an internal error) when attempting to clear the configuration in flash memory. The message includes the reporting subroutine filename and line number.

**Recommended Action** For performance reasons, the end host should be configured not to inject IP fragments. This configuration change is probably because of NFS. Set the read and write size equal to the interface MTU for NFS.

### 209003

**Error Message** %FTD-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number

**Explanation**

Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (to raise the maximum, see the `fragment size` command in the command reference guide). The Firepower Threat Defense device limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the Firepower Threat Defense device under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. An exception is in a network environment with NFS over UDP where a large percentage is fragmented traffic; if this type of traffic is relayed through the Firepower Threat Defense device, consider using NFS over TCP instead. To prevent fragmentation, see the `sysopt connection tcpmss bytes` command in the command reference guide.

**Recommended Action** If this message persists, a denial of service (DoS) attack might be in progress. Contact the remote peer administrator or upstream provider.

### 209004

**Error Message** %FTD-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number
**Explanation** An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.

**Recommended Action** A possible intrusion event may be in progress. If this message persists, contact the remote peer administrator or upstream provider.

---

**209005**

**Error Message** %FTD-4-209005: Discard IP fragment set with more than number elements: src - Too many elements are in a fragment set.

**Explanation** The Firepower Threat Defense device disallows any IP packet that is fragmented into more than 24 fragments. For more information, see the `fragment` command in the command reference guide.

**Recommended Action** A possible intrusion event may be in progress. If the message persists, contact the remote peer administrator or upstream provider. You can change the number of fragments per packet by using the `fragment chain xxx interface_name` command.

---

**210001**

**Error Message** %FTD-3-210001: LU sw_module_name error - number

**Explanation** A Stateful Failover error occurred.

**Recommended Action** If this error persists after traffic lessens through the Firepower Threat Defense device, report this error to the Cisco TAC.

---

**210002**

**Error Message** %FTD-3-210002: LU allocate block (bytes) failed.

**Explanation** Stateful Failover cannot allocate a block of memory to transmit stateful information to the standby Firepower Threat Defense device.

**Recommended Action** Check the failover interface using the `show interface` command to make sure its transmit is normal. Also check the current block memory using the `show block` command. If current available count is 0 within any of the blocks of memory, then reload the Firepower Threat Defense software to recover the lost blocks of memory.

---

**210003**

**Error Message** %FTD-3-210003: Unknown LU Object number

**Explanation** Stateful Failover received an unsupported Logical Update object and was unable to process it. This can be caused by corrupted memory, LAN transmissions, and other events.

**Recommended Action** If you see this error infrequently, then no action is required. If this error occurs frequently, check the Stateful Failover link LAN connection. If the error was not caused by a faulty failover link LAN connection, determine if an external user is trying to compromise the protected network. Also check for misconfigured clients.
210005

Error Message %FTD-3-210005: LU allocate secondary (optional) connection failed for protocol [TCP | UDP] connection from ingress interface name :Real IP Address /Real Port to egress interface name :Real IP Address /Real Port

Explanation Stateful Failover cannot allocate a new connection on the standby unit. This may be caused by little or no RAM memory available within the Firepower Threat Defense device.

Note The secondary field in the syslog message is optional and appears only if the connection is a secondary connection.

Recommended Action Check the available memory using the show memory command to make sure that the Firepower Threat Defense device has free memory. If there is no available memory, add more physical memory to the Firepower Threat Defense device.

210006

Error Message %FTD-3-210006: LU look NAT for IP_address failed

Explanation Stateful Failover was unable to locate a NAT group for the IP address on the standby unit. The active and standby Firepower Threat Defense devices may be out-of-sync with each other.

Recommended Action Use the write standby command on the active unit to synchronize system memory with the standby unit.

210007

Error Message %FTD-3-210007: LU allocate xlate failed for type [static | dynamic]=[NAT | PAT] secondary (optional) protocol translation from ingress interface name :Real IP Address /real port (Mapped IP Address /Mapped Port ) to egress interface name :Real IP Address /Real Port (Mapped IP Address /Mapped Port )

Explanation Stateful Failover failed to allocate a translation slot record.

Recommended Action Check the available memory by using the show memory command to make sure that the Firepower Threat Defense device has free memory available. If no memory is available, add more memory.

210008

Error Message %FTD-3-210008: LU no xlate for inside_address /inside_port outside_address /outside_port

Explanation The Firepower Threat Defense device cannot find a translation slot record for a Stateful Failover connection; as a result, the Firepower Threat Defense device cannot process the connection information.

Recommended Action Use the write standby command on the active unit to synchronize system memory between the active and standby units.
**210010**

**Error Message**  
%FTD-3-210010: LU make UDP connection for outside_address :outside_port  
inside_address :inside_port failed

**Explanation**  
Stateful Failover was unable to allocate a new record for a UDP connection.

**Recommended Action**  
Check the available memory by using the `show memory` command to make sure that the Firepower Threat Defense device has free memory available. If no memory is available, add more memory.

**210020**

**Error Message**  
%FTD-3-210020: LU PAT port port reserve failed

**Explanation**  
Stateful Failover is unable to allocate a specific PAT address that is in use.

**Recommended Action**  
Use the `write standby` command on the active unit to synchronize system memory between the active and standby units.

**210021**

**Error Message**  
%FTD-3-210021: LU create static xlate global_address iface interface_name failed

**Explanation**  
Stateful Failover is unable to create a translation slot.

**Recommended Action**  
Enter the `write standby` command on the active unit to synchronize system memory between the active and standby units.

**210022**

**Error Message**  
%FTD-6-210022: LU missed number updates

**Explanation**  
Stateful Failover assigns a sequence number for each record sent to the standby unit. When a received record sequence number is out of sequence with the last updated record, the information in between is assumed to be lost, and this error message is sent as a result.

**Recommended Action**  
Unless LAN interruptions occur, check the available memory on both Firepower Threat Defense units to ensure that enough memory is available to process the stateful information. Use the `show failover` command to monitor the quality of stateful information updates.

**Messages 211001 to 219002**

This chapter includes messages from 211001 to 219002.

**211001**

**Error Message**  
%FTD-3-211001: Memory allocation Error

**Explanation**  
The Firepower Threat Defense device failed to allocate RAM system memory.

**Recommended Action**  
If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.
211003

Error Message %FTD-3-211003: Error in computed percentage CPU usage value

Explanation The percentage of CPU usage is greater than 100 percent.

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

211004

Error Message %FTD-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.

Explanation The Firepower Threat Defense device does not meet the minimum memory requirements for this version.

• ver—Running image version number
• min—Minimum required amount of RAM to run the installed image.
• actual—Amount of RAM currently installed in the system

Recommended Action Install the required amount of RAM.

212001

Error Message %FTD-3-212001: Unable to open SNMP channel (UDP port port ) on interface interface_number , error code = code

Explanation The Firepower Threat Defense device is unable to receive SNMP requests destined for the Firepower Threat Defense device from SNMP management stations located on this interface. The SNMP traffic passing through the Firepower Threat Defense device on any interface is not affected. The error codes are as follows:

• An error code of -1 indicates that the Firepower Threat Defense device cannot open the SNMP transport for the interface. This can occur when the user attempts to change the port on which SNMP accepts queries to one that is already in use by another feature. In this case, the port used by SNMP will be reset to the default port for incoming SNMP queries (UDP 161).
• An error code of -2 indicates that the Firepower Threat Defense device cannot bind the SNMP transport for the interface.

Recommended Action After the Firepower Threat Defense device reclaims some of its resources when traffic is lighter, reenter the snmp-server host command for that interface.

212002

Error Message %FTD-3-212002: Unable to open SNMP trap channel (UDP port port ) on interface interface_number , error code = code

Explanation The Firepower Threat Defense device is unable to send its SNMP traps from the Firepower Threat Defense device to SNMP management stations located on this interface. The SNMP traffic passing through the Firepower Threat Defense device on any interface is not affected. The error codes are as follows:
• An error code of -1 indicates that the Firepower Threat Defense device cannot open the SNMP trap transport for the interface.
• An error code of -2 indicates that the Firepower Threat Defense device cannot bind the SNMP trap transport for the interface.
• An error code of -3 indicates that the Firepower Threat Defense device cannot set the trap channel as write-only.

**Recommended Action** After the Firepower Threat Defense device reclaims some of its resources when traffic is lighter, reenter the snmp-server host command for that interface.

---

**212003**

**Error Message** `%FTD-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.`

**Explanation** An internal error occurred in receiving an SNMP request destined for the Firepower Threat Defense device on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Firepower Threat Defense device cannot find a supported transport type for the interface.
- An error code of -5 indicates that the Firepower Threat Defense device received no data from the UDP channel for the interface.
- An error code of -7 indicates that the Firepower Threat Defense device received an incoming request that exceeded the supported buffer size.
- An error code of -14 indicates that the Firepower Threat Defense device cannot determine the source IP address from the UDP channel.
- An error code of -22 indicates that the Firepower Threat Defense device received an invalid parameter.

**Recommended Action** None required. The Firepower Threat Defense SNMP agent goes back to wait for the next SNMP request.

---

**212004**

**Error Message** `%FTD-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code`

**Explanation** An internal error occurred in sending an SNMP response from the Firepower Threat Defense device to the specified host on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Firepower Threat Defense device cannot find a supported transport type for the interface.
- An error code of -2 indicates that the Firepower Threat Defense device sent an invalid parameter.
- An error code of -3 indicates that the Firepower Threat Defense device was unable to set the destination IP address in the UDP channel.
- An error code of -4 indicates that the Firepower Threat Defense device sent a PDU length that exceeded the supported UDP segment size.
- An error code of -5 indicates that the Firepower Threat Defense device was unable to allocate a system block to construct the PDU.

**Recommended Action** None required.
212005

Error Message %FTD-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.

Explanation The length of the incoming SNMP request that is destined for the Firepower Threat Defense device exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing. The Firepower Threat Defense device is unable to process this request. The SNMP traffic passing through the Firepower Threat Defense device on any interface is not affected.

Recommended Action Have the SNMP management station resend the request with a shorter length. For example, instead of querying multiple MIB variables in one request, try querying only one MIB variable in a request. You may need to modify the configuration of the SNMP manager software.

212006

Error Message %FTD-3-212006: Dropping SNMP request from src_addr /src_port to ifc : dst_addr /dst_port because: reason username

Explanation The Firepower Threat Defense device cannot process the SNMP request being sent to it for the following reasons:

• user not found—The username cannot be located in the local SNMP user database.
• username exceeds maximum length—The username embedded in the PDU exceeds the maximum length allowed by the SNMP RFCs.
• authentication algorithm failure—An authentication failure caused by an invalid password or a packet authenticated using the incorrect algorithm.
• privacy algorithm failure—A privacy failure caused by an invalid password or a packet encrypted using the incorrect algorithm.
• error decrypting request—An error occurred in the platform crypto module decrypting the user request.
• error encrypting response—An error occurred in the platform crypto module encrypting the user response or trap notification.
• engineBoots has reached maximum value—The engineBoots variable has reached the maximum allowed value. For more information, see message 212011.

Note The username appears after each reason listed.

Recommended Action Check the Firepower Threat Defense SNMP server settings and confirm that the NMS configuration is using the expected user, authentication, and encryption settings. Enter the show crypto accelerator statistics command to isolate errors in the platform crypto module.

212009

Error Message %FTD-5-212009: Configuration request for SNMP group groupname failed. User username , reason .

Explanation A user has tried to change the SNMP server group configuration. One or more users that refer to the group have insufficient settings to comply with the requested group changes.

• groupname—A string that represents the group name
• username — A string that represents the username
• reason — A string that represents one of the following reasons:
  - missing auth-password — A user has tried to add authentication to the group, and the user has not specified an authentication password
  - missing priv-password — A user has tried to add privacy to the group, and the user has not specified an encryption password
  - reference group intended for removal — A user has tried to remove a group that has users belonging to it

**Recommended Action** The user must update the indicated user configurations before changing the group or removing indicated users, and then add them again after making changes to the group.

---

**212010**

**Error Message** %FTD-3-212010: Configuration request for SNMP user %s failed. Host %s reason.

**Explanation** A user has tried to change the SNMP server user configuration by removing one or more hosts that reference the user. One message is generated per host.

- %s — A string that represents the username or hostname
- reason — A string that represents the following reason:
  - references user intended for removal — The name of the user to be removed from the host.

**Recommended Action** The user must either update the indicated host configuration before changing a user or remove the indicated hosts, then add them again after making changes to the user.

---

**212011**

**Error Message** %FTD-3-212011: SNMP engineBoots is set to maximum value. Reason: %s User intervention necessary.

For example:

%FTD-3-212011: SNMP engineBoots is set to maximum value. Reason: error accessing persistent data. User intervention necessary.

**Explanation** The device has rebooted 214783647 times, which is the maximum allowed value of the engineBoots variable, or an error reading the persistent value from flash memory has occurred. The engineBoots value is stored in flash memory in the flash:/snmp/ctx-name file, where ctx-name is the name of the context. In single mode, the name of this file is flash:/snmp/single_vf. In multi-mode, the name of the file for the admin context is flash:/snmp/admin. During a reboot, if the device is unable to read from the file or write to the file, the engineBoots value is set to the maximum.

- %s — A string that represents the reason that the engineBoots value is set to the maximum allowed value.
  The two valid strings are “device reboots” and “error accessing persistent data.”

**Recommended Action** For the first string, the administrator must delete all SNMP Version 3 users and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed. For the second string, the administrator must delete the context-specific file, then delete all SNMP Version users, and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed.
212012

Error Message %FTD-3-212012: Unable to write SNMP engine data to persistent storage.

Explanation The SNMP engine data is written to the file, flash:/snmp/context-name. For example: in single mode, the data is written to the file, flash:/snmp/single_vf. In the admin context in multi-mode, the file is written to the directory, flash:/snmp/admin. The error may be caused by a failure to create the flash:/snmp directory or the flash:/snmp/context-name file. The error may also be caused by a failure to write to the file.

Recommended Action The system administrator should remove the flash:/snmp/context-name file, then remove all SNMP Version 3 users, and add them again. This procedure should recreate the flash:/snmp/context-name file. If the problem persists, the system administrator should try reformattting the flash.

214001

Error Message %FTD-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes.

Explanation An incoming encrypted data packet destined for the Firepower Threat Defense management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The Firepower Threat Defense device immediately terminates this management connection.

Recommended Action Ensure that the management connection was initiated by Cisco Secure Policy Manager.

215001

Error Message %FTD-2-215001: Bad route_compress() call, sdb = number

Explanation An internal software error occurred.

Recommended Action Contact the Cisco TAC.

216001

Error Message %FTD-n-216001: internal error in: function : message

Explanation Various internal errors have occurred that should not appear during normal operation. The severity level varies depending on the cause of the message.

- n—The message severity
- function—The affected component
- message—A message describing the cause of the problem

Recommended Action Search the Bug Toolkit for the specific text message and try to use the Output Interpreter to resolve the problem. If the problem persists, contact the Cisco TAC.

216002

Error Message FTD-3-216002: Unexpected event (major: major_id , minor: minor_id ) received by task_string in function at line: line_num
**Explanation** A task registers for event notification, but the task cannot handle the specific event. Events that can be watched include those associated with queues, booleans, and timer services. If any of the registered events occur, the scheduler wakes up the task to process the event. This message is generated if an unexpected event woke up the task, but it does not know how to handle the event.

If an event is left unprocessed, it can wake up the task very often to make sure that it is processed, but this should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- **major_id** — Event identifier
- **minor_id** — Event identifier
- **task_string** — Custom string passed by the task to identify itself
- **function** — The function that received the unexpected event
- **line_num** — Line number in the code

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

---

**216003**

**Error Message** 
%FTD-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num

**Explanation** An unexpected timer event woke up the task, but the task does not know how to handle the event. A task can register a set of timer services with the scheduler. If any of the timers expire, the scheduler wakes up the task to take action. This message is generated if the task is awakened by an unrecognized timer event.

An expired timer, if left unprocessed, wakes up the task continuously to make sure that it is processed, and this is undesirable. This should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- **timer_ptr** — Pointer to the timer
- **timer_id** — Timer identifier
- **task_string** — Custom string passed by the task to identify itself
- **function** — The function that received the unexpected event
- **line_num** — Line number in the code

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

---

**216004**

**Error Message** 
%FTD-4-216004: prevented: error in function at file (line) - stack trace

**Explanation** An internal logic error has occurred, which should not occur during normal operation.

- **error** — Internal logic error. Possible errors include the following:
  - Exception
  - Dereferencing null pointer
  - Array index out of bounds
  - Invalid buffer size
  - Writing from input
- Source and destination overlap
- Invalid date
- Access offset from array indices
  - function — The calling function that generated the error
  - file(line) — The file and line number that generated the error
  - stack trace — Full call stack traceback, starting with the calling function. For example: ("0x001010a4 0x00304e58 0x00670060 0x00130b04")

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

### 217001

<table>
<thead>
<tr>
<th>Error Message</th>
<th>%FTD-2-217001: No memory for string in string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>An operation failed because of low memory.</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended Action</strong> If sufficient memory exists, then send the error message, the configuration, and any details about the events leading up to the error to the Cisco TAC.</td>
</tr>
</tbody>
</table>

### 218001

<table>
<thead>
<tr>
<th>Error Message</th>
<th>%FTD-2-218001: Failed Identification Test in slot# [fail #/res ].</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>The module in slot# of the Firepower Threat Defense device cannot be identified as a genuine Cisco product. Cisco warranties and support programs apply only to genuine Cisco products. If Cisco determines that the cause of a support issue is related to non-Cisco memory, SSM modules, SSC modules, or other modules, Cisco may deny support under your warranty or under a Cisco support program such as SmartNet.</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended Action</strong> If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.</td>
</tr>
</tbody>
</table>

### 218002

<table>
<thead>
<tr>
<th>Error Message</th>
<th>%FTD-2-218002: Module (slot# ) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>The hardware in the specified location is a prototype module that came from a Cisco lab.</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended Action</strong> If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.</td>
</tr>
</tbody>
</table>

### 218003

<table>
<thead>
<tr>
<th>Error Message</th>
<th>%FTD-2-218003: Module Version in slot# is obsolete. The module in slot – slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>Obsolete hardware has been detected or the show module command has been run for the module. This message is generated once per minute after it first appears.</td>
</tr>
</tbody>
</table>
**Recommended Action** If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

---

**218004**

**Error Message**  %FTD-2-218004: Failed Identification Test in slot# [fail# /res ]

**Explanation** A problem occurred while identifying hardware in the specified location.

**Recommended Action** If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

---

**218005**

**Error Message**  %FTD-2-218005: Inconsistency detected in the system information programmed in non-volatile memory

**Explanation** System information programmed in non-volatile memory is not consistent. This syslog will be generated during bootup if Firepower Threat Defense device detects that the contents of the IDPROM are not identical to the contents of ACT2 EEPROM. Since the IDPROM and ACT2 EEPROM are programmed with exactly the same contents in manufacturing, this would happen either due to an error in manufacturing or if the IDPROM contents are tampered with.

**Recommended Action** If the message recurs, collect the output of the show tech-support command and contact Cisco TAC.

---

**219002**

**Error Message**  %FTD-3-219002: I2C_API_name error, slot = slot_number , device = device_number , address = address , byte count = count . Reason: reason_string

**Explanation** The I2C serial bus API has failed because of a hardware or software problem.

- **I2C_API_name** —The I2C API that failed, which can be one of the following:
  - I2C_read_byte_w_wait()
  - I2C_read_word_w_wait()
  - I2C_read_block_w_wait()
  - I2C_write_byte_w_wait()
  - I2C_write_word_w_wait()
  - I2C_write_block_w_wait()
  - I2C_read_byte_w_suspend()
  - I2C_read_word_w_suspend()
  - I2C_read_block_w_suspend()
  - I2C_write_byte_w_suspend()
  - I2C_write_word_w_suspend()
  - I2C_write_block_w_suspend()

- **slot_number** —The hexadecimal number of the slot where the I/O operation that generated the message occurred. The slot number cannot be unique to a slot in the chassis. Depending on the chassis, two
different slots might have the same I2C slot number. Also, the value is not necessarily less than or equal to the number of slots. The value depends on the way the I2C hardware is wired.

- **device_number** — The hexadecimal number of the device on the slot for which the I/O operation was performed
- **address** — The hexadecimal address of the device on which the I/O operation occurred
- **byte_count** — The byte count in decimal format of the I/O operation
- **error_string** — The reason for the error, which can be one of the following:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event. If the message does not occur continuously and disappears after a few minutes, it might be because the I2C serial bus is busy.
2. Reboot the software running on the Firepower Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure that you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.
Syslog Messages 302003 to 341011

This chapter contains the following sections:

- Messages 302003 to 319004, on page 99
- Messages 320001 to 341011, on page 125

Messages 302003 to 319004

This chapter includes messages from 302003 to 319004.

302003

**Error Message**  %FTD-6-302003: Built H245 connection for foreign_address outside_address /outside_port local_address inside_address /inside_port

**Explanation** An H.245 connection has been started from the **outside_address** to the **inside_address**. The Firepower Threat Defense device has detected the use of an Intel Internet Phone. The foreign port (**outside_port**) only appears on connections from outside the Firepower Threat Defense device. The local port value (**inside_port**) only appears on connections that were started on an internal interface.

**Recommended Action** None required.

302004

**Error Message**  %FTD-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address /outside_port to local_address inside_address /inside_port

**Explanation** An H.323 UDP back connection has been preallocated to the foreign address (**outside_address**) from the local address (**inside_address**). The Firepower Threat Defense device has detected the use of an Intel Internet Phone. The foreign port (**outside_port**) only appears on connections from outside the Firepower Threat Defense device. The local port value (**inside_port**) only appears on connections that were started on an internal interface.

**Recommended Action** None required.

302010

**Error Message**  %FTD-6-302010: connections in use, connections most used
Explanation Provides information on the number of connections that are in use and most used.

- connections—The number of connections

Recommended Action None required.

Error Message %FTD-6-302012: Pre-allocate H.225 Call Signalling Connection for faddr IP_address /port to laddr IP_address

Explanation An H.225 secondary channel has been preallocated.

Recommended Action None required.

Error Message %FTD-6-302013: Built {inbound|outbound} TCP connection_id for interface :real-address /real-port {mapped-address(mapped-port) (idfw_user)[]} to interface :real-address /real-port {mapped-address(mapped-port) (idfw_user)[]} [(user)[]]

Explanation A TCP connection slot between two hosts was created.

- connection_id—A unique identifier
- interface, real-address, real-port—The actual sockets
- mapped-address, mapped-port—The mapped sockets
- user—The AAA name of the user
- idfw_user—The name of the identity firewall user

If inbound is specified, the original control connection was initiated from the outside. For example, for FTP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, the original control connection was initiated from the inside.

Recommended Action None required.

Error Message %FTD-6-302014: Teardown TCP connection id for interface :real-address /real-port [(idfw_user)[]] to interface :real-address /real-port [(idfw_user)[]] duration hh:mm:ss bytes bytes [reason [from teardown-initiator]] [(user)[]]}

Explanation A TCP connection between two hosts was deleted. The following list describes the message values:

- id—A unique identifier
- interface, real-address, real-port—The actual socket
- duration—The lifetime of the connection
- bytes—The data transfer of the connection
- User—The AAA name of the user
- idfw_user—The name of the identity firewall user

Recommended Action None required.
- **reason**—The action that causes the connection to terminate. Set the `reason` variable to one of the TCP termination reasons listed in the following table.

- **teardown-initiator**—Interface name of the side that initiated the teardown.

### Table 4: TCP Termination Reasons

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conn-timeout</td>
<td>The connection ended when a flow is closed because of the expiration of its inactivity timer.</td>
</tr>
<tr>
<td>Deny Terminate</td>
<td>Flow was terminated by application inspection.</td>
</tr>
<tr>
<td>Failover primary closed</td>
<td>The standby unit in a failover pair deleted a connection because of a message received from the active unit.</td>
</tr>
<tr>
<td>FIN Timeout</td>
<td>Force termination after 10 minutes awaiting the last ACK or after half-closed timeout.</td>
</tr>
<tr>
<td>Flow closed by inspection</td>
<td>Flow was terminated by the inspection feature.</td>
</tr>
<tr>
<td>Flow terminated by IPS</td>
<td>Flow was terminated by IPS.</td>
</tr>
<tr>
<td>Flow reset by IPS</td>
<td>Flow was reset by IPS.</td>
</tr>
<tr>
<td>Flow terminated by TCP Intercept</td>
<td>Flow was terminated by TCP Intercept.</td>
</tr>
<tr>
<td>Flow timed out</td>
<td>Flow has timed out.</td>
</tr>
<tr>
<td>Flow timed out with reset</td>
<td>Flow has timed out, but was reset.</td>
</tr>
<tr>
<td>Flow is a loopback</td>
<td>Flow is a loopback.</td>
</tr>
<tr>
<td>Free the flow created as result of packet injection</td>
<td>The connection was built because the packet tracer feature sent a simulated packet through the Firepower Threat Defense device.</td>
</tr>
<tr>
<td>Invalid SYN</td>
<td>The SYN packet was not valid.</td>
</tr>
<tr>
<td>IPS fail-close</td>
<td>Flow was terminated because the IPS card is down.</td>
</tr>
<tr>
<td>No interfaces associated with zone</td>
<td>Flows were torn down after the “no nameif” or “no zone-member” leaves a zone with no interface members.</td>
</tr>
<tr>
<td>No valid adjacency</td>
<td>This counter is incremented when the Firepower Threat Defense device tried to obtain an adjacency and could not obtain the MAC address for the next hop. The packet is dropped.</td>
</tr>
<tr>
<td>Pinhole Timeout</td>
<td>The counter is incremented to report that the Firepower Threat Defense device opened a secondary flow, but no packets passed through this flow within the timeout interval, and so it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel.</td>
</tr>
<tr>
<td>Reason</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Route change</td>
<td>When the Firepower Threat Defense device adds a lower cost (better metric) route, packets arriving that match the new route cause their existing connection to be torn down after the user-configured timeout (floating-conn) value. Subsequent packets rebuild the connection out of the interface with the better metric. To prevent the addition of lower cost routes from affecting active flows, you can set the floating-conn configuration timeout value to 0:0:0.</td>
</tr>
<tr>
<td>SYN Control</td>
<td>A back channel initiation occurred from the wrong side.</td>
</tr>
<tr>
<td>SYN Timeout</td>
<td>Force termination after 30 seconds, awaiting three-way handshake completion.</td>
</tr>
<tr>
<td>TCP bad retransmission</td>
<td>The connection was terminated because of a bad TCP retransmission.</td>
</tr>
<tr>
<td>TCP FINs</td>
<td>A normal close-down sequence occurred. The IP address follows the reason.</td>
</tr>
<tr>
<td>TCP Invalid SYN</td>
<td>Invalid TCP SYN packet.</td>
</tr>
<tr>
<td>TCP Reset - APPLIANCE</td>
<td>The flow is closed when a TCP reset is generated by the Firepower Threat Defense device.</td>
</tr>
<tr>
<td>TCP Reset - I</td>
<td>Reset was from the inside.</td>
</tr>
<tr>
<td>TCP Reset - O</td>
<td>Reset was from the outside.</td>
</tr>
<tr>
<td>TCP segment partial overlap</td>
<td>A partially overlapping segment was detected.</td>
</tr>
<tr>
<td>TCP unexpected window size variation</td>
<td>A connection was terminated due to variation in the TCP window size.</td>
</tr>
<tr>
<td>Tunnel has been torn down</td>
<td>Flow was terminated because the tunnel is down.</td>
</tr>
<tr>
<td>Unauth Deny</td>
<td>An authorization was denied by a URL filter.</td>
</tr>
<tr>
<td>Unknown</td>
<td>An unknown error has occurred.</td>
</tr>
<tr>
<td>Xlate Clear</td>
<td>A command line was removed.</td>
</tr>
</tbody>
</table>

**Recommended Action** None required.

**Error Message** `@FTD-6-302015: Built {inbound|outbound} UDP connection number for interface_name :real_address /real_port (mapped_address /mapped_port) [{idfw_user }] to interface_name :real_address /real_port (mapped_address /mapped_port) [{idfw_user }] [{user }]`

**Explanation** A UDP connection slot between two hosts was created. The following list describes the message values:

- **number**—A unique identifier
Recommended Action  None required.
• **translated_address**—IP address after translation
• **translated_cid**—Translated call
• **user**—AAA user name
  • **idfw_user**—The name of the identity firewall user

**Recommended Action** None required.

---

**302019**

**Error Message** `%FTD-3-302019: H.323 library_name ASN Library failed to initialize, error code number`

**Explanation** The specified ASN library that the Firepower Threat Defense device uses for decoding the H.323 messages failed to initialize; the Firepower Threat Defense device cannot decode or inspect the arriving H.323 packet. The Firepower Threat Defense device allows the H.323 packet to pass through without any modification. When the next H.323 message arrives, the Firepower Threat Defense device tries to initialize the library again.

**Recommended Action** If this message is generated consistently for a particular library, contact the Cisco TAC and provide them with all log messages (preferably with timestamps).

---

**302020**

**Error Message** `%FTD-6-302020: Built {in | out} bound ICMP connection for faddr {faddr | icmp_seq_num} [{idfw_user}] gaddr {gaddr | icmp_type} laddr laddr [{idfw_user}] type {type} code {code}`

**Explanation** An ICMP session was established in the fast-path when stateful ICMP was enabled using the inspect icmp command. The following list describes the message values:
• **faddr** — Specifies the IP address of the foreign host
• **gaddr** — Specifies the IP address of the global host
• **laddr** — Specifies the IP address of the local host
• **idfw_user** — The name of the identity firewall user
• **user** — The username associated with the host from where the connection was initiated
• **type** — Specifies the ICMP type
• **code** — Specifies the ICMP code

**Recommended Action** None required.

### 302021

**Error Message** `%FTD-6-302021: Teardown ICMP connection for faddr {faddr | icmp_seq_num } [(idfw_user )] gaddr {gaddr | icmp_type } laddr laddr [(idfw_user )] type {type } code {code }

**Explanation** An ICMP session is removed in the fast-path when stateful ICMP is enabled using the inspect icmp command. The following list describes the message values:

• **faddr** — Specifies the IP address of the foreign host
• **gaddr** — Specifies the IP address of the global host
• **laddr** — Specifies the IP address of the local host
• **idfw_user** — The name of the identity firewall user
• **user** — The username associated with the host from where the connection was initiated
• **type** — Specifies the ICMP type
• **code** — Specifies the ICMP code

**Recommended Action** None required.

### 302022

**Error Message** `%FTD-6-302022: Built role stub TCP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port)

**Explanation** A TCP director/backup/forwarder flow has been created.

**Recommended Action** None required.

### 302023

**Error Message** `%FTD-6-302023: Teardown stub TCP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason

**Explanation** A TCP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.
**302024**

**Error Message** %FTD-6-302024: Built role stub UDP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port )

**Explanation** A UDP director/backup/forwarder flow has been created.

**Recommended Action** None required.

**302025**

**Error Message** %FTD-6-302025: Teardown stub UDP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes

**Explanation** A UDP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

**302026**

**Error Message** %FTD-6-302026: Built role stub ICMP connection for interface :real-address /real-port (mapped-address ) to interface :real-address /real-port (mapped-address )

**Explanation** An ICMP director/backup/forwarder flow has been created.

**Recommended Action** None required.

**302027**

**Error Message** %FTD-6-302027: Teardown stub ICMP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes

**Explanation** An ICMP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

**302033**

**Error Message** %FTD-6-302033: Pre-allocated H323 GUP Connection for faddr interface :foreign address /foreign-port to laddr interface :local-address /local-port

**Explanation** A GUP connection was started from the foreign address to the local address. The foreign port (outside port) only appears on connections from outside the security device. The local port value (inside port) only appears on connections started on an internal interface.

- **interface**—The interface name
- **foreign-address**—IP address of the foreign host
- **foreign-port**—Port number of the foreign host
- **local-address**—IP address of the local host
- **local-port**—Port number of the local host
Recommended Action None required.

302034

Error Message %FTD-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface:foreign address /foreign-port to laddr interface :local-address /local-port

Explanation The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

- interface—The interface name
- foreign-address —IP address of the foreign host
- foreign-port —Port number of the foreign host
- local-address —IP address of the local host
- local-port —Port number of the local host

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC. You can check the size of the global pool compared to the number of inside network clients. Alternatively, shorten the timeout interval of translations and connections. This message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory.

302302

Error Message %FTD-3-302302: ACL — deny; no sa created

Explanation IPsec proxy mismatches have occurred. Proxy hosts for the negotiated SA correspond to a deny access-list command policy.

Recommended Action Check the access-list command statement in the configuration. Contact the administrator for the peer.

302303

Error Message %FTD-6-302303: Built TCP state-bypass connection conn_id from initiator_interface :real_ip /real_port (mapped_ip /mapped_port ) to responder_interface :real_ip /real_port (mapped_ip /mapped_port )

Explanation A new TCP connection has been created, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.

Recommended Action If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the no set connection advanced-options tcp-state-bypass command to disable this feature for TCP traffic.

302304

Error Message %FTD-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface :ip/port to responder_interface :ip/port duration, bytes, teardown reason.

Explanation A new TCP connection has been torn down, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.
• **duration** — The duration of the TCP connection
• **bytes** — The total number of bytes transmitted over the TCP connection
• **teardown reason** — The reason for the teardown of the TCP connection

**Recommended Action** If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the **no set connection advanced-options tcp-state-bypass** command to disable this feature for TCP traffic.

### 302311

**Error Message** %FTD-4-302311: Failed to create a new protocol connection from **ingress interface**:source IP/source port to **egress interface**:destination IP/destination port due to application cache memory allocation failure. The app-cache memory threshold level is **threshold%** and threshold check is **enabled/disabled**.

**Explanation** A new connection could not be created due to app-cache memory allocation failure. The failure could be due to system running out of memory or exceeding app-cache memory threshold.

• **protocol** — The name of the protocol used to create the connection
• **ingress interface** — The interface name
• **source IP** — The source IP address
• **source port** — The source port number
• **egress interface** — The interface name
• **destination IP** — The destination address
• **destination port** — The destination port number
• **threshold%** — The percentage value of memory threshold
• **enabled/disabled** — app-cache memory threshold feature enabled/disabled

**Recommended Action** Disable memory intensive features on the device or reduce the number of through-the-box connections.

### 303002

**Error Message** %FTD-6-303002: FTP connection from **src_ifc** : **src_ip** / **src_port** to **dst_ifc** : **dst_ip** / **dst_port** , user **username** action **file** **filename**

**Explanation** A client has uploaded or downloaded a file from the FTP server.

• **src_ifc** — The interface where the client resides.
• **src_ip** — The IP address of the client.
• **src_port** — The client port.
• **dst_ifc** — The interface where the server resides.
• **dst_ip** — The IP address of the FTP server.
• **dst_port** — The server port.
• **username** — The FTP username.
• **action** — The stored or retrieved actions.
• **filename** — The file stored or retrieved.
Recommended Action: None required.

**303004**

**Error Message** %FTD-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface :source_address /source_port to dest_interface :dest_address/dest_interface

**Explanation** Strict FTP inspection on FTP traffic has been used, and an FTP request message contains a command that is not recognized by the device.

**Recommended Action** None required.

**303005**

**Error Message** %FTD-5-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc :sip /sport to dest_ifc :dip /dport

**Explanation** When FTP inspection matches any of the following configured values: filename, file type, request command, server, or username, then the action specified by the action_string in this message occurs.

- **match_string** — The match clause in the policy map
- **policy-name** — The policy map that matched
- **action_string** — The action to take; for example, Reset Connection
- **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

**Recommended Action** None required.

**305006**

**Error Message** %FTD-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user )] dst interface_name:dest_address/dest_port [(idfw_user )]

**Explanation** A protocol (UDP, TCP, or ICMP) failed to create a translation through the Firepower Threat Defense device. The Firepower Threat Defense device does not allow packets through that are destined for network or broadcast addresses. The Firepower Threat Defense device provides this checking for addresses that are explicitly identified with static commands. For inbound traffic, the Firepower Threat Defense device denies translations for an IP address identified as a network or broadcast address.

The Firepower Threat Defense device does not apply PAT to all ICMP message types; it only applies PAT ICMP echo and echo-reply packets (types 8 and 0). Specifically, only ICMP echo or echo-reply packets create a PAT translation. As a result, when the other ICMP messages types are dropped, this message is generated.

The Firepower Threat Defense device uses the global IP address and mask from configured static commands to differentiate regular IP addresses from network or broadcast IP addresses. If the global IP address is a valid
network address with a matching network mask, then the Firepower Threat Defense device does not create a translation for network or broadcast IP addresses with inbound packets.

For example:

```
static (inside, outside) 10.2.2.128 10.1.1.128 netmask 255.255.255.128
```

The Firepower Threat Defense device responds to global address 10.2.2.128 as a network address and to 10.2.2.255 as the broadcast address. Without an existing translation, the Firepower Threat Defense device denies inbound packets destined for 10.2.2.128 or 10.2.2.255, and logs this message.

When the suspected IP address is a host IP address, configure a separate static command with a host mask in front of the subnet static command (the first match rule for static commands). The following static commands cause the Firepower Threat Defense device to respond to 10.2.2.128 as a host address:

```
static (inside, outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.255
static (inside, outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.128
```

The translation may be created by traffic started from the inside host with the IP address in question. Because the Firepower Threat Defense device views a network or broadcast IP address as a host IP address with an overlapped subnet static configuration, the network address translation for both static commands must be the same.

**Recommended Action** None required.

### Error Message 305009

`%FTD-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user )] to interface_name :mapped_address`

**Explanation** An address translation slot was created. The slot translates the source address from the local side to the global side. In reverse, the slot translates the destination address from the global side to the local side.

**Recommended Action** None required.

### Error Message 305010

`%FTD-6-305010: Teardown {dynamic|static} translation from interface_name :real_address [(idfw_user )] to interface_name :mapped_address duration time`

**Explanation** The address translation slot was deleted.

**Recommended Action** None required.

### Error Message 305011

`%FTD-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name :real_address/real_port [(idfw_user )] to interface_name :mapped_address/mapped_port`

**Explanation** A TCP, UDP, or ICMP address translation slot was created. The slot translates the source socket from the local side to the global side. In reverse, the slot translates the destination socket from the global side to the local side.
**Recommended Action** None required.

**305012**

**Error Message** %FTD-6-305012: Teardown {dynamic/static} {TCP|UDP|ICMP} translation from interface_name [{(acl-name )}:real_address /{real_port |real_ICMP_ID } [{(idfw_user )}] to interface_name :mapped_address /{mapped_port |mapped_ICMP_ID } duration time

**Explanation** The address translation slot was deleted.

**Recommended Action** None required.

**305013**

**Error Message** %FTD-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name :source_address /source_port [{(idfw_user )}] dst interface_name :dst_address /dst_port [{(idfw_user )}] denied due to NAT reverse path failure.

**Explanation** An attempt to connect to a mapped host using its actual address was rejected.

**Recommended Action** When not on the same interface as the host using NAT, use the mapped address instead of the actual address to connect to the host. In addition, enable the `inspect` command if the application embeds the IP address.

**305014**

**Error Message** %FTD-6-305014: %d: Allocated %s block of ports for translation from %s:%B to %s:%B/%d-%d\n.

**Explanation** When CGNAT “block-allocation” is configured, this syslog will be generated on allocation of a new port block.

**Recommended Action** None.

**305016**

**Error Message** %FTD-3-305016: Unable to create protocol connection from real_interface :real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port due to reason .

**Explanation** The maximum port blocks per host limit has been reached for a host or the port blocks have been exhausted.

- `reason` — May be one of the following:
  - reaching per-host PAT port block limit of `value`
  - port block exhaustion in PAT pool

**Recommended Action** For reaching the per-host PAT port block limit, review the maximum blocks per host limit by entering the following command:

```
xlate block-allocation maximum-per-host 4
```
For the port block exhaustion in the PAT pool, we recommend increasing the pool size. Also, review the block size by entering the following command:

```
xlate block-allocation size 512
```

305017

**Error Message**  
%FTD-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from `<source device IP>` to `<destination device IP>`/<Active Port Block>

**Explanation** When CGNAT interim logging feature is turned on. This syslog specifies the Active Port Block from a particular source IP address to a destination IP address at that time.

**Recommended Action** None.

308001

**Error Message**  
%FTD-6-308001: console enable password incorrect for number tries (from `IP_address`)

**Explanation** This is a Firepower Threat Defense management message. This message appears after the specified number of times a user incorrectly types the password to enter privileged mode. The maximum is three attempts.

**Recommended Action** Verify the password and try again.

308002

**Error Message**  
%FTD-4-308002: static `global_address` inside_address netmask netmask overlapped with `global_address` inside_address

**Explanation** The IP addresses in one or more static command statements overlap. `global_address` is the global address, which is the address on the lower security interface, and `inside_address` is the local address, which is the address on the higher security-level interface.

**Recommended Action** Use the show static command to view the static command statements in your configuration and fix the commands that overlap. The most common overlap occurs if you specify a network address such as 10.1.1.0, and in another static command you specify a host within that range, such as 10.1.1.5.

311001

**Error Message**  
%FTD-6-311001: LU loading standby start

**Explanation** Stateful Failover update information was sent to the standby Firepower Threat Defense device when the standby Firepower Threat Defense device is first to be online.

**Recommended Action** None required.

311002

**Error Message**  
%FTD-6-311002: LU loading standby end
Explanation Stateful Failover update information stopped sending to the standby Firepower Threat Defense device.
Recommended Action None required.

311003

Error Message %FTD-6-311003: LU recv thread up
Explanation An update acknowledgment was received from the standby Firepower Threat Defense device.
Recommended Action None required.

311004

Error Message %FTD-6-311004: LU xmit thread up
Explanation A Stateful Failover update was transmitted to the standby Firepower Threat Defense device.
Recommended Action None required.

312001

Error Message %FTD-6-312001: RIP hdr failed from IP_address : cmd=string, version=number, domain=string on interface interface_name
Explanation The Firepower Threat Defense device received a RIP message with an operation code other than reply, the message has a version number different from what is expected on this interface, and the routing domain entry was nonzero. Another RIP device may not be configured correctly to communicate with the Firepower Threat Defense device.
Recommended Action None required.

313001

Error Message %FTD-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
Explanation When using the icmp command with an access list, if the first matched entry is a permit entry, the ICMP packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the Firepower Threat Defense device discards the ICMP packet and generates this message. The icmp command enables or disables pinging to an interface. With pinging disabled, the Firepower Threat Defense device cannot be detected on the network. This feature is also referred to as configurable proxy pinging.
Recommended Action Contact the administrator of the peer device.

313004

Error Message %FTD-4-313004: Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address: no matching session
Explanation ICMP packets were dropped by the Firepower Threat Defense device because of security checks added by the stateful ICMP feature that are usually either ICMP echo replies without a valid echo request.
already passed across the Firepower Threat Defense device or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the Firepower Threat Defense device.

Recommended Action None required.

313005

Error Message %FTD-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface interface_name. Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name :src_address [(idfw_user | FQDN_string), sg_info ]) dst dest_interface_name :dest_address [(idfw_user | FQDN_string), sg_info ]) (type icmp_type, code icmp_code ) embedded_frame_info = prot src source_address /source_port [(idfw_user | FQDN_string), sg_info ]) dst dest_address /dest_port [(idfw_user | FQDN_string), sg_info ]

Explanation ICMP error packets were dropped by the Firepower Threat Defense device because the ICMP error messages are not related to any session already established in the Firepower Threat Defense device.

Recommended Action If the cause is an attack, you can deny the host by using ACLs.

313008

Error Message %FTD-3-313008: Denied ICMPv6 type=number, code=code from IP_address on interface interface_name

Explanation When using the icmp command with an access list, if the first matched entry is a permit entry, the ICMPv6 packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the Firepower Threat Defense device discards the ICMPv6 packet and generates this message.

The icmp command enables or disables pinging to an interface. When pinging is disabled, the Firepower Threat Defense device is undetectable on the network. This feature is also referred to as “configurable proxy pinging.”

Recommended Action Contact the administrator of the peer device.

313009

Error Message %FTD-4-313009: Denied invalid ICMP code icmp-code, for src-ifc :src-address /src-port (mapped-src-address/mapped-src-port) to dest-ifc :dest-address /dest-port (mapped-dest-address/mapped-dest-port) [user ], ICMP id icmp-id , ICMP type icmp-type

Explanation An ICMP echo request/reply packet was received with a malformed code(non-zero).

Recommended Action If it is an intermittent event, no action is required. If the cause is an attack, you can deny the host using the ACLs.

314001

Error Message %FTD-6-314001: Pre-allocated RTSP UDP backconnection for src_intf :src_IP to dst_intf :dst_IP /dst_port.

Explanation The Firepower Threat Defense device opened a UDP media channel for the RTSP client that was receiving data from the server.
314002

**Error Message** %FTD-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP /dst_port : reason_string.

**Explanation** The Firepower Threat Defense device cannot open a new pinhole for the media channel.

- `src_intf` — Source interface name
- `src_IP` — Source interface IP address
- `dst_intf` — Destination interface name
- `dst_IP` — Destination IP address
- `dst_port` — Destination port
- `reason_string` — Pinhole already exists/Unknown

**Recommended Action** If the reason is unknown, check the free memory available by running the `show memory` command, or the number of connections used by running the `show conn` command, because the Firepower Threat Defense device is low on memory.

316001

**Error Message** %FTD-3-316001: Denied new tunnel to IP_address. VPN peer limit (platform_vpn_peer_limit) exceeded

**Explanation** If more VPN tunnels (ISAKMP/IPsec) are concurrently trying to be established than are supported by the platform VPN peer limit, then the excess tunnels are aborted.

**Recommended Action** None required.

316002

**Error Message** %FTD-3-316002: VPN Handle error: protocol=protocol , src in if_num :src_addr , dst out if_num :dst_addr

**Explanation** The Firepower Threat Defense device cannot create a VPN handle, because the VPN handle already exists.

- `protocol` — The protocol of the VPN flow
- `in_if_num` — The ingress interface number of the VPN flow
- `src_addr` — The source IP address of the VPN flow
- `out_if_num` — The egress interface number of the VPN flow
- `dst_addr` — The destination IP address of the VPN flow

**Recommended Action** This message may occur during normal operation; however, if the message occurs repeatedly and a major malfunction of VPN-based applications occurs, a software defect may be the cause.
Enter the following commands to collect more information and contact the Cisco TAC to investigate the issue further:

```
capture
  name
  type asp-drop vpn-handle-error
show asp table classify crypto detail
show asp table vpn-context
```

### 317001
**Error Message** %FTD-3-317001: No memory available for limit_slow
**Explanation** The requested operation failed because of a low-memory condition.
**Recommended Action** Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

### 317002
**Error Message** %FTD-3-317002: Bad path index of number for IP_address , number max
**Explanation** A software error occurred.
**Recommended Action** If the problem persists, contact the Cisco TAC.

### 317003
**Error Message** %FTD-3-317003: IP routing table creation failure - reason
**Explanation** An internal software error occurred, which prevented the creation of a new IP routing table.
**Recommended Action** Copy the message exactly as it appears, and report it to Cisco TAC.

### 317004
**Error Message** %FTD-3-317004: IP routing table limit warning
**Explanation** The number of routes in the named IP routing table has reached the configured warning limit.
**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

### 317005
**Error Message** %FTD-3-317005: IP routing table limit exceeded - reason , IP_address netmask
**Explanation** Additional routes will be added to the table.
**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

### 317006
**Error Message** %FTD-3-317006: Pdb index error pdb , pdb_index , pdb_type
Explanation The index into the PDB is out of range.

- **pdb**—Protocol Descriptor Block, the descriptor of the PDB index error
- **pdb_index**—The PDB index identifier
- **pdb_type**—The type of the PDB index error

**Recommended Action** If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC, and provide the representative with the collected information.

317007

**Error Message** %FTD-6-317007: Added route_type route dest_address netmask via gateway_address [distance /metric ] on interface_name route_type

**Explanation** A new route has been added to the routing table.

Routing protocol type:

- B – BGP, D – EIGRP, EX - EIGRP external, O - OSPF
- IA - OSPF inter area, N1 - OSPF NSSA external type 1
- N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
- E2 - OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS level-1
- L2 - IS-IS level-2, ia - IS-IS inter area

- **dest_address** —The destination network for this route
- **netmask** —The netmask for the destination network
- **gateway_address** —The address of the gateway by which the destination network is reached
- **distance** —Administrative distance for this route
- **metric** —Metric for this route
- **interface_name** —Network interface name through which the traffic is routed

**Recommended Action** None required.

317008

**Error Message** %FTD-6-317008: Deleted route_type route dest_address netmask via gateway_address [distance /metric ] on interface_name route_type

**Explanation** A new route has been deleted from the routing table.

Routing protocol type:

- B – BGP, D – EIGRP, EX - EIGRP external, O - OSPF
- IA - OSPF inter area, N1 - OSPF NSSA external type 1
- N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
- E2 - OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS level-1
- L2 - IS-IS level-2, ia - IS-IS inter area
- **dest_address** — The destination network for this route
- **netmask** — The netmask for the destination network
- **gateway_address** — The address of the gateway by which the destination network is reached
- **distance** — Administrative distance for this route
- **metric** — Metric for this route
- **interface_name** — Network interface name through which the traffic is routed

**Recommended Action** None required.

---

### 317012

**Error Message** %FTD-3-317012: Interface IP route counter negative = nameif-string-value

**Explanation** Indicates that the interface route count is negative.
- **nameif-string-value** — The interface name as specified by the nameif command

**Recommended Action** None required.

---

### 318001

**Error Message** %FTD-3-318001: Internal error: reason

**Explanation** An internal software error occurred. This message occurs at five-second intervals.

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

---

### 318002

**Error Message** %FTD-3-318002: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an area border router without a backbone area configured in the router. This message occurs at five-second intervals.

**Recommended Action** Restart the OSPF process.

---

### 318003

**Error Message** %FTD-3-318003: Reached unknown state in neighbor state machine

**Explanation** An internal software error occurred. This message occurs at five-second intervals.

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

---

### 318004

**Error Message** %FTD-3-318004: area string lsid IP_address mask netmask adv IP_address type number

**Explanation** The OSPF process had a problem locating the link state advertisement, which might lead to a memory leak.

**Recommended Action** If the problem persists, contact the Cisco TAC.
318005

**Error Message**  %FTD-3-318005: lsid ip_address adv IP_address type number gateway gateway_address metric number network IP_address mask netmask protocol hex attr hex net-metric number

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

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

318006

**Error Message**  %FTD-3-318006: if interface_name if_state number

**Explanation** An internal error occurred.

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

318007

**Error Message**  %FTD-3-318007: OSPF is enabled on interface_name during idb initialization

**Explanation** An internal error occurred.

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

318008

**Error Message**  %FTD-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** The OSPF process is being reset, and it is going to select a new router ID. This action will bring down all virtual links.

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

318009

**Error Message**  %FTD-3-318009: OSPF: Attempted reference of stale data encountered in function , line: line_num

**Explanation** OSPF is running and has tried to reference some related data structures that have been removed elsewhere. Clearing interface and router configurations may resolve the problem. However, if this message appears, some sequence of steps caused premature deletion of data structures and this needs to be investigated.

- **function** — The function that received the unexpected event
- **line_num** — Line number in the code

**Recommended Action** If the problem persists, contact the Cisco TAC.
318101

**Error Message**  %FTD-3-318101: Internal error: REASON

**Explanation** An internal software error has occurred.
- *REASON* — The detailed cause of the event

**Recommended Action** None required.

318102

**Error Message**  %FTD-3-318102: 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.

318103

**Error Message**  %FTD-3-318103: Reached unknown state in neighbor state machine

**Explanation** An internal software error has occurred.

**Recommended Action** None required.

318104

**Error Message**  %FTD-3-318104: DB already exist: area AREA_ID_STR lsid i adv i type 0x x

**Explanation** OSPF has a problem locating the LSA, which could lead to a memory leak.
- *AREA_ID_STR* — A string representing the area
- *i* — An integer value
- *x* — A hexadecimal representation of an integer value

**Recommended Action** None required.

318105

**Error Message**  %FTD-3-318105: lsid i adv i type 0x x gateway i metric d network i mask i protocol #x attr #x net-metric d

**Explanation** OSPF found an inconsistency between its database and the IP routing table.
- *i* — An integer value
- *x* — A hexadecimal representation of an integer value
- *d* — A number

**Recommended Action** None required.

318106

**Error Message**  %FTD-3-318106: if IF_NAME if_state d
Explanation An internal error has occurred.

- **IF_NAME** — The name of the affected interface
- **d** — A number

**Recommended Action** None required.

### 318107

**Error Message** %FTD-3-318107: OSPF is enabled on **IF_NAME** during idb initialization

**Explanation** An internal error has occurred.

- **IF_NAME** — The name of the affected interface

**Recommended Action** None required.

### 318108

**Error Message** %FTD-3-318108: OSPF process **d** is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** The OSPF process is being reset, and it is going to select a new router ID, which brings down all virtual links. To make them work again, you need to change the virtual link configuration on all virtual link neighbors.

- **d** — A number representing the process ID

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

### 318109

**Error Message** %FTD-3-318109: OSPFv3 has received an unexpected message: 0x/0x

**Explanation** OSPFv3 has received an unexpected interprocess message.

- **x** — A hexadecimal representation of an integer value

**Recommended Action** None required.

### 318110

**Error Message** %FTD-3-318110: Invalid encrypted key **s**.

**Explanation** The specified encrypted key is not valid.

- **s** — A string representing the encrypted key

**Recommended Action** Either specify a clear text key and enter the `service password-encryption` command for encryption, or ensure that the specified encrypted key is valid. If the specified encrypted key is not valid, an error message appears during system configuration.
318111

**Error Message**  
%FTD-3-318111: SPI \(u\) is already in use with ospf process \(d\).

**Explanation** An attempt was made to use a SPI that has already been used.
- \(u\) — A number representing the SPI
- \(d\) — A number representing the process ID

**Recommended Action** Choose a different SPI.

318112

**Error Message**  
%FTD-3-318112: SPI \(u\) is already in use by a process other than ospf process \(d\).

**Explanation** An attempt was made to use a SPI that has already been used.
- \(u\) — A number representing the SPI
- \(d\) — A number representing the process ID

**Recommended Action** Choose a different SPI. Enter the `show crypto ipv6 ipsec sa` command to view a list of SPIs that are already being used.

318113

**Error Message**  
%FTD-3-318113: \(s\) is already configured with SPI \(u\).

**Explanation** An attempt was made to use a SPI that has already been used.
- \(s\) — A string representing an interface
- \(u\) — A number representing the SPI

**Recommended Action** Unconfigure the SPI first, or choose a different one.

318114

**Error Message**  
%FTD-3-318114: The key length used with SPI \(u\) is not valid.

**Explanation** The key length was incorrect.
- \(u\) — A number representing the SPI

**Recommended Action** Choose a valid IPsec key. An IPsec authentication key must be 32 (MD5) or 40 (SHA-1) hexadecimal digits long.

318115

**Error Message**  
%FTD-3-318115: \(s\) error occurred when attempting to create an IPsec policy for SPI \(u\).

**Explanation** An IPsec API (internal) error has occurred.
- \(s\) — A string representing the error
- \(u\) — A number representing the SPI
Recommended Action: None required.

**318116**

**Error Message:** %FTD-3-318116: SPI \( u \) is not being used by ospf process \( d \).

**Explanation:** An attempt was made to unconfigure a SPI that is not being used with OSPFv3.

- \( u \) — A number representing the SPI
- \( d \) — A number representing the process ID

**Recommended Action:** Enter a `show` command to see which SPIs are used by OSPFv3.

**318117**

**Error Message:** %FTD-3-318117: The policy for SPI \( u \) could not be removed because it is in use.

**Explanation:** An attempt was made to remove the policy for the indicated SPI, but the policy was still being used by a secure socket.

- \( u \) — A number representing the SPI

**Recommended Action:** None required.

**318118**

**Error Message:** %FTD-3-318118: s error occurred when attempting to remove the IPsec policy with SPI \( u \)

**Explanation:** An IPsec API (internal) error has occurred.

- \( s \) — A string representing the specified error
- \( u \) — A number representing the SPI

**Recommended Action:** None required.

**318119**

**Error Message:** %FTD-3-318119: Unable to close secure socket with SPI \( u \) on interface \( s \)

**Explanation:** An IPsec API (internal) error has occurred.

- \( u \) — A number representing the SPI
- \( s \) — A string representing the specified interface

**Recommended Action:** None required.

**318120**

**Error Message:** %FTD-3-318120: OSPFv3 was unable to register with IPsec

**Explanation:** An internal error has occurred.

**Recommended Action:** None required.
318121

**Error Message** %FTD-3-318121: IPsec reported a GENERAL ERROR: message \( s \), count \( d \)

**Explanation** An internal error has occurred.
- \( s \) — A string representing the specified message
- \( d \) — A number representing the total number of generated messages

**Recommended Action** None required.

318122

**Error Message** %FTD-3-318122: IPsec sent a \( s \) message \( s \) to OSPFv3 for interface \( s \). Recovery attempt \( d \)

**Explanation** An internal error has occurred. The system is trying to reopen the secure socket and to recover.
- \( s \) — A string representing the specified message and specified interface
- \( d \) — A number representing the total number of recovery attempts

**Recommended Action** None required.

318123

**Error Message** %FTD-3-318123: IPsec sent a \( s \) message \( s \) to OSPFv3 for interface \( IF\_NAME \).

**Explanation** An internal error has occurred. The maximum number of recovery attempts has been exceeded.
- \( s \) — A string representing the specified message
- \( IF\_NAME \) — The specified interface

**Recommended Action** None required.

318125

**Error Message** %FTD-3-318125: Init failed for interface \( IF\_NAME \)

**Explanation** The interface initialization failed. Possible reasons include the following:
- The area to which the interface is being attached is being deleted.
- It was not possible to create the link scope database.
- It was not possible to create a neighbor datablock for the local router.

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

318126

**Error Message** %FTD-3-318126: Interface \( IF\_NAME \) 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.
- \( IF\_NAME \) — The specified interface
**Recommended Action** None required.

### 318127

**Error Message** %FTD-3-318127: Could not allocate or find the neighbor

**Explanation** An internal error has occurred.

**Recommended Action** None required.

### Messages 320001 to 341011

This chapter includes messages from 320001 to 341011.

#### 320001

**Error Message** %FTD-3-320001: The subject name of the peer cert is not allowed for connection

**Explanation** When the Firepower Threat Defense device is an easy VPN remote device or server, the peer certificate includes a subject name that does not match the output of the `ca verifycertdn` command. A man-in-the-middle attack might be occurring, where a device spoofs the peer IP address and tries to intercept a VPN connection from the Firepower Threat Defense device.

**Recommended Action** None required.

#### 321001

**Error Message** %FTD-5-321001: Resource `var1` limit of `var2` reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** None required.

#### 321002

**Error Message** %FTD-5-321002: Resource `var1` rate limit of `var2` reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** None required.

#### 321003

**Error Message** %FTD-6-321003: Resource `var1` log level of `var2` reached.

**Explanation** A configured resource usage or rate logging level for the indicated resource was reached.

**Recommended Action** None required.
321004

Error Message  %FTD-6-321004: Resource var1 rate log level of var2 reached
Explanation A configured resource usage or rate logging level for the indicated resource was reached.
Recommended Action None required.

321005

Error Message  %FTD-2-321005: System CPU utilization reached utilization %
Explanation The system CPU utilization has reached 95 percent or more and remains at this level for five minutes.
  • utilization % — The percentage of CPU being used
Recommended Action If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the show cpu command and verify the CPU usage. If it is high, contact the Cisco TAC.

321006

Error Message  %FTD-2-321006: System memory usage reached utilization %
Explanation The system memory usage has reached 80 percent or more and remains at this level for five minutes.
  • utilization % — The percentage of memory being used
Recommended Action If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the show memory command and verify the memory usage. If it is high, contact the Cisco TAC.

321007

Error Message  %FTD-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)
Explanation The system is low on free blocks of memory. Running out of blocks may result in traffic disruption.
  • block_size — The block size of memory (for example, 4, 1550, 8192)
  • free_blocks — The number of free blocks, as shown in the CNT column after using the show blocks command
  • max_blocks — The maximum number of blocks that the system can allocate, as shown in the MAX column after using the show blocks command
Recommended Action Use the show blocks command to monitor the amount of free blocks in the CNT column of the output for the indicated block size. If the CNT column remains zero, or very close to it for an extended period of time, then the Firepower Threat Defense device may be overloaded or running into another issue that needs additional investigation.
322001

**Error Message** %FTD-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface

**Explanation** The Firepower Threat Defense device received a packet from the offending MAC address on the specified interface, but the source MAC address in the packet is statically bound to another interface in the configuration. Either a MAC-spoofing attack or a misconfiguration may be the cause.

**Recommended Action** Check the configuration and take appropriate action by either finding the offending host or correcting the configuration.

322002

**Error Message** %FTD-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is {statically|dynamically} bound to MAC Address MAC_address_2.

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets across the Firepower Threat Defense device. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

322003

**Error Message** %FTD-3-322003: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is not bound to any MAC Address.

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured IP-MAC address binding before forwarding ARP packets across the Firepower Threat Defense device. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

322004

**Error Message** %FTD-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface_in :source_address /source_port to interface_out :dest_address /dest_port

**Explanation** The Firepower Threat Defense device dropped a packet because no management IP address was configured in the transparent mode.

- **protocol**—Protocol string or value
• **interface_in**—Input interface name
• **source_address**—Source IP address of the packet
• **source_port**—Source port of the packet
• **interface_out**—Output interface name
• **dest_address**—Destination IP address of the packet
• **dest_port**—Destination port of the packet

**Recommended Action** Configure the device with the management IP address and mask values.

### 323001

**Error Message**  
%FTD-3-323001: Module `module_id` experienced a control channel communications failure.  
%FTD-3-323001: Module in slot `slot_num` experienced a control channel communications failure.

**Explanation** The Firepower Threat Defense device is unable to communicate via control channel with the module installed (in the specified slot).
- **module_id**—For a software services module, specifies the services module name.
- **slot_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

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

### 323002

**Error Message**  
%FTD-3-323002: Module `module_id` is not able to shut down, shut down request not answered.  
%FTD-3-323002: Module in slot `slot_num` is not able to shut down, shut down request not answered.

**Explanation** The module installed did not respond to a shutdown request.
- **module_id**—For a software services module, specifies the service module name.
- **slot_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

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

### 323003

**Error Message**  
%FTD-3-323003: Module `module_id` is not able to reload, reload request not answered.  
%FTD-3-323003: Module in slot `slot_num` is not able to reload, reload request not answered.

**Explanation** The module installed did not respond to a reload request.
- **module_id**—For a software services module, specifies the service module name.
- **slot_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
Recommended Action If the problem persists, contact the Cisco TAC.

323004

Error Message %FTD-3-323004: Module string one failed to write software newver (currently ver ), reason . Hw-module reset is required before further use.

Explanation The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. The module is not usable until the software is updated.

- string one—The text string that specifies the module
- >newver —The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- >ver —The current version number of the software on the module (for example, 1.0(1)0)
- >reason —The reason the new version cannot be written to the module. The possible values for >reason include the following:
  - write failure
  - failed to create a thread to write the image

Recommended Action If the module software cannot be updated, it will not be usable. If the problem persists, contact the Cisco TAC.

323005

Error Message %FTD-3-323005: Module module_id can not be started completely
%FTD-3-323005: Module in slot slot_num cannot be started completely

Explanation This message indicates that the module cannot be started completely. The module will remain in the UNRESPONSIVE state until this condition is corrected. A module that is not fully seated in the slot is the most likely cause.

- module_id—For a software services module, specifies the service module name.
- slot_num—For a hardware services module, specifies the slot number that contains the module.

Recommended Action Verify that the module is fully seated and check to see if any status LEDs on the module are on. It may take a minute after fully reseating the module for the Firepower Threat Defense device to recognize that it is powered up. If this message appears after verifying that the module is seated and after resetting the module using either the sw-module module service-module-name reset command or the hw-module module slotnum reset command, contact the Cisco TAC.

323006

Error Message %FTD-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.

Explanation A data channel communication failure occurred and the Firepower Threat Defense device was unable to forward traffic to the services module. This failure triggers a failover when the failure occurs on the active Firepower Threat Defense device in an HA configuration. The failure also results in the configured fail open or fail closed policy being enforced on traffic that would normally be sent to the services module. This message is generated whenever a communication problem over the Firepower Threat Defense device dataplane
occurs between the system module and the services module, which can be caused when the services module stops, resets, is removed or disabled.

**Recommended Action** For software services modules such as IPS, recover the module using the `sw-module module ips recover` command. For hardware services modules, if this message is not the result of the SSM reloading or resetting and the corresponding syslog message 505010 is not seen after the SSM returns to an UP state, reset the module using the `hw-module module 1 reset` command.

### 323007

**Error Message** `%FTD-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.`

**Explanation** An Firepower Threat Defense device with a 4GE-SSM installed experienced a short power surge, then rebooted. As a result, the 4GE-SSM may come online in an unresponsive state. The Firepower Threat Defense device has detected that the 4GE-SSM is unresponsive, and automatically restarts the 4GE-SSM.

**Recommended Action** None required.

### 325001

**Error Message** `%FTD-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings`  

**Explanation** Another router on the link sent router advertisements with conflicting parameters.

- `ipv6_address`—IPv6 address of the other router
- `interface`—Interface name of the link with the other router

**Recommended Action** Verify that all IPv6 routers on the link have the same parameters in the router advertisement for `hop_limit, managed_config_flag, other_config_flag, reachable_time` and `ns_interval`, and that preferred and valid lifetimes for the same prefix, advertised by several routers, are the same. To list the parameters per interface, enter the `show ipv6 interface` command.

### 325002

**Error Message** `%FTD-4-325002: Duplicate address ipv6_address/MAC_address on interface`  

**Explanation** Another system is using your IPv6 address.

- `ipv6_address`—The IPv6 address of the other router
- `MAC_address`—The MAC address of the other system, if known; otherwise, it is considered unknown.
- `interface`—The interface name of the link with the other system

**Recommended Action** Change the IPv6 address of one of the two systems.

### 326001

**Error Message** `%FTD-3-326001: Unexpected error in the timer library: error_message`  

**Explanation** A managed timer event was received without a context or a correct type, or no handler exists. Alternatively, if the number of events queued exceeds a system limit, an attempt to process them will occur at a later time.
Recommended Action If the problem persists, contact the Cisco TAC.

326002

Error Message %FTD-3-326002: Error in error_message : error_message
Explanation The IGMP process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.
Recommended Action If the problem persists, contact the Cisco TAC.

326004

Error Message %FTD-3-326004: An internal error occurred while processing a packet queue
Explanation The IGMP packet queue received a signal without a packet.
Recommended Action If the problem persists, contact the Cisco TAC.

326005

Error Message %FTD-3-326005: Mrib notification failed for (IP_address, IP_address )
Explanation A packet triggering a data-driven event was received, and the attempt to notify the MRIB failed.
Recommended Action If the problem persists, contact the Cisco TAC.

326006

Error Message %FTD-3-326006: Entry-creation failed for (IP_address, IP_address )
Explanation The MFIB received an entry update from the MRIB, but failed to create the entry related to the addresses displayed. The probable cause is insufficient memory.
Recommended Action If the problem persists, contact the Cisco TAC.

326007

Error Message %FTD-3-326007: Entry-update failed for (IP_address, IP_address )
Explanation The MFIB received an interface update from the MRIB, but failed to create the interface related to the addresses displayed. The probable cause is insufficient memory.
Recommended Action If the problem persists, contact the Cisco TAC.

326008

Error Message %FTD-3-326008: MRIB registration failed
Explanation The MFIB failed to register with the MRIB.
Recommended Action If the problem persists, contact the Cisco TAC.
326009

**Error Message** %FTD-3-326009: MRIB connection-open failed

**Explanation** The MFIB failed to open a connection to the MRIB.

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

326010

**Error Message** %FTD-3-326010: MRIB unbind failed

**Explanation** The MFIB failed to unbind from the MRIB.

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

326011

**Error Message** %FTD-3-326011: MRIB table deletion failed

**Explanation** The MFIB failed to retrieve the table that was supposed to be deleted.

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

326012

**Error Message** %FTD-3-326012: Initialization of string functionality failed

**Explanation** The initialization of a specified functionality failed. This component might still operate without the functionality.

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

326013

**Error Message** %FTD-3-326013: Internal error: string in string line %d (%s )

**Explanation** A fundamental error occurred in the MRIB.

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

326014

**Error Message** %FTD-3-326014: Initialization failed: error_message error_message

**Explanation** The MRIB failed to initialize.

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

326015

**Error Message** %FTD-3-326015: Communication error: error_message error_message

**Explanation** The MRIB received a malformed update.
Recommended Action: If the problem persists, contact the Cisco TAC.

326016

Error Message: %FTD-3-326016: Failed to set un-numbered interface for interface_name (string)
Explanation: The PIM tunnel is not usable without a source address. This situation occurs because a numbered interface cannot be found, or because of an internal error.
Recommended Action: If the problem persists, contact the Cisco TAC.

326017

Error Message: %FTD-3-326017: Interface Manager error - string in string : string
Explanation: An error occurred while creating a PIM tunnel interface.
Recommended Action: If the problem persists, contact the Cisco TAC.

326019

Error Message: %FTD-3-326019: string in string : string
Explanation: An error occurred while creating a PIM RP tunnel interface.
Recommended Action: If the problem persists, contact the Cisco TAC.

326020

Error Message: %FTD-3-326020: List error in string : string
Explanation: An error occurred while processing a PIM interface list.
Recommended Action: If the problem persists, contact the Cisco TAC.

326021

Error Message: %FTD-3-326021: Error in string : string
Explanation: An error occurred while setting the SRC of a PIM tunnel interface.
Recommended Action: If the problem persists, contact the Cisco TAC.

326022

Error Message: %FTD-3-326022: Error in string : string
Explanation: The PIM process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.
Recommended Action: If the problem persists, contact the Cisco TAC.
326023

**Error Message** %FTD-3-326023: string - IP_address : string

**Explanation** An error occurred while processing a PIM group range.

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

326024

**Error Message** %FTD-3-326024: An internal error occurred while processing a packet queue.

**Explanation** The PIM packet queue received a signal without a packet.

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

326025

**Error Message** %FTD-3-326025: string

**Explanation** An internal error occurred while trying to send a message. Events scheduled to occur on the receipt of a message, such as deletion of the PIM tunnel IDB, may not occur.

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

326026

**Error Message** %FTD-3-326026: Server unexpected error: error_message

**Explanation** The MRIB failed to register a client.

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

326027

**Error Message** %FTD-3-326027: Corrupted update: error_message

**Explanation** The MRIB received a corrupt update.

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

326028

**Error Message** %FTD-3-326028: Asynchronous error: error_message

**Explanation** An unhandled asynchronous error occurred in the MRIB API.

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

327001

**Error Message** %FTD-3-327001: IP SLA Monitor: Cannot create a new process

**Explanation** The IP SLA monitor was unable to start a new process.
Recommended Action Check the system memory. If memory is low, then this is probably the cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

327002

Error Message %FTD-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work

Explanation The IP SLA monitor failed to initialize. This condition is caused by either the timer wheel function failing to initialize or a process not being created. Sufficient memory is probably not available to complete the task.

Recommended Action Check the system memory. If memory is low, then this is probably the cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

327003

Error Message %FTD-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize

Explanation The IP SLA monitor cannot initialize the timer wheel.

Recommended Action Check the system memory. If memory is low, then the timer wheel function did not initialize. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

328001

Error Message %FTD-3-328001: Attempt made to overwrite a set stub function in string.

Explanation A single function can be set as a callback for when a stub with a check registry is invoked. An attempt to set a new callback failed because a callback function has already been set.

• string — The name of the function

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

328002

Error Message %FTD-3-328002: Attempt made in string to register with out of bounds key

Explanation In the FASTCASE registry, the key has to be smaller than the size specified when the registry was created. An attempt was made to register with a key out-of-bounds.

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

329001

Error Message %FTD-3-329001: The string0 subblock named string1 was not removed

Explanation A software error has occurred. IDB subblocks cannot be removed.

• string0 — SWIDB or HWIDB
• string1 — The name of the subblock
**331001**

**Error Message**  
%FTD-3-331001: Dynamic DNS Update for 'fqdn_name' = ip_address failed

**Explanation**  
The dynamic DNS subsystem failed to update the resource records on the DNS server. This failure might occur if the Firepower Threat Defense device is unable to contact the DNS server or the DNS service is not running on the destination system.

- *fqdn_name* — The fully qualified domain name for which the DNS update was attempted
- *ip_address* — The IP address of the DNS update

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

---

**331002**

**Error Message**  
%FTD-5-331002: Dynamic DNS type RR for ('fqdn_name' = ip_address | ip_address = 'fqdn_name') successfully updated in DNS server dns_server_ip

**Explanation**  
A dynamic DNS update succeeded in the DNS server.

- *type* — The type of resource record, which may be A or PTR
- *fqdn_name* — The fully qualified domain name for which the DNS update was attempted
- *ip_address* — The IP address of the DNS update
- *dns_server_ip* — The IP address of the DNS server

**Recommended Action**  
Nonerequired.

---

**332001**

**Error Message**  
%FTD-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.

**Explanation**  
An internal error that indicates the WCCP process was unable to open the UDP socket used to listen for protocol messages from caches.

**Recommended Action**  
Ensure that the IP configuration is correct and that at least one IP address has been configured.

---

**332002**

**Error Message**  
%FTD-3-332002: Unable to allocate message buffer, WCCP V2 closing down.

**Explanation**  
An internal error that indicates the WCCP process was unable to allocate memory to hold incoming protocol messages.

**Recommended Action**  
Ensure that enough memory is available for all processes.

---

**332003**

**Error Message**  
%FTD-5-332003: Web Cache IP_address/service_ID acquired
Explanation A service from the web cache of the Firepower Threat Defense device was acquired.

- **IP_address**—The IP address of the web cache
- **service_ID**—The WCCP service identifier

**Recommended Action** None required.

**332004**

**Error Message** %FTD-1-332004: Web Cache IP_address /service_ID lost

**Explanation** A service from the web cache of the Firepower Threat Defense device was lost.

- **IP_address**—The IP address of the web cache
- **service_ID**—The WCCP service identifier

**Recommended Action** Verify operation of the specified web cache.

**333001**

**Error Message** %FTD-6-333001: EAP association initiated - context: EAP-context

**Explanation** An EAP association has been initiated with a remote host.

- **EAP-context**—A unique identifier for the EAP session, displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

**333002**

**Error Message** %FTD-5-333002: Timeout waiting for EAP response - context:EAP-context

**Explanation** A timeout occurred while waiting for an EAP response.

- **EAP-context**—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

**333003**

**Error Message** %FTD-6-333003: EAP association terminated - context:EAP-context

**Explanation** The EAP association has been terminated with the remote host.

- **EAP-context**—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

**333004**

**Error Message** %FTD-7-333004: EAP-SQ response invalid - context:EAP-context
**Explanation** The EAP-Status Query response failed basic packet validation.

- **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

---

**333005**

**Error Message** %FTD-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context

**Explanation** The EAP-Status Query response has one or more invalid TLVs.

- **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

---

**333006**

**Error Message** %FTD-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context

**Explanation** The EAP-Status Query response is missing one or more mandatory TLVs.

- **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

---

**333007**

**Error Message** %FTD-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context

**Explanation** The EAP-Status Query response includes a TLV with an invalid length.

- **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

---

**333008**

**Error Message** %FTD-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context

**Explanation** The EAP-Status Query response includes an invalid nonce TLV.

- **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

---

**333009**

**Error Message** %FTD-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context

**Explanation** The EAP-Status Query response includes a MAC that does not match the calculated MAC.
• **EAP-context** — A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

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

### 333010

**Error Message** %FTD-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context

**Explanation** The EAP-Status Query response includes a validation flags TLV, which indicates that the peer requested a full posture validation.

**Recommended Action** None required.

### 334001

**Error Message** %FTD-6-334001: EAPoUDP association initiated - host-address

**Explanation** An EAPoUDP association has been initiated with a remote host.

• **host-address** — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

### 334002

**Error Message** %FTD-5-334002: EAPoUDP association successfully established - host-address

**Explanation** An EAPoUDP association has been successfully established with the host.

• **host-address** — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

### 334003

**Error Message** %FTD-5-334003: EAPoUDP association failed to establish - host-address

**Explanation** An EAPoUDP association has failed to establish with the host.

• **host-address** — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** Verify the configuration of the Cisco Secure Access Control Server.

### 334004

**Error Message** %FTD-6-334004: Authentication request for NAC Clientless host - host-address

**Explanation** An authentication request was made for a NAC clientless host.

• **host-address** — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.
334005

**Error Message**  %FTD-5-334005: Host put into NAC Hold state - *host-address*

**Explanation**  The NAC session for the host was put into the Hold state.

- *host-address* — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action**  None required.

334006

**Error Message**  %FTD-5-334006: EAPoUDP failed to get a response from host - *host-address*

**Explanation**  An EAPoUDP response was not received from the host.

- *host-address* — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action**  None required.

334007

**Error Message**  %FTD-6-334007: EAPoUDP association terminated - *host-address*

**Explanation**  An EAPoUDP association has terminated with the host.

- *host-address* — The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action**  None required.

334008

**Error Message**  %FTD-6-334008: NAC EAP association initiated - *host-address* , EAP context: *EAP-context*

**Explanation**  EAPoUDP has initiated EAP with the host.

- *host-address* — The IP address of the host in dotted decimal format (for example, 10.86.7.101)
- *EAP-context* — A unique identifier for the EAP session displayed as an eight-digit, hexadecimal number (for example, 0x2D890AE0)

**Recommended Action**  None required.

334009

**Error Message**  %FTD-6-334009: Audit request for NAC Clientless host - *Assigned_IP.*

**Explanation**  An audit request is being sent for the specified assigned IP address.

- *Assigned_IP* — The IP address assigned to the client

**Recommended Action**  None required.
336001

**Error Message** %FTD-3-336001 Route destination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up

**Explanation** The SIA state means that an EIGRP router has not received a reply to a query from one or more neighbors within the time allotted (approximately three minutes). When this happens, EIGRP clears the neighbors that did not send a reply and logs an error message for the route that became active.

- **destination_network** — The route that became active
- **ddb_name** — IPv4
- **as_num** — The EIGRP router

**Recommended Action** Check to see why the router did not get a response from all of its neighbors and why the route disappeared.

336002

**Error Message** %FTD-3-336002: Handle handle_id is not allocated in pool.

**Explanation** The EIGRP router is unable to find the handle for the next hop.

- **handle_id** — The identity of the missing handle

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

336003

**Error Message** %FTD-3-336003: No buffers available for bytes byte packet

**Explanation** The DUAL software was unable to allocate a packet buffer. The Firepower Threat Defense device may be out of memory.

- **bytes** — Number of bytes in the packet

**Recommended Action** Check to see if the Firepower Threat Defense device is out of memory by entering the `show mem` or `show tech` command. If the problem persists, contact the Cisco TAC.

336004

**Error Message** %FTD-3-336004: Negative refcount in pakdesc pakdesc.

**Explanation** The reference count packet count became negative.

- **pakdesc** — Packet identifier

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

336005

**Error Message** %FTD-3-336005: Flow control error, error, on interface_name.

**Explanation** The interface is flow blocked for multicast. Qelm is the queue element, and in this case, the last multicast packet on the queue for this particular interface.
- **error** — Error statement: Qelm on flow ready
- **interface_name** — Name of the interface on which the error occurred

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

### 336006

**Error Message** %FTD-3-336006: num peers exist on IIDB interface_name.

**Explanation** Peers still exist on a particular interface during or after cleanup of the IDB of the EIGRP.

- **num** — The number of peers
- **interface_name** — The interface name

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

### 336007

**Error Message** %FTD-3-336007: Anchor count negative

**Explanation** An error occurred and the count of the anchor became negative when it was released.

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

### 336008

**Error Message** %FTD-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str

**Explanation** An interface is being deleted and some lingering DRDB exists.

- **network** — The destination network
- **address** — The nexthop address
- **interface** — The nexthop interface
- **origin_str** — String defining the origin

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

### 336009

**Error Message** %FTD-3-336009 ddb_name as_id: Internal Error

**Explanation** An internal error occurred.

- **ddb_name** — PDM name (for example, IPv4 PDM)
- **as_id** — Autonomous system ID

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

### 336010

**Error Message** %FTD-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg
**Explanation** A neighbor went up or down.

- **db_name** — IPv4
- **tableid** — Internal ID for the RIB
- **as_id** — Autonomous system ID
- **address** — IP address of the neighbor
- **interface** — Name of the interface
- **event_msg** — Event that is occurring for the neighbor (that is, up or down)
- **msg** — Reason for the event. Possible event_msg and msg value pairs include:
  - resync: peer graceful-restart
  - down: holding timer expired
  - up: new adjacency
  - down: Auth failure
  - down: Stuck in Active
  - down: Interface PEER-TERMINATION received
  - down: K-value mismatch
  - down: Peer Termination received
  - down: stuck in INIT state
  - down: peer info changed
  - down: summary configured
  - down: Max hopcount changed
  - down: metric changed
  - down: [No reason]

**Recommended Action** Check to see why the link on the neighbor is going down or is flapping. This may be a sign of a problem, or a problem may occur because of this.

---

**336011**

**Error Message** %FTD-6-336011: event event

**Explanation** A dual event occurred. The events can be one of the following:

- Redist rt change
- SIA Query while Active

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

---

**336012**

**Error Message** %FTD-3-336012: Interface interface_names going down and neighbor_links links exist

**Explanation** An interface is going down or is being removed from routing through IGRP, but not all links (neighbors) have been removed from the topology table.
**Recommended Action** If the problem persists, contact the Cisco TAC.

336013

**Error Message** %FTD-3-336013: Route iproute, iproute_successors successors, db_successors rdbs

**Explanation** A hardware or software error occurred.

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

336014

**Error Message** %FTD-3-336014: “EIGRP_PDM_Process_name, event_log”

**Explanation** A hardware or software error occurred.

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

336015

**Error Message** %FTD-3-336015: “Unable to open socket for AS as_number”

**Explanation** A hardware or software error occurred.

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

336016

**Error Message** %FTD-3-336016: Unknown timer type timer_type expiration

**Explanation** A hardware or software error occurred.

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

336019

**Error Message** %FTD-3-336019: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached

**Explanation** The number of prefixes in the topology database has reached the configured or default threshold level. The prefix source may be any of the following:

- Neighbor
- Redistributed
- Aggregate

**Recommended Action** Use the `show eigrp accounting` command to obtain details about the source of the prefixes and take corrective action.
337000

**Error Message** %FTD-6-337000: Created BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip>

**Explanation** This syslog message indicates that a BFD active session has been created.

- **id**—A numerical field that denotes the local discriminator value for a particular BFD session
- **real_interface**—The interface name on which the BFD session is running
- **real_host_ip**—The IP address of the neighbor with which the BFD session has come up

**Recommended Action** None.

337001

**Error Message** %FTD-6-337001: Terminated BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip> due to <failure_reason>

**Explanation** This syslog message indicates that an active BFD session has been terminated.

- **id**—A numerical field that denotes the local discriminator value for a particular BFD session
- **real_interface**—The interface name on which the BFD session is running
- **real_host_ip**—The IP address of the neighbor with which the BFD session has come up
- **failure_reason**—One of the following failure reasons: BFD going down on peer’s side, BFD configuration removal on peer’s side, Detection timer expiration, Echo function failure, Path to peer going down, Local BFD configuration removal, BFD client configuration removal

**Recommended Action** None.

337005

**Error Message** %FTD-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port

**Explanation** The adaptive security appliance received an SRTP or RTP packet that was destined to go to the media termination IP address and port, but the corresponding media session to process this packet was not found.

- **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

**Recommended Action** If this message occurs at the end of the call, it is considered normal because the signaling messages may have released the media session, but the endpoint is continuing to send a few SRTP or RTP packets. If this message occurs for an odd-numbered media termination port, the endpoint is sending RTCP, which must be disabled from the CUCM. If this message happens continuously for a call, debug the signaling message transaction either using phone proxy debug commands or capture commands to determine if the signaling messages are being modified with the media termination IP address and port.
**339006**

**Error Message** FTD-3-339006: Umbrella resolver current resolver ipv46 is reachable, resuming Umbrella redirect.

**Explanation** Umbrella had failed to open, and the resolver was unreachable. The resolver is now reachable and service is resumed.

**Recommended Action** None.

**339007**

**Error Message** FTD-3-339007: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-open. Starting probe to resolver.

**Explanation** Umbrella fail-open has been configured and a resolver unreachability has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.

**339008**

**Error Message** FTD-3-339008: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-close.

**Explanation** Umbrella fail-open has NOT been configured and a resolver unreachability has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.

**340001**

**Error Message** FTD-3-340001: Loopback-proxy error: error_string context id context_id , context type - version /request_type /address_type client socket (internal)=client_address_internal /client_port_internal server socket (internal)=server_address_internal /server_port_internal server socket (external)=server_address_external /server_port_external remote socket (external)=remote_address_external /remote_port_external

**Explanation** Loopback proxy allows third-party applications running on the Firepower Threat Defense device to access the network. The loopback proxy encountered an error.

- **context_id** — A unique, 32-bit context ID that is generated for each loopback client proxy request
- **version** — The protocol version
- **request_type** — The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
- **address_type** — The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
- **client_address_internal/server_address_internal** — The addresses that the loopback client and the loopback server used for communication
- **client_port_internal/server_port_internal** — The ports that the loopback client and the loopback server used for communication
- **server_address_external/remote_address_external** — The addresses that the loopback server and the remote host used for communication
• `server_port_external /remote_port_external` — The ports that the loopback server and the remote host used for communication
• `error_string` — The error string that may help troubleshoot the problem

**Recommended Action** Copy the syslog message and contact the Cisco TAC.

---

**340002**

**Error Message** %FTD-6-340002: Loopback-proxy info: error_string context_id context_id, context_type = version /request_type /address_type client_socket (internal)=
client_address_internal /client_port_internal server_socket (internal)=
server_address_internal /server_port_internal server_socket (external)=
server_address_external /server_port_external remote_socket (external)=
remote_address_external /remote_port_external

**Explanation** Loopback proxy allows third-party applications running on the Firepower Threat Defense device to access the network. The loopback proxy generated debugging information for use in troubleshooting.

• `context_id` — A unique, 32-bit context ID that is generated for each loopback client proxy request
• `version` — The protocol version
• `request_type` — The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
• `address_type` — The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
• `client_address_internal/server_address_internal` — The addresses that the loopback client and the loopback server used for communication
• `client_port_internal/server_port_internal` — The ports that the loopback client and the loopback server used for communication
• `server_address_external/remote_address_external` — The addresses that the loopback server and the remote host used for communication
• `server_port_external/remote_port_external` — The ports that the loopback server and the remote host used for communication
• `error_string` — The error string that may help troubleshoot the problem

**Recommended Action** Copy the syslog message and contact the Cisco TAC.

---

**341001**

**Error Message** %FTD-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr

**Explanation** The policy agent processes (DME, ducatiAG, and commonAG) started successfully.

• `vnmc_ip_addr` — The IP address of the VNMC server

**Recommended Action** None.

---

**341002**

**Error Message** %FTD-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_addr

**Explanation** The policy agent processes (DME, ducatiAG, and commonAG) were stopped.

• `vnmc_ip_addr` — The IP address of the VNMC server
Recommended Action None.

341003

Error Message  %FTD-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr
Explanation  The policy agent failed to start.
   • vnmc_ip_addr — The IP address of the VNMC server
Recommended Action  Check for console history and the disk0:/pa/log/vnm_pa_error_status for error messages. To retry starting the policy agent, issue the registration host command again.

341004

Error Message  %FTD-3-341004: Storage device not available: Attempt to shutdown module %s failed.
Explanation  All SSDs have failed or been removed with the system in Up state. The system has attempted to shut down the software module, but that attempt has failed.
   • %s — The software module (for example, cxsc)
Recommended Action  Replace the removed or failed drive and reload the Firepower Threat Defense device.

341005

Error Message  %FTD-3-341005: Storage device not available. Shutdown issued for module %s.
Explanation  All SSDs have failed or been removed with the system in Up state. The system is shutting down the software module.
   • %s — The software module (for example, cxsc)
Recommended Action  Replace the removed or failed drive and reload the software module.

341006

Error Message  %FTD-3-341006: Storage device not available. Failed to stop recovery of module %s.
Explanation  All SSDs have failed or been removed with the system in recovery state. The system attempted to stop the recover, but that attempt failed.
   • %s — The software module (for example, cxsc)
Recommended Action  Replace the removed or failed drive and reload the Firepower Threat Defense device.

341007

Error Message  %FTD-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.
**Explanation** All SSDs have failed or been removed with the system in recovery state. The system is stopping the recovery of the software module.

- %s — The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the software module.

---

**341008**

**Error Message** %FTD-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.

**Explanation** After getting the system into Up state, all SSDs have failed or been removed before reloading the system. Because the default action during boot is to auto-boot the software module, that action is blocked because there is no storage device available.

**Recommended Action** Replace the removed or failed drive and reload the software module.

---

**341010**

**Error Message** %FTD-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no

**Explanation** The Firepower Threat Defense device has detected insertion or removal events and generates this syslog message immediately.

**Recommended Action** None required.

---

**341011**

**Error Message** %FTD-3-341011: Storage device with serial number ser_no in bay bay_no faulty.

**Explanation** The Firepower Threat Defense device polls the hard disk drive (HDD) health status every 10 minutes and generates this syslog message if the HDD is in a failed state.

**Recommended Action** None required.
CHAPTER 5

Syslog Messages 401001 to 450001

This chapter contains the following sections:

- Messages 401001 to 409128, on page 151
- Messages 410001 to 450001, on page 176

Messages 401001 to 409128

This chapter includes messages from 401001 to 409128.

401001

Error Message %FTD-4-401001: Shuns cleared

Explanation The clear shun command was entered to remove existing shuns from memory. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401002

Error Message %FTD-4-401002: Shun added: IP_address IP_address port port

Explanation A shun command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401003

Error Message %FTD-4-401003: Shun deleted: IP_address

Explanation A single shunned host was removed from the shun database. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.
401004

**Error Message**
%FTD-4-401004: Shunned packet: IP_address = IP_address on interface interface_name

**Explanation**
A packet was dropped because the host defined by IP SRC is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface. A record of the activity of shunned hosts was provided. This message and message %FTD-4-401005 can be used to evaluate further risk concerning this host.

**Recommended Action**
None required.

401005

**Error Message**
%FTD-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port

**Explanation**
The Firepower Threat Defense device is out of memory; a shun cannot be applied.

**Recommended Action**
The Cisco IPS should continue to attempt to apply this rule. Try to reclaim memory and reapply a shun manually, or wait for the Cisco IPS to do this.

402114

**Error Message**
%FTD-4-402114: IPSEC: Received a protocol packet (SPI=spi , sequence number=seq_num ) from remote_IP to local_IP with an invalid SPI.

- >protocol—IPsec protocol
- >spi—IPsec Security Parameter Index
- seq_num>—IPsec sequence number
- remote_IP>—IP address of the remote endpoint of the tunnel
- >username—Username associated with the IPsec tunnel
- local_IP>—IP address of the local endpoint of the tunnel

**Explanation**
An IPsec packet was received that specifies an SPI that does not exist in the SA database. This may be a temporary condition caused by slight differences in aging of SAs between the IPsec peers, or it may be because the local SAs have been cleared. It may also indicate incorrect packets sent by the IPsec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

**Recommended Action**
The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish connection successfully. Otherwise, if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer administrator.

402115

**Error Message**
%FTD-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.

**Explanation**
An IPsec packet was received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy, which may indicate an attack. This message is rate limited to no more than one message every five seconds.
**402116**

**Error Message** %FTD-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP. The decapsulated inner packet doesn’t match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot. The SA specifies its local proxy as id_daddr/id_dmask/id_dprot/id_dport and its remote proxy as id_saddr/id_smask/id_sprot/id_sport.

**Explanation** A decapsulated IPSec packet does not match the negotiated identity. The peer is sending other traffic through this security association, which may be caused by a security association selection error by the peer, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

- >protocol— IPSec protocol
- >spi— IPSec Security Parameter Index
- >seq_num— IPSec sequence number
- remote_IP— IP address of the remote endpoint of the tunnel
- >username— Username associated with the IPSec tunnel
- local_IP— IP address of the local endpoint of the tunnel
- pkt_daddr— Destination address from the decapsulated packet
- pkt_saddr— Source address from the decapsulated packet
- pkt_prot— Transport protocol from the decapsulated packet
- id_daddr— Local proxy IP address
- id_dmask— Local proxy IP subnet mask
- id_dprot— Local proxy transport protocol
- id_dport— Local proxy port
- id_saddr— Remote proxy IP address
- id_smask— Remote proxy IP subnet mask
- id_sprot— Remote proxy transport protocol
- id_sport— Remote proxy port

**Recommended Action** Contact the administrator of the peer and compare policy settings.

---

**402117**

**Error Message** %FTD-4-402117: IPSEC: Received a non-IPsec (protocol) packet from remote_IP to local_IP.

**Explanation** The received packet matched the crypto map ACL, but it is not IPSec-encapsulated. The IPSec peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall may be configured to only accept encrypted Telnet traffic to the outside interface port 23. If you attempt to use Telnet without IPSec encryption to access the outside interface on port 23, this
message appears, but not with Telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This message is not generated except under these conditions (for example, it is not generated for traffic to the Firepower Threat Defense interfaces themselves). See messages 710001, 710002, and 710003, which track TCP and UDP requests. This message is rate limited to no more than one message every five seconds.

- **protocol** — IPsec protocol
- **remote_IP** — IP address of the remote endpoint of the tunnel
- **local_IP** — IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the peer to compare policy settings.

---

**402118**

**Error Message**

FTD-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.

**Explanation**

A decapsulated IPsec packet included an IP fragment with an offset less than or equal to 128 bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

- **protocol** — IPsec protocol
- **spi** — IPsec Security Parameter Index
- **seq_num** — IPsec sequence number
- **remote_IP** — IP address of the remote endpoint of the tunnel
- **username** — Username associated with the IPsec tunnel
- **local_IP** — IP address of the local endpoint of the tunnel
- **frag_len** — IP fragment length
- **frag_offset** — IP fragment offset in bytes

**Recommended Action** Contact the administrator of the remote peer to compare policy settings.

---

**402119**

**Error Message**

FTD-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.

**Explanation**

An IPsec packet was received with an invalid sequence number. The peer is sending packets including sequence numbers that may have been previously used. This message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

- **protocol** — IPsec protocol
- **spi** — IPsec Security Parameter Index
- **seq_num** — IPsec sequence number
- **remote_IP** — IP address of the remote endpoint of the tunnel
- **username** — Username associated with the IPsec tunnel
- **local_IP** — IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the peer.
402120

**Error Message** %FTD-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP that failed authentication.

**Explanation** An IPsec packet was received and failed authentication. The packet is dropped. The packet may have been corrupted in transit, or the peer may be sending invalid IPsec packets, which may indicate an attack if many of these packets were received from the same peer. This message is rate limited to no more than one message every five seconds.

- `protocol` — IPsec protocol
- `spi` — IPsec Security Parameter Index
- `seq_num` — IPsec sequence number
- `remote_IP` — IP address of the remote endpoint of the tunnel
- `username` — Username associated with the IPsec tunnel
- `local_IP` — IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the remote peer if many failed packets were received.

402121

**Error Message** %FTD-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number=seq_num) from peer_addr (username) to lcl_addr that was dropped by IPsec (drop_reason).

**Explanation** An IPsec packet to be decapsulated was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Firepower Threat Defense configuration or with the Firepower Threat Defense device itself.

- `protocol` — IPsec protocol
- `spi` — IPsec Security Parameter Index
- `seq_num` — IPsec sequence number
- `peer_addr` — IP address of the remote endpoint of the tunnel
- `username` — Username associated with the IPsec tunnel
- `lcl_addr` — IP address of the local endpoint of the tunnel
- `drop_reason` — Reason that the packet was dropped

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

402122

**Error Message** %FTD-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPsec that was dropped by IPsec (drop_reason).

**Explanation** A packet to be encapsulated in IPsec was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Firepower Threat Defense configuration or with the Firepower Threat Defense device itself.

- `src_addr` — Source IP address
- `dest_addr` — Destination IP address
- `drop_reason` — Reason that the packet was dropped

**Recommended Action** If the problem persists, contact the Cisco TAC.
402123

**Error Message** %FTD-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code=error_string) while executing crypto command command.

**Explanation** An error was detected while running a crypto command with a hardware accelerator, which may indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the crypto accelerator counters to help determine the cause.

- accel_type—Hardware accelerator type
- >error_string—Code indicating the type of error
- command—Crypto command that generated the error

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

402124

**Error Message** %FTD-4-402124: CRYPTO: The FTD hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).

**Explanation** The crypto hardware chip has reported a fatal error, indicating that the chip is inoperable. The information from this message captures the details to allow further analysis of the problem. The crypto chip is reset when this condition is detected to unobtrusively allow the Firepower Threat Defense device to continue functioning. Also, the crypto environment at the time this issue is detected is written to a crypto archive directory on flash to provide further debugging information. Various parameters related to the crypto hardware are included in this message, as follows:

- HWErrAddr—Hardware address (set by crypto chip)
- Core—Crypto core experiencing the error
- HwErrCode—Hardware error code (set by crypto chip)
- IstatReg—Interrupt status register (set by crypto chip)
- PciErrReg—PCI error register (set by crypto chip)
- CoreErrStat—Core error status (set by crypto chip)
- CoreErrAddr—Core error address (set by crypto chip)
- Doorbell Size—Maximum crypto commands allowed
- DoorBell Outstanding—Crypto commands outstanding
- SWReset—Number of crypto chip resets since boot

**Note** The %FTD-vpn-4-402124: CRYPTO: The FTD hardware accelerator encountered an error (HWErrAddr=0x40EE9800, Core=0, HwErrCode=23, IstatReg=0x8, PciErrReg=0x0, CoreErrStat=0x41, CoreErrAddr=0x844E9800, Doorbell Size[0]=2048, DoorBell Outstanding[0]=0, Doorbell Size[1]=0, DoorBell Outstanding[1]=0, SWReset=99) error message indicates a AnyConnect problem and the workaround for this to upgrade to AnyConnect 3.1.x.

**Recommended Action** Forward the message information to the Cisco TAC for further analysis.
402125

**Error Message** %FTD-4-402125: The FTD hardware accelerator ring timed out (parameters).

**Explanation** The crypto driver has detected that either the IPSEC descriptor ring or SSL/Admin descriptor ring is no longer progressing, meaning the crypto chip no longer appears to be functioning. The crypto chip is reset when this condition is detected to unobtrusively allow the Firepower Threat Defense device to continue functioning. Also, the crypto environment at the time this issue was detected was written to a crypto archive directory on flash to provide further debugging information.

- >ring— IPSEC or Admin ring
- parameters >— Include the following:
  - Desc>— Descriptor address
  - CtrlStat>— Control/status value
  - ResultP>— Success pointer
  - ResultVal>— Success value
  - Cmd>— Crypto command
  - CmdSize>— Command size
  - Param>— Command parameters
  - Dlen>— Data length
  - DataP>— Data pointer
  - CtxtP>— VPN context pointer
  - SWReset>— Number of crypto chip resets since boot

**Recommended Action** Forward the message information to the Cisco TAC for further analysis.

402126

**Error Message** %FTD-4-402126: CRYPTO: The FTD created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.

**Explanation** A functional problem with the hardware crypto chip was detected (see syslog messages 402124 and 402125). To further debug the crypto problem, a crypto archive file was generated that included the current crypto hardware environment (hardware registers and crypto description entries). At boot time, a crypto_archive directory was automatically created on the flash file system (if it did not exist previously). A maximum of two crypto archive files are allowed to exist in this directory.

- >Archive Filename— The name of the crypto archive file name. The crypto archive file names are of the form, crypto_arch_x.bin, where x = (1 or 2).

**Recommended Action** Forward the crypto archive files to the Cisco TAC for further analysis.

402127

**Error Message** %FTD-4-402127: CRYPTO: The FTD is skipping the writing of latest Crypto Archive File as the maximum # of files, max_number, allowed have been written to archive_directory
Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.

**Explanation** A functional problem with the hardware crypto chip was detected (see messages 4402124 and 4402125). This message indicates a crypto archive file was not written, because the maximum number of crypto archive files already existed.

- **max_number** — Maximum number of files allowed in the archive directory; currently set to two
- **archive_directory** — Name of the archive directory

**Recommended Action** Forward previously generated crypto archive files to the Cisco TAC. Remove the previously generated archive file(s) so that more can be written (if deemed necessary).

---

**402128**

**Error Message** %FTD-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit

**Explanation** An SSL connection is attempting to use more memory than allowed. The request has been denied.

- **size** — The size of the memory block being allocated
- **limit** — The maximum size of allocated memory permitted

**Recommended Action** If this message persists, an SSL denial of service attack may be in progress. Contact the remote peer administrator or upstream provider.

---

**402129**

**Error Message** %FTD-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address

**Explanation** An internal software error has occurred.

- **address** — The address being freed

**Recommended Action** Contact the Cisco TAC for assistance.

---

**402130**

**Error Message** %FTD-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number=0x7B) from 75.2.96.101 (user=user) to 85.2.96.10 with incorrect IPsec padding.

**Explanation** The Firepower Threat Defense device crypto hardware accelerator detected an IPsec packet with invalid padding. The ATT VPN client sometimes pads IPsec packets incorrectly.

- **SPI** — The SPI associated with the packet
- **sequence number** — The sequence number associated with the packet
- **user** — Username string
- **padding** — Padding data from the packet

**Recommended Action** While this message is None required and does not indicate a problem with the Firepower Threat Defense device, customers using the ATT VPN client may wish to upgrade their VPN client software.
402131

**Error Message** `%FTD-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias`.

**Explanation** The hardware accelerator configuration has been changed on the Firepower Threat Defense device. Some Firepower Threat Defense platforms have multiple hardware accelerators. One syslog message is generated for each hardware accelerator change.

- **status** — Indicates success or failure
- **accel_instance** — The instance of the hardware accelerator
- **old_config_bias** — The old configuration
- **new_config_bias** — The new configuration

**Recommended Action** If any of the accelerators fails when attempting to change its configuration, collect logging information and contact the Cisco TAC. If a failure occurs, the software will retry the configuration change multiple times. The software will fall back to the original configuration bias if the retry attempts fail. If multiple attempts to reconfigure the hardware accelerator fail, it may indicate a hardware failure.

402140

**Error Message** `%FTD-3-402140: CRYPTO: RSA key generation error: modulus len len`.

**Explanation** An error occurred during an RSA public key pair generation.

- **len** — The prime modulus length in bits

**Recommended Action** Contact the Cisco TAC for assistance.

402141

**Error Message** `%FTD-3-402141: CRYPTO: Key zeroization error: key set type, reason reason`.

**Explanation** An error occurred during an RSA public key pair generation.

- **type** — The key set type, which can be any of the following: DH, RSA, DSA, or unknown
- **reason** — The unexpected crypto session type

**Recommended Action** Contact the Cisco TAC for assistance.

402142

**Error Message** `%FTD-3-402142: CRYPTO: Bulk data op error: algorithm alg, mode mode`.

**Explanation** An error occurred during a symmetric key operation.

- **op** — The operation, which can be either encryption or decryption
- **alg** — The encryption algorithm, which can be any of the following: DES, 3DES, AES, or RC4
- **mode** — The mode, which can be any of the following: CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4

**Recommended Action** Contact the Cisco TAC for assistance.
**402143**

**Error Message** %FTD-3-402143: CRYPTO: alg type key op

**Explanation** An error occurred during an asymmetric key operation.

- *alg* — The encryption algorithm, which can be either RSA or DSA
- *type* — The key type, which can be either public or private
- *op* — The operation, which can be either encryption or decryption

**Recommended Action** Contact the Cisco TAC for assistance.

---

**402144**

**Error Message** %FTD-3-402144: CRYPTO: Digital signature error: signature algorithm sig , hash algorithm hash

**Explanation** An error occurred during digital signature generation.

- *sig* — The signature algorithm, which can be either RSA or DSA
- *hash* — The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

**Recommended Action** Contact the Cisco TAC for assistance.

---

**402145**

**Error Message** %FTD-3-402145: CRYPTO: Hash generation error: algorithm hash

**Explanation** A hash generation error occurred.

- *hash* — The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

**Recommended Action** Contact the Cisco TAC for assistance.

---

**402146**

**Error Message** %FTD-3-402146: CRYPTO: Keyed hash generation error: algorithm hash , key len

**Explanation** A keyed hash generation error occurred.

- *hash* — The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512
- *len* — The key length in bits

**Recommended Action** Contact the Cisco TAC for assistance.

---

**402147**

**Error Message** %FTD-3-402147: CRYPTO: HMAC generation error: algorithm alg

**Explanation** An HMAC generation error occurred.
• **alg** — The HMAC algorithm, which can be any of the following: HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC

**Recommended Action** Contact the Cisco TAC for assistance.

### 402148

**Error Message** %FTD-3-402148: CRYPTO: Random Number Generator error

**Explanation** A random number generator error occurred.

**Recommended Action** Contact the Cisco TAC for assistance.

### 402149

**Error Message** %FTD-3-402149: CRYPTO: weak encryption type (length ). Operation disallowed. Not FIPS 140-2 compliant

**Explanation** The Firepower Threat Defense device tried to use an RSA key that is less than 2048 bits or DH groups 1, 2, or 5.

• **encryption type** — The encryption type
  • **length** — The RSA key length or DH group number

**Recommended Action** Configure the Firepower Threat Defense device or external application to use an RSA key that is at least 2048 bits, or to configure a DH group that is not 1, 2, or 5.

### 402150

**Error Message** %FTD-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg ). Operation disallowed. Not FIPS 140-2 compliant

**Explanation** An unacceptable hashing algorithm has been used for digital certificate signing or verification for FIPS 140-2 certification.

• **operation** — Sign or verify
  • **hash alg** — The name of the unacceptable hashing algorithm

**Recommended Action** Make sure that you use the minimum acceptable hashing algorithm for digital certificate signing or verification for FIPS 140-2 certification. These include SHA-256, SHA-384, and SHA-512.

### 403500

**Error Message** %FTD-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name.

**Explanation** The Firepower Threat Defense device requested the PPPoE service *any* from the access controller at the Internet service provider. The response from the service provider includes other services, but does not include the service *any*. This is a discrepancy in the implementation of the protocol. The PADO packet is processed normally, and connection negotiations continue.

**Recommended Action** None required.
Error Message %FTD-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.

Explanation The Firepower Threat Defense device sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Firepower Threat Defense device was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

Recommended Action Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

Error Message %FTD-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.

Explanation The Firepower Threat Defense device sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Firepower Threat Defense device was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

Recommended Action Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

Error Message %FTD-3-403503: PPPoE:PPP link down:reason

Explanation The PPP link has gone down. There are many reasons why this can happen. The first format will display a reason if PPP provides one.

Recommended Action Check the network link to ensure that the link is connected. The access concentrator may be down. Make sure that your authentication protocol matches the access concentrator and that your name and password are correct. Verify this information with your ISP or network support person.

Error Message %FTD-3-403504: PPPoE:No 'vdpn group group_name ' for PPPoE is created

Explanation PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username, and a password. The following example configures the Firepower Threat Defense device for PPPoE dialout. The my-username and my-password commands are used to authenticate the access concentrator, using PAP if necessary.

For example:

ciscoftd# vpdn group my-pppoe request dialout pppoe

ciscoftd# vpdn group my-pppoe ppp authentication pap

ciscoftd# vpdn group my-pppoe localname my-username

ciscoftd# vpdn username my-username password my-password

ciscoftd# ip address outside pppoe setroute
**Recommended Action** Configure a VPDN group for PPPoE.

**403505**

**Error Message** %FTD-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name

**Explanation** This message is usually followed by the message, default route already exists.

**Recommended Action** Remove the current default route or remove the setroute parameter so that there is no conflict between PPPoE and the manually configured route.

**403506**

**Error Message** %FTD-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name

**Explanation** This message is followed by one of the followings messages: subnet is the same as interface, or on failover channel.

**Recommended Action** In the first case, change the address causing the conflict. In the second case, configure the PPPoE on an interface other than the failover interface.

**403507**

**Error Message** %FTD-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name

**Explanation** You can configure the PPPoE client on an interface to use a particular VPDN group by entering the pppoe client vpdn group group_name command. If a PPPoE VPDN group of the configured name was not located during system startup, this message is generated.

- **interface** — The interface on which the PPPoE client failed
- **group_name** — The VPDN group name of the PPPoE client on the interface

**Recommended Action** Perform the following steps:

1. Add the required VPDN group by entering the vpdn group group_name command. Request dialout PPPoE in global configuration mode, and add all the group properties.
2. Remove the pppoe client vpdn group group_name command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.

**Note** All changes take effect only after the PPPoE client on the interface is restarted by entering the ip address pppoe command.

**405001**

**Error Message** %FTD-4-405001: Received ARP {request | response} collision from IP_address /MAC_address on interface interface_name with existing ARP entry IP_address /MAC_address
**Explanation** The Firepower Threat Defense device received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and to see if they belong to a valid host.

**405002**

**Error Message** %FTD-4-405002: Received mac mismatch collision from IP_address / MAC_address for authenticated host

**Explanation** This packet appears for one of the following conditions:

- The Firepower Threat Defense device received a packet with the same IP address, but a different MAC address from one of its uauth entries.
- You configured the **vpnclient mac-exempt** command on the Firepower Threat Defense device, and the Firepower Threat Defense device received a packet with an exempt MAC address, but a different IP address from the corresponding uauth entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that a spoofing attack is in progress. Check the source MAC address and IP address to determine where the packets are coming from and if they belong to a valid host.

**405003**

**Error Message** %FTD-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name, MAC_address.

**Explanation** A client IP address in the network is the same as the Firepower Threat Defense interface IP address.

**Recommended Action** Change the IP address of the client.

**405101**

**Error Message** %FTD-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address [/outside_port ] to local_address inside_address [/inside_port ]

**Explanation** The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** If this message occurs periodically, it can be ignored. You can check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory. If the problem persists, contact the Cisco TAC.

**405102**

**Error Message** %FTD-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address [/outside_port ] to local_address inside_address [/inside_port ]
**Explanation** The Firepower Threat Defense device failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translations and connections. In addition, reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

---

**405103**

**Error Message** %FTD-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex

**Explanation** The Firepower Threat Defense device is expecting the protocol discriminator, 0x08, but it received something other than 0x08. The endpoint may be sending a bad packet, or received a message segment other than the first segment. The packet is allowed through.

**Recommended Action** None required.

---

**405104**

**Error Message** %FTD-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP

**Explanation** An H.225 message was received out of order, before the initial SETUP message, which is not allowed. The Firepower Threat Defense device must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

**Recommended Action** None required.

---

**405105**

**Error Message** %FTD-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest

**Explanation** A gatekeeper has sent an ACF, but the Firepower Threat Defense device did not send an ARQ to the gatekeeper.

**Recommended Action** Check the gatekeeper with the specified source_address to determine why it sent an ACF without receiving an ARQ from the Firepower Threat Defense device.

---

**406001**

**Error Message** %FTD-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name

**Explanation** A client entered an FTP port command and supplied a port less than 1024 (in the well-known port range usually devoted to server ports). This is indicative of an attempt to avert the site security policy. The Firepower Threat Defense device drops the packet, terminates the connection, and logs the event.

**Recommended Action** None required.
406002

Error Message  %FTD-4-406002: FTP port command different address: IP_address(IP_address ) to IP_address on interface interface_name

Explanation  A client entered an FTP port command and supplied an address other than the address used in the connection. An attempt to avert the site security policy occurred. For example, an attacker might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The Firepower Threat Defense device drops the packet, terminates the connection, and logs the event. The address in parentheses is the address from the port command.

Recommended Action  None required.

407001

Error Message  %FTD-4-407001: Deny traffic for local-host interface_name :inside_address , license limit of number exceeded

Explanation  The host limit was exceeded. An inside host is counted toward the limit when one of the following conditions is true:

- The inside host has forwarded traffic through the Firepower Threat Defense device within the last five minutes.
- The inside host has reserved an xlate connection or user authentication at the Firepower Threat Defense device.

Recommended Action  The host limit is enforced on the low-end platforms. Use the show version command to view the host limit. Use the show local-host command to view the current active hosts and the inside users that have sessions at the Firepower Threat Defense device. To forcefully disconnect one or more users, use the clear local-host command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower as given in the table below:

Table 5: Timeouts and Recommended Values

<table>
<thead>
<tr>
<th>Timeout</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>xlate</td>
<td>00:05:00 (five minutes)</td>
</tr>
<tr>
<td>conn</td>
<td>00:01:00 (one hour)</td>
</tr>
<tr>
<td>uauth</td>
<td>00:05:00 (five minutes)</td>
</tr>
</tbody>
</table>

407002

Error Message  %FTD-4-407002: Embryonic limit nconns /elimit for through connections exceeded.outside_address /outside_port to global_address (inside_address )/inside_port on interface interface_name

Explanation  The number of connections from a specified foreign address over a specified global address to the specified local address exceeded the maximum embryonic limit for that static. The Firepower Threat Defense device tries to accept the connection if it can allocate memory for that connection. It proxies on behalf of the local host and sends a SYN_ACK packet to the foreign host. The Firepower Threat Defense device
retains pertinent state information, drops the packet, and waits for the acknowledgment from the client. The message might indicate legitimate traffic or that a DoS attack is in progress.

**Recommended Action** Check the source address to determine where the packets are coming from and whether or not a valid host is sending them.

### 407003

**Error Message** %FTD-4-407003: Established limit for RPC services exceeded number

**Explanation** The Firepower Threat Defense device tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

**Recommended Action** Wait for other holes to be closed (through associated timeout expiration), or limit the number of active pairs of servers or services.

### 408001

**Error Message** %FTD-4-408001: IP route counter negative - reason , IP_address Attempt: number

**Explanation** An attempt to decrement the IP route counter into a negative value failed.

**Recommended Action** Enter the `clear ip route` command to reset the route counter. If the problem persists, contact the Cisco TAC.

### 408002

**Error Message** %FTD-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP : interface1 address2 netmask2 [distance2 /metric2 ] interface2

**Explanation** A network update was received from a different interface with the same distance and a better metric than the existing route. The new route overrides the existing route that was installed through another interface. The new route is for redundancy purposes only and means that a path has shifted in the network. This change must be controlled through topology and redistribution. Any existing connections affected by this change are probably disabled and will time out. This path shift only occurs if the network topology has been specifically designed to support path redundancy, in which case it is expected.

**Recommended Action** None required.

### 408003

**Error Message** %FTD-4-408003: can't track this type of object hex

**Explanation** A component of the tracking system has encountered an object type that is not supported by the component. A STATE object was expected.

- *hex* — A hexadecimal value(s) depicting variable value(s) or addresses in memory

**Recommended Action** Reconfigure the track object to make it a STATE object.
**408101**

**Error Message** %FTD-4-408101: KEYMAN : Type encryption_type encryption unknown. Interpreting keystring as literal.

**Explanation** The format type was not recognized by the system. A keystring format type value of 0 (unencrypted keystring) or 7 (hidden keystring), followed by a space, can precede the actual keystring to indicate its format. An unknown type value will be accepted, but the system will consider the keystring as being unencrypted.

**Recommended Action** Use the correct format for the value type or remove the space following the value type.

**408102**

**Error Message** %FTD-4-408102: KEYMAN : Bad encrypted keystring for key id key_id.

**Explanation** The system could not successfully decrypt an encrypted keystring. The keystring may have been corrupted during system configuration.

**Recommended Action** Re-enter the key-string command, and reconfigure the key string.

**409001**

**Error Message** %FTD-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstall

**Explanation** The software detected an unexpected condition. The router will take corrective action and continue.

**Recommended Action** None required.

**409002**

**Error Message** %FTD-4-409002: db_free: external LSA IP_address netmask

**Explanation** An internal software error occurred.

**Recommended Action** None required.

**409003**

**Error Message** %FTD-4-409003: Received invalid packet: reason from IP_address , interface_name

**Explanation** An invalid OSPF packet was received. Details are included in the error message. The cause might be an incorrect OSPF configuration or an internal error in the sender.

**Recommended Action** Check the OSPF configuration of the receiver and the sender configuration for inconsistency.

**409004**

**Error Message** %FTD-4-409004: Received reason from unknown neighbor IP_address
Explanation The OSPF hello, database description, or database request packet was received, but the router cannot identify the sender.

Recommended Action None required.

409005

Error Message %FTD-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name

Explanation The Firepower Threat Defense device received an OSPF packet with a field length of less than normal header size or that was inconsistent with the size of the IP packet in which it arrived. This indicates a configuration error in the sender of the packet.

Recommended Action From a neighboring address, locate the problem router and reboot it.

409006

Error Message %FTD-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name

Explanation The router received an LSA with an invalid LSA type. The cause is either memory corruption or unexpected behavior on a router.

Recommended Action From a neighboring address, locate the problem router and reboot it. If the problem persists, contact the Cisco TAC.

409007

Error Message %FTD-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask

Explanation An internal software error occurred.

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

409008

Error Message %FTD-4-409008: Found generating default LSA with non-zero mask LSA type: number Mask: netmask metric: number area: string

Explanation The router tried to generate a default LSA with an incorrect mask and possibly incorrect metric because an internal software error occurred.

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

409009

Error Message %FTD-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

Explanation OSPF failed while attempting to allocate a router ID from the IP address of one of its interfaces.
**Recommended Action** Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough interfaces up so that each of them can obtain a router ID.

**409010**

**Error Message** %FTD-4-409010: Virtual link information found in non-backbone area: string

**Explanation** An internal error occurred.

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

**409011**

**Error Message** %FTD-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

**409012**

**Error Message** %FTD-4-409012: Detected router with duplicate router ID IP_address in area string

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

**409013**

**Error Message** %FTD-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

**409014**

**Error Message** %FTD-4-409014: No valid authentication send key is available on interface nameif.

**Explanation** The authentication key configured on the interface is not valid.

**Recommended Action** Configure a new key.
**409015**

**Error Message** %FTD-4-409015: Key ID key-id received on interface nameif.

**Explanation** The ID is not found in the configured key chain.

**Recommended Action** Configure a new security association with the Key ID.

**409016**

**Error Message** %FTD-4-409016: Key chain name key-chain-name on nameif is invalid.

**Explanation** The key-chain name configured under OSPF interface does not match global key chain configuration.

**Recommended Action** Fix configuration. Either remove OSPF authentication command or configure key chain in global configuration mode.

**409017**

**Error Message** %FTD-4-409017: Key ID key-id in key chain key-chain-name is invalid.

**Explanation** The Key ID configured in the key chain is out of range for OSPF. This may happen because the key chain allows Key ID values of the range which is not acceptable for OSPF.

**Recommended Action** Configure a new security association with a Key ID that is in the range 1-255.

**409023**

**Error Message** %FTD-4-409023: Attempting AAA Fallback method method_name for request_type request for user user :Auth-server group server_tag unreachable

**Explanation** An authentication or authorization attempt to an external server has failed and will be performed using the local user database.

- **aaa_operation**—Either authentication or authorization
- **username**—The user associated with the connection
- **server_group**—The name of the AAA server whose servers were unreachable

**Recommended Action** Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the Firepower Threat Defense device. Make sure that the daemons are running on the AAA server.

**409101**

**Error Message** %FTD-4-409101: Received invalid packet: s from P, s

**Explanation** An invalid OSPF packet was received. Details are included in the error message. The cause might be a misconfigured OSPF or an internal error in the sender.

**Recommended Action** Check the OSPF configuration of the receiver and the sender for inconsistencies.
### 409102

**Error Message** %FTD-4-409102: Received packet with incorrect area from P, s, area AREA_ID_STR, packet area AREA_ID_STR

**Explanation** An OSPF packet was received with an area ID in its header that does not match the area of this interface.

**Recommended Action** Check the OSPF configuration of the receiver and the sender for inconsistencies.

### 409103

**Error Message** %FTD-4-409103: Received s from unknown neighbor i

**Explanation** An OSPF hello, database description, or database request packet was received, but the router could not identify the sender.

**Recommended Action** None required.

### 409104

**Error Message** %FTD-4-409104: Invalid length d in OSPF packet type d from P (ID i), s

**Explanation** The system received an OSPF packet with a length field of less than normal header size or inconsistent with the size of the IP packet in which it arrived. An error in the sender of the packet has occurred.

**Recommended Action** None required.

### 409105

**Error Message** %FTD-4-409105: Invalid lsa: s: Type 0x x, Length 0x x, LSID u from i

**Explanation** The router received an LSA with invalid data. The LSA includes an invalid LSA type, incorrect checksum, or incorrect length, which is caused by either memory corruption or unexpected behavior on a router.

**Recommended Action** From a neighboring address, locate the problem router and do the following:

- Collect a running configuration of the router by entering the `show running-config` command.
- Enter the `show ipv6 ospf database` command to gather data that may help identify the nature of the error.
- Enter the `show ipv6 ospf database link-state-id` command. The `link-state-id` argument is the IP address of the invalid LSA.
- Enter the `show logging` command to gather data that may help identify the nature of the error.
- Reboot the router.

If you cannot determine the nature of the error from the collected information, contact the Cisco TAC and provide the gathered information.

### 409106

**Error Message** %FTD-4-409106: Found generating default LSA with non-zero mask LSA type: 0x x Mask: i metric: iu area: AREA_ID_STR
Explanation The router tried to generate the default LSA with the incorrect mask and possibly an incorrect metric because of an internal software error.

Recommended Action None required.

409107

ErrorMessage %FTD-4-409107: OSPFv3 process d could not pick a router-id, please configure manually

Explanation OSPFv3 failed while attempting to allocate a router ID from the IP address of one of its interfaces.

Recommended Action Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough up interfaces so that each of them can obtain a router ID.

409108

ErrorMessage %FTD-4-409108: Virtual link information found in non-backbone area: AREA_ID_STR

Explanation An internal error has occurred.

Recommended Action None required.

409109

ErrorMessage %FTD-4-409109: OSPF detected duplicate router-id i from P on interface IF_NAME

Explanation OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established. The OSPF router ID should be unique.

Recommended Action Change the neighbor router ID.

409110

ErrorMessage %FTD-4-409110: Detected router with duplicate router ID i in area AREA_ID_STR

Explanation OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established. The OSPF router ID should be unique.

Recommended Action Change the neighbor router ID.

409111

ErrorMessage %FTD-4-409111: Multiple interfaces (IF_NAME /IF_NAME ) on a single link detected.

Explanation OSPFv3 enabled on multiple interfaces that are on the same link is not supported.

Recommended Action OSPFv3 should be disabled or made passive on all except one of the interfaces.
409112

**Error Message** %FTD-4-409112: Packet not written to the output queue

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409113

**Error Message** %FTD-4-409113: Doubly linked list linkage is NULL

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409114

**Error Message** %FTD-4-409114: Doubly linked list prev linkage is NULL

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409115

**Error Message** %FTD-4-409115: Unrecognized timer d in OSPF s

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409116

**Error Message** %FTD-4-409116: Error for timer d in OSPF process s

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409117

**Error Message** %FTD-4-409117: Can't find LSA database type x, area AREA_ID_STR, interface x

**Explanation** An internal error has occurred.

**Recommended Action** None required.

409118

**Error Message** %FTD-4-409118: Could not allocate DBD packet

**Explanation** An internal error has occurred.
Recommended Action None required.

409119

Error Message %FTD-4-409119: Invalid build flag x for LSA i , type 0x x
Explanation An internal error has occurred.
Recommended Action None required.

409120

Error Message %FTD-4-409120: Router-ID i is in use by ospf process d
Explanation The Firepower 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.

409121

Error Message %FTD-4-409121: 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.

409122

Error Message %FTD-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.
Explanation A virtual link was configured. For the virtual link to function, a global IPv6 address must be available. However, no global IPv6 address could be found on the router.
Recommended Action Configure a global IPv6 address on an interface on this router.

409123

Error Message %FTD-4-409123: Neighbor command allowed only on NBMA networks
Explanation The neighbor command is allowed only on NBMA networks.
Recommended Action Check the configuration options for the neighbor command, and correct the options or the network type for the neighbor interface.

409125

Error Message %FTD-4-409125: 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 interface.

409128

Error Message %FTD-4-409128: OSPFv3-d Area AREA_ID_STR : Router i originating invalid type 0x x LSA, ID u, Metric d on Link ID d Link Type d

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 exists in the network.

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

Messages 410001 to 450001

This chapter includes messages from 410001 to 450001.

410001

Error Message %FTD-4-410001: UDP DNS request from source_interface :source_address /source_port to dest_interface :dest_address /dest_port ; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.

Explanation The domain-name length exceeds 255 bytes in a UDP DNS packet. See RFC 1035, Section 3.1 for more information.

Recommended Action None required.

411001

Error Message %FTD-4-411001: Line protocol on interface interface_name changed state to up

Explanation The status of the line protocol has changed from down to up. If `interface_name` is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from down to up. If `interface_name` is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from down to up.

Recommended Action None required.

411002

Error Message %FTD-4-411002: Line protocol on interface interface_name changed state to down

Explanation The status of the line protocol has changed from up to down. If `interface_name` is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from up to down. In this case, the physical interface line protocol status is not affected. If
**interface_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from up to down.

**Recommended Action** If this is an unexpected event on the interface, check the physical line.

### 411003

**Error Message** `%FTD-4-411003: Configuration status on interface interface_name changed state to down up`

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** If this is an unexpected event, check the physical line.

### 411004

**Error Message** `%FTD-4-411004: Configuration status on interface interface_name changed state to up`

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** None required.

### 411005

**Error Message** `%FTD-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.`

**Explanation** The interface experienced a hardware transmit freeze that required a reset of the Ethernet controller to restore the interface to full operation.

- **variable 1** —The interface name, such as GigabitEthernet0/0

**Recommended Action** None required.

### 412001

**Error Message** `%FTD-4-412001: MAC MAC_address moved from interface_1 to interface_2`

**Explanation** A host move was detected from one module interface to another. In a transparent Firepower Threat Defense, mapping between the host (MAC) and Firepower Threat Defense port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to an Firepower Threat Defense port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

**Recommended Action** The host move might be valid or might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, no action is required.
**412002**

**Error Message** %FTD-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num

**Explanation** The bridge table was full and an attempt was made to add one more entry. The Firepower Threat Defense device maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table. This might be an attempted attack.

**Recommended Action** Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to control access to vulnerable hosts.

---

**413001**

**Error Message** %FTD-4-413001: Module module_id is not able to shut down. Module Error: errnum message

**Explanation** The module identified by module_id was not able to comply with a request from the Firepower Threat Defense system module to shut down. It may be performing a task that cannot be interrupted, such as a software upgrade. The errnum and message text describes the reason why the module cannot shut down, and the recommended corrective action.

**Recommended Action** Wait for the task on the module to complete before shutting down the module, or use the session command to access the CLI on the module, and stop the task that is preventing the module from shutting down.

---

**413002**

**Error Message** %FTD-4-413002: Module module_id is not able to reload. Module Error: errnum message

**Explanation** The module identified by module_id was not able to comply with a request from the Firepower Threat Defense module to reload. It may be performing a task that cannot be interrupted, such as a software upgrade. The errnum and message text describes the reason why the module cannot reload, and the recommended corrective action.

**Recommended Action** Wait for the task on the module to complete before reloading the module, or use the session command to access the CLI on the module and stop the task that is preventing the module from reloading.

---

**413003**

**Error Message** %FTD-4-413003: Module string one is not a recognized type

**Explanation** A module was detected that is not recognized as a valid module type.

**Recommended Action** Upgrade to a version of Firepower Threat Defense software that supports the module type installed.
**413004**

**Error Message** %FTD-4-413004: Module *string one* failed to write software *newver* (currently *ver*), *reason*. Trying again.

**Explanation** The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

- *string one*— The text string that specifies the module
- *newver*— The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *ver*— The current version number of the software on the module (for example, 1.0(1)0)
- *reason*— The reason the new version cannot be written to the module. The possible values for *reason* include the following:
  - write failure
  - failed to create a thread to write the image

**Recommended Action** None required. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the `show module` command.

---

**413005**

**Error Message** %FTD-4-413005: Module *module_id*, application is not supported *app_name* version *app_vers* type *app_type*

**Error Message** %FTD-4-413005: Module *prod_id* in slot *slot_num*, application is not supported *app_name* version *app_vers* type *app_type*

**Explanation** The module installed in slot *slot_num* was running an unsupported application version or type.

- *module_id*— The name of the software services module
- *prod_id*— Product ID string
- *slot_num*— The slot number in which the module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *app_name*— Application name (string)
- *app_vers*— Application version (string)
- *app_type*— Application type (decimal)

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

---

**413006**

**Error Message** %FTD-4-413006: *prod-id* Module software version mismatch; slot slot is *prod-id* version *running-vers*. Slot slot *prod-id* requires *required-vers*.

**Explanation** The version of software running on the module in slot *slot* was not the version required by another module.

- *slot*— Slot 0 indicates the system main board. Slot 1 indicates the module installed in the expansion slot.
- *prod_id*— Product ID string for the device installed in slot *slot*
- *running_vers*— Version of software currently running on the module installed in slot *slot*
required

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

414001

ErrorMessage %FTD-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]

Explanation The logging module failed to save the logging buffer to an external FTP server.

Recommended Action Take applicable actions based on the failed reason:

• Protocol error—Make sure no connectivity issue exists between the FTP server and Firepower Threat Defense device, and that the FTP server can accept the FTP port command and PUT requests.
• Invalid username or password—Make sure that the configured FTP client username and password are correct.
• All other errors—If the problem persists, contact the Cisco TAC.

414002

ErrorMessage %FTD-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]

Explanation The logging module failed to save the logging buffer to system flash.

Recommended Action If the failed reason is caused by insufficient space, check the flash free space, and make sure that the configured limits of the logging flash-size command are set correctly. If the error is a flash file system I/O error, then contact the Cisco TAC for assistance.

414003

ErrorMessage %FTD-3-414003: TCP Syslog Server intf: IP_Address /port not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.

Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted or denied based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted. If not configured, a new connection is denied.

• intf—Interface of the Firepower Threat Defense device to which the server is connected
• IP_Address—IP address of the remote TCP syslog server
• port—Port of the remote TCP syslog server

Recommended Action Validate that the configured TCP syslog server is up. To permit new connections, configure the logging permit-hostdown policy. To deny new connections, do not configure the logging permit-hostdown policy.

414005

ErrorMessage %FTD-3-414005: TCP Syslog Server intf: IP_Address /port connected, New connections are permitted based on logging permit-hostdown policy
Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted.

- \textit{inf} — Interface of the Firepower Threat Defense device to which the server is connected
- \textit{IP \_Address} — IP address of the remote TCP syslog server
- \textit{port} — Port of the remote TCP syslog server

**Recommended Action** None required.

**414006**

**Error Message** %FTD-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.

**Explanation** The logging queue is close to reaching the configured limit, so there is a risk that syslog messages will be discarded.

**Recommended Action** See the "Configuring the Logging Queue" section in the CLI configuration guide for information about how to tune the queue size to avoid this situation. If you want to deny new connections in this case, use the no logging permit-hostdown command. If you want to allow new connections in this case, use the logging permit-hostdown command.

**415020**

**Error Message** %FTD-5-415020: HTTP - matched matched_string in policy-map map_name, a non-ASCII character was matched connection_action from int_type :IP_address /port_num to int_type :IP_address /port_num

**Explanation** A non-ASCII character was found.

- \textit{matched_string}—The matched string is one of the following:
  - The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
  - The actual match command that initiated the message. This string appears when the class map is internal.
    - \textit{map_name} — The name of the policy map
    - \textit{connection_action} — Dropping the connection or resetting the connection
    - \textit{interface_type} — The type of interface (for example, DMZ or outside)
    - \textit{IP \_address} — The IP address of the interface
    - \textit{port_num} — The port number

**Recommended Action** Enter the match \{request | response\} header non-ascii command to correct the problem.

**417001**

**Error Message** %FTD-4-417001: Unexpected event received: number

**Explanation** A process received a signal, but no handler was found for the event.

**Recommended Action** If the problem persists, contact the Cisco TAC.
417004

**Error Message** %FTD-4-417004: Filter violation error: conn number *(string :string )* in *(string )

**Explanation** A client tried to modify a route attribute that the client does not own.

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

417006

**Error Message** %FTD-4-417006: No memory for *(string )* in *(string )* . Handling: *(string )

**Explanation** An operation failed because of low memory, but will be handled with another mechanism.

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

418001

**Error Message** %FTD-4-418001: Through-the-device packet to/from management-only network is denied: *(protocol_string ) from *(interface_name ) *(IP_address ) [*(port )]* [*(idfw_user |FQDN_string ), *(sg_info )*]* to *(interface_name ) *(IP_address ) [*(port )]* [*(idfw_user |FQDN_string ), *(sg_info )*]*

**Explanation** A packet from the specified source to the destination was dropped because it is traversing the Firepower Threat Defense device to and from the management-only network.

- **protocol_string**—TCP, UDP, ICMP, or protocol ID as a number in decimal
- **interface_name**—Interface name
- **IP_address**—IP address
- **port**—Port number
- **sg_info**—Security group name or tag for the specified IP address

**Recommended Action** Determine who is generating this packet and why.

419001

**Error Message** %FTD-4-419001: Dropping TCP packet from *(src_ifc )*(src_IP ) / *(src_port )* to *(dest_ifc )*(dest_IP ) / *(dest_port )* , reason : MSS exceeded, MSS size , data size

**Explanation** The length of the TCP packet exceeded the MSS advertised in the three-way handshake.

- **>src_ifc**—Input interface name
- **>src_IP**—The source IP address of the packet
- **>src_port**—The source port of the packet
- **>dest_ifc**—The output interface name
- **>dest_IP**—The destination IP address of the packet
- **>dest_port**—The destination port of the packet

**Recommended Action** If there is a need to allow packets that exceed the MSS, create a TCP map using the exceed-mss command, as in the following example:

```
ciscoftd# access-list http-list permit tcp any host server_ip eq 80
ciscoftd# class-map http
ciscoftd# match access-list http-list
```
419002

**Error Message**  %FTD-4-419002: Received duplicate TCP SYN from *in_interface* : *src_address* / *src_port* to *out_interface* : *dest_address* / *dest_port* with different initial sequence number.

**Explanation**  A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in_interface**—The input interface
- **src_address**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_interface**—The output interface
- **dest_address**—The destination IP address of the packet
- **dest_port**—The destination port of the packet

**Recommended Action**  None required.

419003

**Error Message**  %FTD-4-419003: Cleared TCP urgent flag from *out_ifc* : *src_ip* / *src_port* to *in_ifc* : *dest_ip* / *dest_port*.

**Explanation**  A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **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

**Recommended Action**  If you need to keep the urgent flag in TCP headers, use the urgent-flag allow command in TCP map configuration mode.

**Error Message**  %FTD-7-419003: Cleared TCP urgent flag.

**Explanation**  This syslog is displayed when urgent flag or urgent pointer of tcp packet is cleared. This could be due to user configuration (tcp-map) or having some value for the urgent pointer in a tcp packet but the urgent flag is not set.

**Recommended Action**  Verify if the tcp-map configurations whether the urget flag is set to clear.
419004

**Error Message**  %FTD-6-419004: TCP connection ID from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port is probed by DCD

**Explanation**
A TCP connection was probed by Dead Connection Detection (DCD) to determine if connection was still valid.

**Recommended Action**  None.

419005

**Error Message**  %FTD-6-419005: TCP connection ID from src_ifc:src_ip/src_port duration hh:mm:ss data bytes, is kept open by DCD as valid connection

**Explanation**
A TCP connection was kept open by Dead Connection Detection (DCD) as a valid connection.

**Recommended Action**  None.

419006

**Error Message**  %FTD-6-419006: TCP connection ID from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port duration hh:mm:ss data bytes, DCD probe was not responded from client/server interface ifc_name

**Explanation**
A TCP connection was closed by Dead Connection Detection (DCD) as it is no longer required.

**Recommended Action**  None.

421005

**Error Message**  %FTD-6-421005: interface_name:IP_address is counted as a user of application

**Explanation** A host has been counted toward the license limit. The specified host was counted as a user of application. The total number of users in 24 hours is calculated at midnight for license validation.

- interface_name—The interface name
- IP_address—The IP address
- application—The CSC SSM

**Recommended Action**  None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

421007

**Error Message**  %FTD-3-421007: TCP|UDP flow from interface_name:IP_address /port to interface_name:IP_address /port is skipped because application has failed.
Explaination A flow was skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

- **IP_address**—The IP address
- **port**—The port number
- **interface_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM

Recommended Action Determine the problem with the service module.

**42204**

Error Message `%FTD-4-42204: IP SLA Monitor number0 : Duplicate event received. Event number number1`

Explanation The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied. This is only a warning message.

- **number0**—The SLA operation number
- **number1**—The SLA operation event ID

Recommended Action If this recurs, enter the `show sla monitor configuration SLA_operation_id` command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact the Cisco TAC and provide the representative with the information that you have, along with information about the application that is configuring and polling the SLA probes.

**42205**

Error Message `%FTD-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.`

Explanation One or more IP SLA monitor probes cannot be scheduled because the system clock was not set.

Recommended Action Make sure that the system clock is functional by using NTP or another mechanism.

**42206**

Error Message `%FTD-4-422006: IP SLA Monitor Probe number : string`

Explanation The IP SLA monitor probe cannot be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

- **number**—The SLA operation ID
- **string**—A string describing the error

Recommended Action Reschedule the failed probe with a valid start time.

**424001**

Error Message `%FTD-4-424001: Packet denied protocol_string intf_in : src_ip / src_port [(idfw_user | FQDN_string ), sg_info ] intf_out : dst_ip / dst_port [(idfw_user | FQDN_string ), sg_info ]]. [Ingress|Egress] interface is in a backup state.`
**Explanation** A packet was dropped because it was traversing the Firepower Threat Defense device to or from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the backup interface command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the Firepower Threat Defense device from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the Firepower Threat Defense device from the primary interface will be denied.

- **protocol_string** — The protocol string; for example, TCP or protocol ID (a decimal number)
- **inf_in** — The input interface name
- **src_ip** — The source IP address of the packet
- **src_port** — The source port of the packet
- **inf_out** — The output interface name
- **dst_ip** — The destination IP address of the packet
- **dst_port** — The destination port of the packet
- **sg_info** — The security group name or tag for the specified IP address

**Recommended Action** Determine the source of the denied packet.

---

**Error Message** %FTD-4-424002: Connection to the backup interface is denied: protocol_string
inf : src_ip / src_port inf : dst_ip / dst_port

**Explanation** A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the backup interface command. If the default route to the primary interface is up, any connection to the Firepower Threat Defense device through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the Firepower Threat Defense device through the primary interface will be denied.

- **protocol_string** — The protocol string; for example, TCP or protocol ID (a decimal number)
- **inf_in** — The input interface name
- **src_ip** — The source IP address of the packet
- **src_port** — The source port of the packet
- **inf_out** — The output interface name
- **dst_ip** — The destination IP address of the packet
- **dst_port** — The destination port of the packet

**Recommended Action** Determine the source of the denied packet.

---

**Error Message** %FTD-6-425001 Redundant interface redundant _interface_name created.

**Explanation** The specified redundant interface was created in the configuration.

- **redundant_interface_name** — Redundant interface name

**Recommended Action** None required.
425002

Error Message  %FTD-6-425002 Redundant interface redundant _interface_name removed.
Explanation The specified redundant interface was removed from the configuration.
  • redundant_interface_name — Redundant interface name
Recommended Action None required.

425003

Error Message  %FTD-6-425003 Interface interface_name added into redundant interface redundant _interface_name.
Explanation The specified physical interface was added to the specified redundant interface as a member interface.
  • interface_name — An interface name
  • redundant_interface_name — Redundant interface name
Recommended Action None required.

425004

Error Message  %FTD-6-425004 Interface interface_name removed from redundant interface redundant _interface_name.
Explanation The specified redundant interface was removed from the specified redundant interface.
  • interface_name — An interface name
  • redundant_interface_name — Redundant interface name
Recommended Action None required.

425005

Error Message  %FTD-5-425005 Interface interface_name become active in redundant interface redundant _interface_name.
Explanation Within a redundant interface, one member interface is the active member. Traffic only passes through the active member interface. The specified physical interface became the active member of the specified redundant interface. Member interface switchover occurs when one of the following is true:
  • The redundant-interface interface-name active-member interface-name command was executed.
  • The active member interface is down, while the standby member interface is up.
  • The standby member interface comes up (from down), while the active member interface remains down.
  • interface_name — An interface name
  • redundant_interface_name — Redundant interface name
Recommended Action Check the status of the member interfaces.
425006

**Error Message** %FTD-3-425006 Redundant interface redundant INTERFACE_NAME switch active member to INTERFACE_NAME failed.

**Explanation** An error occurred when member interface switchover was attempted.

- redundant INTERFACE_NAME — Redundant interface name
- INTERFACE_NAME — An interface name

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

426001

**Error Message** %FTD-6-426001: PORT-CHANNEL: Interface IFC_NAME bundled into EtherChannel interface Port-channel NUM

**Explanation** The interface port-channel NUM or the channel-group NUM mode mode command has been used on a nonexistent port channel.

- IFC_NAME — The EtherChannel interface name
- NUM — The port channel number

**Recommended Action** None required.

426002

**Error Message** %FTD-6-426002: PORT-CHANNEL: Interface IFC_NAME unbundled from EtherChannel interface Port-channel NUM

**Explanation** The no interface port-channel NUM command has been used.

- IFC_NAME — The EtherChannel interface name
- NUM — The port channel number

**Recommended Action** None required.

426003

**Error Message** %FTD-6-426003: PORT-CHANNEL: Interface IFC_NAME1 has become standby in EtherChannel interface Port-channel NUM

**Explanation** The channel-group NUM mode mode command has been used.

- IFC_NAME1 — The EtherChannel interface name
- NUM — The port channel number

**Recommended Action** None required.

426004

**Error Message** %FTD-4-426004: PORT-CHANNEL: Interface IFC_NAME1 is not compatible with IFC_NAME and will be suspended (speed of IFC_NAME1 is X Mbps, Y is 1000 Mbps).
Error Message %FTD-4-426004: Interface ifc_name1 is not compatible with ifc_name1 and will be suspended
(ifc_name1 is Full-duplex, ifc_name1 is Half-duplex)

Explanation The channel-group num mode mode command is executed on a physical interface and there is
a speed or duplex mismatch of this physical interface with that of the port channel.

- ifc_name — The interface that is being added to the port channel
- ifc_name1 — The interface that is already in the port channel and in a bundled state

Recommended Action Do one of the following:

- Change the speed of the physical interface to that of the port channel and execute the channel-group
  num mode mode command again.
- Leave the member interface in a suspended state. When the last active member is removed, then that
  member will try to reestablish LACP on the suspended member.

426101

Error Message %FTD-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP

Explanation A port has been bundled in a span-cluster channel group.

Recommended Action None required.

426102

Error Message %FTD-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP

Explanation A port has been moved to hot-standby state in a span-cluster channel group.

Recommended Action None required.

426103

Error Message %FTD-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP

Explanation A standby port has been selected to move to bundled state in a span-cluster channel group.

Recommended Action None required.

426104

Error Message %FTD-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP

Explanation A bundled port has been unbundled in a span-cluster channel group to obtain space for other
ports to be bundled.

Recommended Action None required.
428002

**Error Message** %FTD-6-428002: WAAS confirmed from in_interface :src_ip_addr/src_port to out_interface :dest_ip_addr/dest_port, inspection services bypassed on this connection.

**Explanation** WAAS optimization was detected on a connection. All layer 7 inspection services, including IPS, are bypassed on WAAS-optimized connections.

**Recommended Action** No action is required if the network includes WAE devices; otherwise, the network administrator should investigate the use of the WAAS option on this connection.

429008

**Error Message** %FTD-4-429008: Unable to respond to VPN query from CX for session 0x%x.

**Reason** %s

**Explanation** The CX sent a VPN session query to the Firepower Threat Defense device, but it did not respond either because of an invalid session ID or another reason. Valid reasons can be any of the following:

- TLV length is invalid
- TLV memory allocation failed
- VPN session query message enqueue failed
- VPN session ID is invalid

**Recommended Action** None required.

430001

This message number was introduced in Release 6.3. It identifies an intrusion event.

For more information about this and other security event messages, see [Security Event Syslog Messages](#), on page 1.

430002

This message number was introduced in Release 6.3. It identifies a connection event logged at the beginning of the connection.

For more information about this and other security event messages, see [Security Event Syslog Messages](#), on page 1.

430003

This message number was introduced in Release 6.3. It identifies a connection event logged at the end of the connection.

For more information about this and other security event messages, see [Security Event Syslog Messages](#), on page 1.
430004

This message number was introduced in Release 6.4. It identifies a file event. See also 430005, on page 191 for file malware events.

For more information about this and other security event messages, see Security Event Syslog Messages, on page 1.

430005

This message number was introduced in Release 6.4. It identifies a file malware event. See also 430004, on page 191 for file events.

For more information about this and other security event messages, see Security Event Syslog Messages, on page 1.

4302310

Error Message
%FTD-5-4302310: SCTP packet received from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port contains unsupported Hostname Parameter.

Explanation
A init/init-ack packet is received with the hostname parameter.

- packet init/init-ack — The message carrying the hostname parameter
- src-ifc — Indicates the ingress interface
- src-ip/src-port — Indicates the Source IP and Port in the packet
- dst-ifc — Indicates the egress interface
- dst_ip/dst_port — Indicates the Source IP and Port in the packet

Recommended Action
Use the real IP addresses of endpoints rather than the hostname. Disable the hostname parameter.

434001

Error Message
%FTD-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address /source port to egress interface :destination IP address /destination port

Explanation
A packet has been dropped because of a fail-close configuration for the module. Your loss of connectivity for all the flows is caused by redirecting them to the module, because the fail-close configuration is designed to drop all the flows if the module is down.

Recommended Action
Try to understand the reason for failure and restore services. Alternatively, you can use the fail-open option even if the card does not recover immediately. Note that in the fail-open configuration, all packets to the module are bypassed if the card status is down.

434004

Error Message
%FTD-5-434004: SFR requested FTD to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally
**Explanation** SourceFire (SFR) has determined not to inspect more traffic of a flow and requests the Firepower Threat Defense device to stop redirecting the flow of traffic to SFR.

**Recommended Action** None Required.

**446003**

**Error Message** %FTD-4-446003: Denied TLS Proxy session from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , UC-IME license is disabled.

**Explanation** The UC-IME license is either on or off. Once enabled, UC-IME can use any number of available TLS sessions, according to the Firepower Threat Defense limit and the K8 export limit.

- **src_int** — The source interface name (inside or outside)
- **src_ip** — The source IP address
- **src_port** — The source port
- **dst_int** — The destination interface name (inside or outside)
- **dst_ip** — The destination IP address
- **dst_port** — The destination port

**Recommended Action** Check to see if UC-IME is disabled. If so, activate it.

**447001**

**Error Message** %FTD-4-447001: ASP DP to CP queue_name was full. Queue length length , limit limit

**Explanation** This message indicates a particular data path (DP) to control point (CP) event queue is full, and one or more multiple enqueue actions have failed. If the event contains a packet block, such as for CP application inspection, the packet will be dropped by the DP, and a counter from the `show asp drop` command will increment. If the event is for punt to CP, a typical counter is the Punt no memory ASP-drop counter.

- **queue** — The name of the DP-CP event queue.
- **length** — The current number of events on the queue.
- **limit** — The maximum number of events that are allowed on the queue.

**Recommended Action** The queue-full condition reflects the fact that the load on the CP has exceeded the CP processing ability, which may or may not be a temporary condition. You should consider reducing the feature load on the CP if this message appears repeatedly. Use the `show asp event dp-cp` command to identify the features that contribute the most load on the event queue.

**448001**

**Error Message** %FTD-4-448001: Denied SRTP crypto session setup on flow from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , licensed K8 SRTP crypto session of limit exceeded

**Explanation** For a K8 platform, the limit of 250 SRTP crypto sessions is enforced. Each pair of SRTP encrypt or decrypt sessions is counted as one SRTP crypto session. A call is counted toward this limit only when encryption or decryption is required for a medium, which means that if the pass-through is set for the call, even if both legs use SRTP, they are not counted toward this limit.

- **src_int** — The source interface name (inside or outside)
- **src_ip** — The source IP address
- `src_port` — The source port
- `dst_int` — The destination interface name (inside or outside)
- `dst_ip` — The destination IP address
- `dst_port` — The destination port
- `limit` — The K8 limit of SRTP crypto sessions (250)

**Recommended Action**  None required. You can set up new SRTP crypto sessions only when existing SRTP crypto sessions have been released.
CHAPTER 6

Syslog Messages 500001 to 520025

This chapter contains the following sections:

• Messages 500001 to 504002, on page 195
• Messages 505001 to 520025, on page 199

Messages 500001 to 504002

This chapter includes messages from 500001 to 504002.

500001

**Error Message** %FTD-5-500001: ActiveX content in java script is modified: src src ip dest dest ip on interface interface name

**Explanation** Ensure the blocking of Java/ActiveX content present in Java script when the policy (filter Java (or) filter ActiveX) is enabled on the Firepower Threat Defense device.

**Recommended Action** None required.

500002

**Error Message** %FTD-5-500002: Java content in java script is modified: src src ip dest dest ip on interface interface name

**Explanation** Ensure the blocking of Java/ActiveX content present in Java script when the policy (filter Java (or) filter ActiveX) is enabled on the Firepower Threat Defense device.

**Recommended Action** None required.

500003

**Error Message** %FTD-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address /source_port to dest_address /dest_port, flags: tcp_flags, on interface interface_name

**Explanation** A header length in TCP was incorrect. Some operating systems do not handle TCP resets (RSTs) correctly when responding to a connection request to a disabled socket. If a client tries to connect to an FTP...
server outside the Firepower Threat Defense device and the FTP server is not listening, then it sends an RST. Some operating systems send incorrect TCP header lengths, which causes this problem. UDP uses ICMP port unreachable messages.

The TCP header length may indicate that it is larger than the packet length, which results in a negative number of bytes being transferred. A negative number appears by a message as an unsigned number, which makes it appear much larger than it would be normally; for example, it may show 4 GB transferred in one second. This message should occur infrequently.

**Recommended Action** None required.

### 500004

**Error Message** %FTD-4-500004: Invalid transport field for protocol=protocol, from source_address /source_port to dest_address /dest_port

**Explanation** An invalid transport number was used, in which the source or destination port number for a protocol is zero. The protocol value is 6 for TCP and 17 for UDP.

**Recommended Action** If these messages persist, contact the administrator of the peer.

### 500005

**Error Message** %FTD-3-500005: Connection terminated for protocol from in_ifc_name :src_address /src_port to out_ifc_name :dest_address /dest_port due to invalid combination of inspections on same flow. Inspect inspect_name is not compatible with filter filter_name.

**Explanation** A connection matched with single or multiple inspection and/or single or multiple filter features that are not allowed to be applied to the same connection.

- **protocol** — The protocol that the connection was using
- **in_ifc_name** — The input interface name
- **src_address** — The source IP address of the connection
- **src_port** — The source port of the connection
- **out_ifc_name** — The output interface name
- **dest_address** — The destination IP address of the connection
- **dest_port** — The destination port of the packet
- **inspect_name** — The inspect or filter feature name
- **filter_name** — The filter feature name

**Recommended Action** Review the class-map, policy-map, service-policy, and/or filter command configurations that are causing the referenced inspection and/or filter features that are matched for the connection. The rules for inspection and filter feature combinations for a connection are as follows:

- The **inspect http [http-policy-map]** and/or **filter url** and/or **filter java** and/or **filter activex** commands are valid.
- The **inspect ftp [ftp-policy-map]** and/or **filter ftp** commands are valid.
- The **filter https** command with any other inspect command or filter command is not valid.

Besides these listed combinations, any other inspection and/or filter feature combinations are not valid.
501101

**Error Message** %FTD-5-501101: User transitioning priv level

**Explanation** The privilege level of a command was changed.

**Recommended Action** None required.

502101

**Error Message** %FTD-5-502101: New user added to local dbase: Uname: user Priv: privilege_level
Encpass: string

**Explanation** A new username record was created, which included the username, privilege level, and encrypted password.

**Recommended Action** None required.

502102

**Error Message** %FTD-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level
Encpass: string

**Explanation** A username record was deleted, which included the username, privilege level, and encrypted password.

**Recommended Action** None required.

502103

**Error Message** %FTD-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level

**Explanation** The privilege level of a user changed.

**Recommended Action** None required.

502111

**Error Message** %FTD-5-502111: New group policy added: name: policy_name Type: policy_type

**Explanation** A group policy was configured using the **group-policy** CLI command.

- **policy_name**—The name of the group policy
- **policy_type**—Either internal or external

**Recommended Action** None required.

502112

**Error Message** %FTD-5-502112: Group policy deleted: name: policy_name Type: policy_type

**Explanation** A group policy has been removed using the **group-policy** CLI command.
• **policy_name**—The name of the group policy
• **policy_type**—Either internal or external

**Recommended Action** None required.

---

### 503001

**Error Message** `%FTD-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason`

**Explanation** An OSPFv2 neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the `log-adjacency-changes` command is configured for the OSPF process.

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

---

### 503002

**Error Message** `%FTD-5-503002: The last key has expired for interface nameif, packets sent using last valid key.`

**Explanation** None of the security associations have a lifetime that include the current system time.

**Recommended Action** Configure a new security association or alter the lifetime of a current security association.

---

### 503003

**Error Message** `%FTD-5-503003: Packet sent | received on interface nameif with expired Key ID key-id.`

**Explanation** The Key ID configured on the interface expired.

**Recommended Action** Configure a new key.

---

### 503004

**Error Message** `%FTD-5-503004: Key ID key-id in key chain key-chain-name does not have a key.`

**Explanation** OSPF has been configured to use cryptographic authentication, however a key or password has not been configured.

**Recommended Action** Configure a new security association or alter the lifetime of a current security association.

---

### 503005

**Error Message** `%FTD-5-503005: Key ID key-id in key chain key-chain-name does not have a cryptographic algorithm.`

**Explanation** OSPF has been configured to use cryptographic authentication, however an algorithm has not been configured.

**Recommended Action** Configure a cryptographic-algorithm for the security association.
503101

**Error Message** %FTD-5-503101: Process d, Nbr i on s from s to s, s

**Explanation** An OSPFv3 neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the `log-adjacency-changes` command is configured for the OSPF process.

**Recommended Action** None required.

504001

**Error Message** %FTD-5-504001: Security context context_name was added to the system

**Explanation** A security context was successfully added to the Firepower Threat Defense device.

**Recommended Action** None required.

504002

**Error Message** %FTD-5-504002: Security context context_name was removed from the system

**Explanation** A security context was successfully removed from the Firepower Threat Defense device.

**Recommended Action** None required.

**Messages 505001 to 520025**

This chapter includes messages from 505001 to 520025.

505001

**Error Message** %FTD-5-505001: Module string one is shutting down. Please wait...

**Explanation** A module is being shut down.

**Recommended Action** None required.

505002

**Error Message** %FTD-5-505002: Module ips is reloading. Please wait...

**Explanation** An IPS module is being reloaded.

**Recommended Action** None required.

505003

**Error Message** %FTD-5-505003: Module string one is resetting. Please wait...

**Explanation** A module is being reset.

**Recommended Action** None required.
505004

**Error Message** %FTD-5-505004: Module string one shutdown is complete.

**Explanation** A module has been shut down.

**Recommended Action** None required.

505005

**Error Message** %FTD-5-505005: Module module_name is initializing control communication. Please wait...

**Explanation** A module has been detected, and the Firepower Threat Defense device is initializing control channel communication with it.

**Recommended Action** None required.

505006

**Error Message** %FTD-5-505006: Module string one is Up.

**Explanation** A module has completed control channel initialization and is in the UP state.

**Recommended Action** None required.

505007

**Error Message** %FTD-5-505007: Module module_id is recovering. Please wait...

**Error Message** %FTD-5-505007: Module prod_id in slot slot_num is recovering. Please wait...

**Explanation** A software module is being recovered with the `sw-module module service-module-name recover boot` command, or a hardware module is being recovered with the `hw-module module slotnum recover boot` command.

- **module_id** — The name of the software services module.
- **prod_id** — The product ID string.
- **slot_num** — The slot in which the hardware services module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

**Recommended Action** None required.

505008

**Error Message** %FTD-5-505008: Module module_id software is being updated to newver (currently ver )

**Error Message** %FTD-5-505008: Module module_id in slot slot_num software is being updated to newver (currently ver )

**Explanation** The services module software is being upgraded. The update is proceeding normally.

- **module_id** — The name of the software services module
- **slot_num** — The slot number that contains the hardware services module
• >newver — The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
• >ver — The current version number of the software on the module (for example, 1.0(1)0)

Recommended Action None required.

505009

ErrorMessage %FTD-5-505009: Module string one software was updated to newver

Explanation The 4GE SSM module software was successfully upgraded.
  • string one — The text string that specifies the module
  • newver — The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
  • ver — The current version number of the software on the module (for example, 1.0(1)0)

Recommended Action None required.

505010

ErrorMessage %FTD-5-505010: Module in slot slot removed.

Explanation An SSM was removed from the Firepower Threat Defense device chassis.
  • slot — The slot from which the SSM was removed

Recommended Action None required.

505011

ErrorMessage %FTD-1-505011: Module ips, data channel communication is UP.

Explanation The data channel communication recovered from a DOWN state.

Recommended Action None required.

505012

ErrorMessage %FTD-5-505012: Module module_id, application stopped application, version version

ErrorMessage %FTD-5-505012: Module prod_id in slot slot_num, application stopped application, version version

Explanation An application was stopped or removed from a services module. This may occur when the services module upgraded an application or when an application on the services module was stopped or uninstalled.
  • module_id — The name of the software services module
  • prod_id — The product ID string for the device installed in the hardware services module
  • slot_num — The slot in which the application was stopped
  • application — The name of the application stopped
  • version — The application version stopped
Recommended Action  If an upgrade was not occurring on the 4GE SSM or the application was not intentionally stopped or uninstalled, review the logs from the 4GE SSM to determine why the application stopped.

505013

Error Message  %FTD-5-505013: Module module_id application changed from: application version to: newapplication version newversion .

Error Message  %FTD-5-505013: Module prod_id in slot slot_num application changed from: application version to: newapplication version newversion .

Explanation An application version changed, such as after an upgrade. A software update for the application on the services module is complete.

- module_id — The name of the software services module
- application — The name of the application that was upgraded
- version — The application version that was upgraded
- prod_id — The product ID string for the device installed in the hardware services module
- slot_num — The slot in which the application was upgraded
- application — The name of the application that was upgraded
- version — The application version that was upgraded
- newapplication — The new application name
- newversion — The new application version

Recommended Action  Verify that the upgrade was expected and that the new version is correct.

505014

Error Message  %FTD-1-505014: Module module_id , application down name , version version reason

Error Message  %FTD-1-505014: Module prod_id in slot slot_num , application down name , version version reason

Explanation The application running on the module is disabled.

- module_id — The name of the software services module
- prod_id — The product ID string for the device installed in the hardware services module
- slot_num — The slot in which the application was disabled. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- name — Application name (string)
- application — The name of the application that was upgraded
- version — The application version (string)
- reason — Failure reason (string)

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

505015

Error Message  %FTD-1-505015: Module module_id , application up application , version version
### Error Message

**%FTD-1-505015:** Module `prod_id` in slot `slot_num`, application up `application`, version `version`

**Explanation**  The application running on the SSM in slot `slot_num` is up and running.

- **module_id**—The name of the software services module
- **prod_id**—The product ID string for the device installed in the hardware services module
- **slot_num**—The slot in which the application is running. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- **application**—The application name (string)
- **version**—The application version (string)

**Recommended Action**  None required.

### 505016

**Error Message**  `%FTD-3-505016:` Module `module_id` application changed from: `name version version` state `state` to: `name version version` state `state`.

**Error Message**  `%FTD-3-505016:` Module `prod_id` in slot `slot_num` application changed from: `name version version` state `state` to: `name version version` state `state`.

**Explanation**  The application version or a name change was detected.

- **module_id**—The name of the software services module
- **prod_id**—The product ID string for the device installed in the hardware services module
- **slot_num**—The slot in which the application changed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- **name**—Application name (string)
- **version**—The application version (string)
- **state**—Application state (string)
- **application**—The name of the application that changed

**Recommended Action**  Verify that the change was expected and that the new version is correct.

### 506001

**Error Message**  `%FTD-5-506001:` `event_source_string event_string`

**Explanation**  The status of a file system has changed. The event and the source of the event that caused a file system to become available or unavailable appear. Examples of sources and events that can cause a file system status change are as follows:

- External CompactFlash removed
- External CompactFlash inserted
- External CompactFlash unknown event

**Recommended Action**  None required.
507001

Error Message %FTD-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside :dest_address /dest_port - reassembly limit of limit bytes exceeded

Explanation The assembly buffer limit was exceeded during TCP segment reassembly.

- source_address/source_port—The source IP address and the source port of the packet initiating the connection
- dest_address/dest_port—The destination IP address and the destination port of the packet initiating the connection
- interface_inside—The name of the interface on which the packet which initiated the connection arrives
- interface_outside—The name of the interface on which the packet which initiated the connection exits
- limit—The configured embryonic connection limit for the traffic class

Recommended Action None required.

507002

Error Message %FTD-4-507002: Data copy in proxy-mode exceeded the buffer limit

Explanation An operational error occurred during processing of a fragmented TCP message.

Recommended Action None required.

507003

Error Message %FTD-3-507003: The flow of type protocol from the originating interface: src_ip /src_port to dest_if :dest_ip /dest_port terminated by inspection engine, reason-

Explanation The TCP proxy or session API terminated a connection for various reasons, which are provided in the message.

- protocol—The protocol for the flow
- src_ip—The source IP address for the flow
- src_port—The name of the source port for the flow
- dest_if—The destination interface for the flow
- dest_ip—The destination IP address for the flow
- dest_port—The destination port for the flow
- reason—The description of why the flow is being terminated by the inspection engine. Valid reasons include:
  - Failed to create flow
  - Failed to initialize session API
  - Filter rules installed/matched are incompatible
  - Failed to consolidate new buffer data with original
  - Reset unconditionally
  - Reset based on “service reset inbound” configuration
  - Disconnected, dropped packet
- Packet length changed
- Reset reflected back to sender
- Proxy inspector reset unconditionally
- Proxy inspector drop reset
- Proxy inspector received data after FIN
- Proxy inspector disconnected, dropped packet
- Inspector reset unconditionally
- Inspector drop reset
- Inspector received data after FIN
- Inspector disconnected, dropped packet
- Could not buffer unprocessed data
- Session API proxy forward failed
- Conversion of inspect data to session data failed

**Recommended Action** None required.

**509001**

**Error Message** %FTD-5-509001: Connection attempt from src_intf : src_ip / src_port (((idfw_user | FQDN_string ), sg_info )) to dst_intf : dst_ip / dst_port (((idfw_user | FQDN_string ), sg_info )) was prevented by "no forward" command.

**Explanation** The **no forward interface** command was entered to block traffic from the source interface to the destination interface given in the message. This command is required on low-end platforms to allow the creation of interfaces beyond the licensed limit.

- **src_intf**—The name of the source interface to which the **no forward interface** command restriction applies
- **dst_intf**—The name of the destination interface to which the **no forward interface** command restriction applies
- **sg_info**—The security group name or tag for the specified IP address

**Recommended Action** Upgrade the license to remove the requirement of this command on low-end platforms, then remove the command from the configuration.

**520001**

**Error Message** %FTD-3-520001: error_string

**Explanation** A malloc failure occurred in ID Manager. The error string can be either of the following:

- Malloc failure—id_reserve
- Malloc failure—id_get

**Recommended Action** Contact the Cisco TAC.
520002

Error Message %FTD-3-520002: bad new ID table size

Explanation A bad new table request to the ID Manager occurred.

Recommended Action Contact the Cisco TAC.

520003

Error Message %FTD-3-520003: bad id in error_string (id: 0xid_num)

Explanation An ID Manager error occurred. The error string may be any of the following:

- id_create_new_table (no more entries allowed)
- id_destroy_table (bad table ID)
- id_reserve
- id_reserve (bad ID)
- id_reserve: ID out of range
- id_reserve (unassigned table ID)
- id_get (bad table ID)
- id_get (unassigned table ID)
- id_get (out of IDs!)
- id_to_ptr
- id_to_ptr (bad ID)
- id_to_ptr (bad table ID)
- id_get_next_id_ptr (bad table ID)
- id_delete
- id_delete (bad ID)
- id_delete (bad table key)

Recommended Action Contact the Cisco TAC.

520004

Error Message %FTD-3-520004: error_string

Explanation An id_get was attempted at the interrupt level.

Recommended Action Contact the Cisco TAC.

520005

Error Message %FTD-3-520005: error_string

Explanation An internal error occurred with the ID Manager.

Recommended Action Contact the Cisco TAC.
520010

Error Message: %FTD-3-520010: Bad queue elem - qelem_ptr : flink flink_ptr , blink blink_ptr , flink-blink flink_blink_ptr , blink-flink blink_flink_ptr

Explanation: An internal software error occurred, which can be any of the following:
- `qelem_ptr` — A pointer to the queue data structure
- `flink_ptr` — A pointer to the forward element of the queue data structure
- `blink_ptr` — A pointer to the backward element of the queue data structure
- `flink_blink_ptr` — A pointer to the forward element’s backward pointer of the queue data structure
- `blink_flink_ptr` — A pointer to the backward element’s forward pointer of the queue data structure

Recommended Action: Contact the Cisco TAC.

520011

Error Message: %FTD-3-520011: Null queue elem

Explanation: An internal software error occurred.

Recommended Action: Contact the Cisco TAC.

520013

Error Message: %FTD-3-520013: Regular expression access check with bad list acl_ID

Explanation: A pointer to an access list is invalid.

Recommended Action: The event that caused this message to be issued should not have occurred. It can mean that one or more data structures have been overwritten. If this message recurs, and you decide to report it to your TAC representative, you should copy the text of the message exactly as it appears and include the associated stack trace. Because access list corruption may have occurred, a TAC representative should verify that access lists are functioning correctly.

520020

Error Message: %FTD-3-520020: No memory available

Explanation: The system is out of memory.

Recommended Action: Try one of the following actions to correct the problem:
- Reduce the number of routes accepted by this router.
- Upgrade hardware.
- Use a smaller subset image on run-from-RAM platforms.

520021

Error Message: %FTD-3-520021: Error deleting trie entry, error_message

Explanation: A software programming error occurred. The error message can be any of the following:
- Inconsistent annotation
• Couldn't find our annotation
• Couldn't find deletion target

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

### 520022

**Error Message** %FTD-3-520022: Error adding mask entry, *error_message*

**Explanation** A software or hardware error occurred. The error message can be any of the following:

- Mask already in tree
- Mask for route not entered
- Non-unique normal route, mask not entered

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

### 520023

**Error Message** %FTD-3-520023: Invalid pointer to head of tree, 0x *radix_node_ptr*

**Explanation** A software programming error occurred.

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

### 520024

**Error Message** %FTD-3-520024: Orphaned mask #*radix_mask_ptr*, reccount= *radix_mask_ptr’s ref count at #*radix_node_address*, next= #*radix_node_nxt*

**Explanation** A software programming error occurred.

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

### 520025

**Error Message** %FTD-3-520025: No memory for radix initialization: *err_msg*

**Explanation** The system ran out of memory during initialization. This should only occur if an image is too large for the existing dynamic memory. The error message can be either of the following: Initializing leaf nodes, Mask housekeeping

**Recommended Action** Use a smaller subset image or upgrade hardware.
CHAPTER 7

Syslog Messages 602101 to 622102

This chapter contains the following sections:

- Messages 602101 to 609002, on page 209
- Messages 610101 to 622102, on page 217

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 Firepower 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 An 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 Firepower Threat Defense DHCP client successfully obtained an IP address from a DHCP server. The dhcpc command statement allows the Firepower 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 Firepower 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)
604104

Explanation The Firepower 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 Firepower 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.

---

**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.

---

**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.

---

**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 Firepower 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.

---

**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 SCCP 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**

**ErrorMessage**  %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**

**ErrorMessage**  %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**

**ErrorMessage**  %FTD-6-611101: User authentication succeeded: IP, **IP address** : Uname: **user**

**Explanation**  User authentication succeeded when accessing the Firepower 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.
611102

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

**Explanation** User authentication failed when attempting to access the Firepower 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 Firepower 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.

**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

**Explaination** 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

**Explaination** The VPN client policy for DHCP was installed.

**Recommended Action** None required.

---

**611306**

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

**Explaination** 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

**Explaination** 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

**Explaination** 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

**Explaination** 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: VNPClient: Backup Server List: reason

**Explanation** When the Firepower Threat Defense device is an Easy VPN remote device, the Easy VPN server downloaded a list of backup servers to the Firepower Threat Defense device. This list overrides any backup servers that you have configured locally. If the downloaded list is empty, then the Firepower 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: VNPClient: Backup Server List Error: reason

**Explanation** When the Firepower Threat Defense device is an Easy VPN remote device, and the Easy VPN server downloads a backup server list to the Firepower Threat Defense device, the list includes an invalid IP address or a hostname. The Firepower 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: VNPClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address

**Explanation** When the Firepower Threat Defense device is an Easy VPN remote device, the master server of the load balancing cluster redirected the Firepower 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

**Explanation** When the Firepower 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 Firepower 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 Firepower 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: 

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

- **IP_address**—The server IP address to which the Firepower Threat Defense device sends authentication requests.
- **port**—The server port to which the Firepower 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 Firepower Threat Defense device is an Easy VPN remote device, the downloaded VPN policy disabled IUA for users on the Firepower Threat Defense inside network.

**Recommended Action** None required.
611320

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

**Explanation** When the Firepower 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 Firepower Threat Defense device.

**Recommended Action** None required.

611321

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

**Explanation** When the Firepower 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 Firepower 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 mechanisms to authenticate the Firepower 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 Firepower 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 Firepower 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 Area 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 Firepower 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 Firepower 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 persist, 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.
Syslog Messages 701001 to 714011

This chapter contains the following sections:

- Messages 701001 to 713109, on page 235
- Messages 713112 to 714011, on page 252

Messages 701001 to 713109

This section includes messages from 701001 to 713109.

701001

Error Message  %FTD-7-701001: alloc_user() out of Tcp_user objects
Explanation A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.
Recommended Action Enable Flood Defender with the floodguard enable command.

701002

Error Message  %FTD-7-701002: alloc_user() out of Tcp_proxy objects
Explanation A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.
Recommended Action Enable Flood Defender with the floodguard enable command.

703001

Error Message  %FTD-7-703001: H.225 message received from interface_name :IP_address /port to interface_name :IP_address /port is using an unsupported version number
Explanation The Firepower Threat Defense device received an H.323 packet with an unsupported version number. The Firepower Threat Defense device might reencode the protocol version field of the packet to the highest supported version.
Recommended Action Use the version of H.323 that the Firepower Threat Defense device supports in the VoIP network.
703002

**Error Message** %FTD-7-703002: Received H.225 Release Complete with newConnectionNeeded for `interface_name :IP_address` to `interface_name :IP_address /port`

**Explanation** The Firepower Threat Defense device received the specified H.225 message, and the Firepower Threat Defense device opened a new signaling connection object for the two specified H.323 endpoints.

**Recommended Action** None required.

703008

**Error Message** %FTD-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d

**Explanation** This message indicates that an outside endpoint requested an incoming call to an inside host and wants the inside host to send FACILITY message before SETUP message towards Gatekeeper and wants to follow H.460.18.

**Recommended Action** Ensure that the setup indeed intends to allow early FACILITY message before SETUP message for incoming H.323 calls as described in H.640.18.

709001, 709002

**Error Message** %FTD-7-709001: FO replication failed: cmd=`command` returned=`code`

**Error Message** %FTD-7-709002: FO unreplicable: cmd=`command`

**Explanation** Failover messages that only appear during the development debugging and testing phases.

**Recommended Action** None required.

709003

**Error Message** %FTD-1-709003: (Primary) Beginning configuration replication: Sending to mate.

**Explanation** A failover message that appears when the active unit starts replicating its configuration to the standby unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

709004

**Error Message** %FTD-1-709004: (Primary) End Configuration Replication (ACT)

**Explanation** A failover message that appears when the active unit completes replication of its configuration on the standby unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

709005

**Error Message** %FTD-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
**Explanation** The standby Firepower Threat Defense device received the first part of the configuration replication from the active Firepower Threat Defense device. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

**709006**

**Error Message** %FTD-1-709006: (Primary) End Configuration Replication (STB)

**Explanation** A failover message that appears when the standby unit completes replication of a configuration sent by the active unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

**709007**

**Error Message** %FTD-2-709007: Configuration replication failed for command

**Explanation** A failover message that appears when the standby unit is unable to complete replication of a configuration sent by the active unit. The command that caused the failure appears at the end of the message.

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

**709008**

**Error Message** %FTD-4-709008: (Primary | Secondary) Configuration sync in progress. Command: `command` executed from (terminal/http) will not be replicated to or executed by the standby unit.

**Explanation** A command was issued during the configuration sync, which triggered an interactive prompt to indicate that this command would not be issued on the standby unit. To continue, note that the command will be issued on the active unit only and will not be replicated on the standby unit.

- Primary | Secondary—The device is either primary or secondary
- `command`—The command issued while the configuration sync is in progress
- terminal/http—Issued from the terminal or via HTTP.

**Recommended Action** None.

**710001**

**Error Message** %FTD-7-710001: TCP access requested from `source_address` `/source_port` to `interface_name` :`dest_address` `/service`

**Explanation** The first TCP packet destined to the Firepower Threat Defense device requests to establish a TCP session. This packet is the first SYN packet of the three-way handshake. This message appears when the respective (Telnet, HTTP, or SSH) has permitted the packet. However, the SYN cookie verification is not yet completed and no state is reserved.

**Recommended Action** None required.
**ErrorMessage** %FTD-7-710002: {TCP|UDP} access permitted from source_address /source_port to interface_name :dest_address /service

**Explanation** For a TCP connection, the second TCP packet destined for the Firepower Threat Defense device requested to establish a TCP session. This packet is the final ACK of the three-way handshake. The respective (Telnet, HTTP, or SSH) has permitted the packet. Also, the SYN cookie verification was successful and the state is reserved for the TCP session.

For a UDP connection, the connection was permitted. For example, the module received an SNMP request from an authorized SNMP management station, and the request has been processed. This message is rate limited to one message every 10 seconds.

**Recommended Action** None required.

---

**ErrorMessage** %FTD-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name :dest_IP/service

**Explanation** The Firepower Threat Defense device denied an attempt to connect to the interface service. For example, the Firepower Threat Defense device received an SNMP request from an unauthorized SNMP management station. If this message appears frequently, it can indicate an attack.

For example:

%FTD-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to outside:95.1.1.13/1005

**Recommended Action** Use the show run http, show run ssh, or show run telnet commands to verify that the Firepower Threat Defense device is configured to permit the service access from the host or network.

---

**ErrorMessage** %FTD-7-710004: TCP connection limit exceeded from Src_ip /Src_port to In_name :Dest_ip /Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)

**Explanation** The maximum number of Firepower Threat Defense management connections for the service was exceeded. The Firepower Threat Defense device permits at most five concurrent management connections per management service. Alternatively, an error may have occurred in the to-the-box connection counter.

- **Src_ip** — The source IP address of the packet
- **Src_port** — The source port of the packet
- **In_ifc** — The input interface
- **Dest_ip** — The destination IP address of the packet
- **Dest_port** — The destination port of the packet
- **Curr_conn** — The number of current to-the-box admin connections
- **Conn_lmt** — The connection limit

**Recommended Action** From the console, use the kill command to release the unwanted session. If the message was generated because of an error in the to-the-box counter, run the show conn all command to display connection details.
**710005**

**Error Message** %FTD-7-710005: {TCP|UDP|SCTP} request discarded from source_address /source_port to interface_name :dest_address /service

**Explanation** The Firepower Threat Defense device does not have a UDP server that services the UDP request. Also, a TCP packet that does not belong to any session on the Firepower Threat Defense device may have been discarded. In addition, this message appears (with the SNMP service) when the Firepower Threat Defense device receives an SNMP request with an empty payload, even if it is from an authorized host. When the service is SNMP, this message occurs a maximum of once every 10 seconds so that the log receiver is not overwhelmed. This message is also applicable for SCTP packets.

**Recommended Action** In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

---

**710006**

**Error Message** %FTD-7-710006: protocol request discarded from source_address to interface_name :dest_address

**Explanation** The Firepower Threat Defense device does not have an IP server that services the IP protocol request; for example, the Firepower Threat Defense device receives IP packets that are not TCP or UDP, and the Firepower Threat Defense device cannot service the request.

**Recommended Action** In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

---

**710007**

**Error Message** %FTD-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500

**Explanation** The Firepower Threat Defense device received NAT-T keepalive messages.

**Recommended Action** None required.

---

**711001**

**Error Message** %FTD-7-711001: debug_trace_msg

**Explanation** You have entered the **logging debug-trace** command for the logging feature. When the **logging debug-trace** command is enabled, all debugging messages will be redirected to the message for processing. For security reasons, the message output must be encrypted or sent over a secure out-of-band network.

**Recommended Action** None required.

---

**711002**

**Error Message** %FTD-4-711002: Task ran for elapsed_time msecs, process = process_name , PC = PC Tracebeback = traceback
**Explanation** A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- **PC**—Instruction pointer of the CPU hogging process
- **traceback**—Stack trace of the CPU hogging process, which can include up to 12 addresses

**Recommended Action** None required.

**711003**

**Error Message** FTD-7-711003: Unknown/Invalid interface identifier (vpifnum) detected.

**Explanation** An internal inconsistency that should not occur during normal operation has occurred. However, this message is not harmful if it rarely occurs. If it occurs frequently, it might be worthwhile debugging.

- **vpifnum**—The 32-bit value corresponding to the interface

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

**711004**

**Error Message** %FTD-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call_stack

**Explanation** A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- **msec**—Length of the detected CPU hog in milliseconds
- **process_name**—Name of the hogging process
- **pc**—Instruction pointer of the CPU hogging process
- **call stack**—Stack trace of the CPU hogging process, which can include up to 12 addresses

**Recommended Action** None required.

**711005**

**Error Message** %FTD-5-711005: Traceback: call_stack

**Explanation** An internal software error that should not occur has occurred. The device can usually recover from this error, and no harmful effect to the device results.

- **call_stack**—The EIPs of the call stack

**Recommended Action** Contact the Cisco TAC.

**711006**

**Error Message** %FTD-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string.

**Explanation** CPU profiling has started.

- **n-samples**—The specified number of CPU profiling samples
- **reason-string**—The possible values are:
“CPU utilization passed cpu-utilization %”
“Process process-name CPU utilization passed cpu-utilization %”
Recommended Action “None specified”
Recommended Action Collect CPU profiling results and provide them to Cisco TAC.

713004
Error Message %FTD-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num, for Peer IP_address ignored
Explanation The Firepower Threat Defense device has received an IKE packet from a remote entity trying to initiate a tunnel. Because the Firepower Threat Defense device is scheduled for a reboot or shutdown, it does not allow any more tunnels to be established. The IKE packet is ignored and dropped.
Recommended Action None required.

713201
Error Message %FTD-5-713201: Duplicate Phase Phase packet detected. Action
Explanation The Firepower Threat Defense device has received a duplicate of a previous Phase 1 or Phase 2 packet, and will transmit the last message. A network performance or connectivity issue may have occurred, in which the peer is not receiving sent packets in a timely manner.
• Phase—Phase 1 or 2
• Action—Retransmitting last packet, or No last packet to transmit.
Recommended Action Verify network performance or connectivity.

713202
Error Message %FTD-6-713202: Duplicate IP_addr packet detected.
Explanation The Firepower Threat Defense device has received a duplicate first packet for a tunnel that the Firepower Threat Defense device is already aware of and negotiating, which indicates that the Firepower Threat Defense device probably received a retransmission of a packet from the peer.
• IP_addr—The IP address of the peer from which the duplicate first packet was received
Recommended Action None required, unless the connection attempt is failing. If this is the case, debug further and diagnose the problem.

713006
Error Message %FTD-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
Explanation The Firepower Threat Defense device does not know about the received message ID. The message ID is used to identify a specific IKE Phase 2 negotiation. An error condition on the Firepower Threat Defense device may have occurred, and may indicate that the two IKE peers are out-of-sync.
Recommended Action None required.
713008

Error Message %FTD-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel

Explanation A key ID value was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using preshared keys authentication. This is an invalid value, and the session is rejected. Note that the key ID specified would never work because a group name of that size cannot be created in the Firepower Threat Defense device.

Recommended Action Make sure that the client peer (most likely an Altiga remote access client) specifies a valid group name. Notify the user to change the incorrect group name on the client. The current maximum length for a group name is 32 characters.

713009

Error Message %FTD-3-713009: OU in DN in ID payload too big for Certs IKE tunnel

Explanation An OU value in the DN was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using Certs authentication. This OU is skipped, and another OU or other criteria may find a matching group.

Recommended Action For the client to be able to use an OU to find a group in the Firepower Threat Defense device, the group name must be a valid length. The current maximum length of a group name is 32 characters.

713010

Error Message %FTD-5-713010: IKE area: failed to find entry for message Id message_number

An attempt was made to locate a conn_entry (IKE phase 2 structure that corresponds to an IPsec SA) using the unique message ID, which failed. The internal structure was not found, which may occur if a session was terminated in a nonstandard way, but it is more likely that an internal error occurred.

If this problem persists, investigate the peer.

713012

Error Message %FTD-3-713012: Unknown protocol (protocol ). Not adding SA w/spi=SPI value

Explanation An illegal or unsupported IPsec protocol has been received from the peer.

Recommended Action Check the ISAKMP Phase 2 configuration on the peer(s) to make sure it is compatible with the Firepower Threat Defense device.

713014

Error Message %FTD-3-713014: Unknown Domain of Interpretation (DOI): DOI value

Explanation The ISAKMP DOI received from the peer is unsupported.

Recommended Action Check the ISAKMP DOI configuration on the peer.
713016

Error Message  %FTD-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
Explanation  The ID received from the peer is unknown. The ID can be an unfamiliar valid ID or an invalid or corrupted ID.
Recommended Action  Check the configuration on the headend and peer.

713017

Error Message  %FTD-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
Explanation  The Phase 1 or Phase 2 ID received from the peer is legal, but not supported.
Recommended Action  Check the configuration on the headend and peer.

713018

Error Message  %FTD-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
Explanation  Tn internal software error has occurred.
Recommended Action  If the problem persists, contact the Cisco TAC.

713020

Error Message  %FTD-3-713020: No Group found by matching OU(s) from ID payload: OU_value
Explanation  Tn internal software error has occurred.
Recommended Action  If the problem persists, contact the Cisco TAC.

713022

Error Message  %FTD-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
Explanation  group exists in the group database with the same name as the value (key ID or IP address) specified by the peer.
Recommended Action  Verify the configuration on the peer.

713024

Error Message  %FTD-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
Explanation  The Firepower Threat Defense device has received the Phase 2 local proxy ID payload from the remote peer.
Recommended Action  None required.
713025

**Error Message** %FTD-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port

**Explanation** The Firepower Threat Defense device has received the Phase 2 local proxy ID payload from the remote peer.

**Recommended Action** None required.

713028

**Error Message** %FTD-7-713028:Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port

**Explanation** The Firepower Threat Defense device has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

**Recommended Action** None required.

713029

**Error Message** %FTD-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port

**Explanation** The Firepower Threat Defense device has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

**Recommended Action** None required.

713032

**Error Message** %FTD-3-713032: Received invalid local Proxy Range IP_address - IP_address

**Explanation** The local ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

713033

**Error Message** %FTD-3-713033: Received invalid remote Proxy Range IP_address - IP_address

**Explanation** The remote ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

713034

**Error Message** %FTD-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
713035

**Explanation** The local IP proxy subnet data has been received in the Phase 2 ID payload.

**Recommended Action** None required.

**Error Message** %FTD-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port

**Explanation** The remote IP proxy subnet data has been received in the Phase 2 ID payload.

**Recommended Action** None required.

713039

**Error Message** %FTD-7-713039: Send failure: Bytes (number), Peer: IP_address

**Explanation** An internal software error has occurred, and the ISAKMP packet cannot be transmitted.

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

713040

**Error Message** %FTD-7-713040: Could not find connection entry and can not encrypt: msgid message_number

**Explanation** An internal software error has occurred, and a Phase 2 data structure cannot be found.

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

713041

**Error Message** %FTD-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number, IKE Peer IP_address local Proxy Address IP_address, remote Proxy Address IP_address, Crypto map (crypto map tag)

**Explanation** Firepower Threat Defense device is negotiating a tunnel as the initiator.

**Recommended Action** None required.

713042

**Error Message** %FTD-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address

**Explanation** The IPsec fast path processed a packet that triggered IKE, but the IKE policy lookup failed. This error may be timing related. The ACLs that triggered IKE might have been deleted before IKE processed the initiation request. This problem will most likely correct itself.

**Recommended Action** If the condition persists, check the L2L configuration, paying special attention to the type of ACL associated with crypto maps.
713043

Error Message %FTD-3-713043: Cookie/peer address IP_address session already in progress
Explanation IKE has been triggered again while the original tunnel is in progress.
Recommended Action None required.

713048

Error Message %FTD-3-713048: Error processing payload: Payload ID: id
Explanation A packet has been received with a payload that cannot be processed.
Recommended Action If this problem persists, a misconfiguration may exist on the peer.

713049

Error Message %FTD-5-713049: Security negotiation complete for tunnel_type type (group_name)
Initiator / Responder, Inbound SPI = SPI, Outbound SPI = SPI
Explanation An IPsec tunnel has been started.
Recommended Action None required.

713050

Error Message %FTD-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address
Explanation An IPsec tunnel has been terminated. Possible termination reasons include:
  • IPsec SA Idle Timeout
  • IPsec SA Max Time Exceeded
  • Administrator Reset
  • Administrator Reboot
  • Administrator Shutdown
  • Session Disconnected
  • Session Error Terminated
  • Peer Terminate
Recommended Action None required.

713052

Error Message %FTD-7-713052: User (user) authenticated.
Explanation remote access user was authenticated.
Recommended Action None required.
**713056**

**Error Message** `%FTD-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!

**Explanation** The IPsec SA was not found.

**Recommended Action** If this is a remote access tunnel, check the group and user configuration, and verify that a tunnel group and group policy have been configured for the specific user group. For externally authenticated users and groups, check the returned authentication attributes.

---

**713060**

**Error Message** `%FTD-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.

**Explanation** The user is configured for a different group than what was sent in the IPsec negotiation.

**Recommended Action** If you are using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the Firepower Threat Defense device. If you are using digital certificates, the group is dictated either by the OU field of the certificate, or the user automatically defaults to the remote access default group.

---

**713061**

**Error Message** `%FTD-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst:dest_address!

**Explanation** The Firepower Threat Defense device was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Firepower Threat Defense device. This is most likely a misconfiguration.

**Recommended Action** Check the protected network configuration in the crypto ACLs on both sides and make sure that the local net on the initiator is the remote net on the responder and vice-versa. Pay special attention to wildcard masks, and host addresses versus network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or red networks.

---

**713062**

**Error Message** `%FTD-3-713062: IKE Peer address same as our interface address IP_address!

**Explanation** The IP address configured as the IKE peer is the same as the IP address configured on one of the Firepower Threat Defense IP interfaces.

**Recommended Action** Check the L2L and IP interface configurations.

---

**713063**

**Error Message** `%FTD-3-713063: IKE Peer address not configured for destination IP_address!

**Explanation** The IKE peer address is not configured for an L2L tunnel.

**Recommended Action** Check the L2L configuration.
**713065**

**Error Message** %FTD-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute

**Explanation** An internal software error has occurred.

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

**713066**

**Error Message** %FTD-7-713066: IKE Remote Peer configured for SA: SA_name

**Explanation** The crypto policy settings of the peer have been configured.

**Recommended Action** None required.

**713068**

**Error Message** %FTD-5-713068: Received non-routine Notify message: notify_type (notify_value)

**Explanation** Notification messages that caused this event are not explicitly handled in the notify processing code.

**Recommended Action** Examine the specific reason to determine the action to take. Many notification messages indicate a configuration mismatch between the IKE peers.

**713072**

**Error Message** %FTD-3-713072: Password for user (user) too long, truncating to number characters

**Explanation** The password of the user is too long.

**Recommended Action** Correct password lengths on the authentication server.

**713073**

**Error Message** %FTD-5-713073: Responder forcing change of Phase 1 /Phase 2 rekeying duration from larger_value to smaller_value seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.

**Recommended Action** None required.

**713074**

**Error Message** %FTD-5-713074: Responder forcing change of IPsec rekeying duration from larger_value to smaller_value Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.
**Recommended Action** None required.

**713075**

**Error Message** %FTD-5-713075: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

**Recommended Action** None required.

**713076**

**Error Message** %FTD-5-713076: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

**Recommended Action** None required.

**713078**

**Error Message** %FTD-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value

**Explanation** An internal software error has occurred while processing modecfg attributes.

**Recommended Action** Disable any unnecessary tunnel group attributes, or shorten any text messages that are excessively long. If the problem persists, contact the Cisco TAC.

**713081**

**Error Message** %FTD-3-713081: Unsupported certificate encoding type encoding_type

**Explanation** One of the loaded certificates is unreadable, and may be an unsupported encoding scheme.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

**713082**

**Error Message** %FTD-3-713082: Failed to retrieve identity certificate

**Explanation** The identity certificate for this tunnel cannot be found.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

**713083**

**Error Message** %FTD-3-713083: Invalid certificate handle

**Explanation** The identity certificate for this tunnel cannot be found.
**Recommended Action** Check the configuration of digital certificates and trustpoints.

**713084**

**Error Message** %FTD-3-713084: Received invalid phase 1 port value (`port`) in ID payload

**Explanation** The port value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 500 (ISAKMP is also known as IKE).

**Recommended Action** Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

**713085**

**Error Message** %FTD-3-713085: Received invalid phase 1 protocol (`protocol`) in ID payload

**Explanation** The protocol value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 17 (UDP).

**Recommended Action** Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

**713086**

**Error Message** %FTD-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))

**Explanation** A certificate payload was received, but our internal certificate handle indicates that we do not have an identity certificate. The certificate handle was not obtained through a normal enrollment method. One likely reason this can happen is that the authentication method is not made through RSA or DSS signatures, although the IKE SA negotiation should fail if each side is misconfigured.

**Recommended Action** Check the trustpoint and ISAKMP configuration settings on the Firepower Threat Defense device and its peer.

**713088**

**Error Message** %FTD-3-713088: Set Cert filehandle failure: no IPsec SA in group `group_name`

**Explanation** The tunnel group cannot be found, based on the digital certificate information.

**Recommended Action** Verify that the tunnel group is set up correctly to handle the certificate information of the peer.

**713092**

**Error Message** %FTD-5-713092: Failure during phase 1 rekeying attempt due to collision

**Explanation** An internal software error has occurred. This is often a benign event.

**Recommended Action** If the problem persists, contact the Cisco TAC.
713094

Error Message %FTD-7-713094: Cert validation failure: handle invalid for Main /Aggressive Mode Initiator /Responder!

Explanation An internal software error has occurred.

Recommended Action You may have to reenroll the trustpoint. If the problem persists, contact the Cisco TAC.

713098

Error Message %FTD-3-713098: Aborting: No identity cert specified in IPsec SA (SA_name)!

Explanation An attempt was made to establish a certificate-based IKE session, but no identity certificate has been specified in the crypto policy.

Recommended Action Specify the identity certificate or trustpoint that you want to transmit to peers.

713099

Error Message %FTD-7-713099: Tunnel Rejected: Received NONCE length number is out of range!

Explanation An internal software error has occurred.

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

713102

Error Message %FTD-3-713102: Phase 1 ID Data length number too long - reject tunnel!

Explanation IKE has received an ID payload that includes an identification data field of 2 K or larger.

Recommended Action None required.

713103

Error Message %FTD-7-713103: Invalid (NULL) secret key detected while computing hash

Explanation An internal software error has occurred.

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

713104

Error Message %FTD-7-713104: Attempt to get Phase 1 ID data failed while hash computation

Explanation An internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.
713105

**ErrorMessage** %FTD-3-713105: Zero length data in ID payload received during phase 1 or 2 processing

**Explanation** A peer sent an ID payload without including any ID data, which is invalid.

**Recommended Action** Check the configuration of the peer.

---

713107

**ErrorMessage** %FTD-3-713107: IP_Address request attempt failed!

**Explanation** An internal software error has occurred.

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

---

713109

**ErrorMessage** %FTD-3-713109: Unable to process the received peer certificate

**Explanation** The Firepower Threat Defense device was unable to process the certificate received from the remote peer, which can occur if the certificate data was malformed (for example, if the public key size is larger than 4096 bits) or if the data in the certificate cannot be stored by the Firepower Threat Defense device.

**Recommended Action** Try to reestablish the connection using a different certificate on the remote peer.

---

**Messages 713112 to 714011**

This section includes messages from 713112 to 714011.

---

713112

**ErrorMessage** %FTD-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!

**Explanation** The Firepower Threat Defense device was unable to successfully process the notification payload that included the CONNECTED notify type. This may occur if the IKE phase 2 structure cannot be found using the SPI to locate it, or the commit bit had not been set in the received ISAKMP header. The latter case may indicate a nonconforming IKE peer.

**Recommended Action** If the problem persists, check the configuration of the peer and/or disable commit bit processing.

---

713113

**ErrorMessage** %FTD-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count

**Explanation** An IKE SA is being deleted with a nonzero tunnel count, which means that either the IKE SA tunnel count has lost synchronization with the associated connection entries or the associated connection cookie fields for the entries have lost synchronization with the cookie fields of the IKE SA to which the
connection entry points. If this occurs, the IKE SA and its associated data structures will not be freed, so that
the entries that may point to it will not have a stale pointer.

**Recommended Action** None required. Error recovery is built-in.

### 713114

**Error Message** %FTD-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match

**Explanation** An internal software error has occurred.

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

### 713115

**Error Message** %FTD-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec

**Explanation** The client rejected an attempt by the Firepower Threat Defense device to use IPsec over UDP. IPsec over UDP is used to allow multiple clients to establish simultaneous tunnels to the Firepower Threat Defense device through a NAT device. The client may have rejected the request, either because it does not support this feature or because it is configured not to use it.

**Recommended Action** Verify the configuration on the headend and peer.

### 713117

**Error Message** %FTD-7-713117: Received Invalid SPI notify (SPI SPI_Value)!

**Explanation** The IPsec SA identified by the SPI value is no longer active on the remote peer, which might indicate that the remote peer has rebooted or been reset.

**Recommended Action** This problem should correct itself once DPDs recognize that the peer no longer has the appropriate SAs established. If DPD is not enabled, this may require you to manually reestablish the affected tunnel.

### 713118

**Error Message** %FTD-3-713118: Detected invalid Diffie-Hellmann group_descriptor group_number, in IKE area

**Explanation** The group_descriptor field included an unsupported value. Currently we support only groups 1, 2, 5, and 7. In the case of a centry, the group_descriptor field may also be set to 0 to indicate that perfect forward secrecy is disabled.

**Recommended Action** Check the peer Diffie-Hellman configuration.

### 713119

**Error Message** %FTD-5-713119: Group group IP ip PHASE 1 COMPLETED

**Explanation** IKE Phase 1 has completed successfully.
Recommended Action: None required.

**713120**

**Error Message**: %FTD-5-713120: PHASE 2 COMPLETED (msgid=msg_id)

**Explanation**: IKE Phase 2 has completed successfully.

**Recommended Action**: None required.

**713121**

**Error Message**: %FTD-7-713121: Keep-alive type for this connection: keepalive_type

**Explanation**: The type of keepalive mechanism that is being used for this tunnel is specified.

**Recommended Action**: None required.

**713122**

**Error Message**: %FTD-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)

**Explanation**: Keepalives were configured on or off for this device, but the IKE peer does or does not support keepalives.

**Recommended Action**: No action is required if this configuration is intentional. If it is not intentional, change the keepalive configuration on both devices.

**713123**

**Error Message**: %FTD-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)

**Explanation**: The remote IKE peer did not respond to keepalives within the expected window of time, so the connection to the IKE peer was terminated. The message includes the keepalive mechanism used.

**Recommended Action**: None required.

**713124**

**Error Message**: %FTD-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #

**Explanation**: The remote IKE peer sent a DPD with a sequence number that did not match the expected sequence number. The packet is discarded. This might indicate a packet loss problem with the network.

**Recommended Action**: None required.

**713127**

**Error Message**: %FTD-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
**Explanation** The peer wanted to perform a XAUTH, but the Firepower Threat Defense device did not choose the XAUTH IKE proposal.

**Recommended Action** Check the priorities of the IKE xauth proposals in the IKE proposal list.

---

**713128**

**Error Message** %FTD-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing

**Explanation** A connection attempt has been made to the VCPIP and has been redirected to a less loaded peer using load balancing.

**Recommended Action** None required.

---

**713129**

**Error Message** %FTD-3-713129: Received unexpected Transaction Exchange payload type: payload_id

**Explanation** An unexpected payload has been received during XAUTH or Mode Cfg, which may indicate that the two peers are out-of-sync, that the XAUTH or Mode Cfg versions do not match, or that the remote peer is not complying with the appropriate RFCs.

**Recommended Action** Verify the configuration between peers.

---

**713130**

**Error Message** %FTD-5-713130: Received unsupported transaction mode attribute: attribute_id

**Explanation** The device received a request for a valid transaction mode attribute (XAUTH or Mode Cfg) that is currently not supported. This is generally a benign condition.

**Recommended Action** None required.

---

**713131**

**Error Message** %FTD-5-713131: Received unknown transaction mode attribute: attribute_id

**Explanation** The Firepower Threat Defense device has received a request for a transaction mode attribute (XAUTH or Mode Cfg) that is outside the range of known attributes. The attribute may be valid but only supported in later versions of configuration mode, or the peer may be sending an illegal or proprietary value. This should not cause connectivity problems, but may affect the functionality of the peer.

**Recommended Action** None required.

---

**713132**

**Error Message** %FTD-3-713132: Cannot obtain an IP_address for remote peer

**Explanation** A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied.

**Recommended Action** Check the configuration of IP address assignment methods.
713133

**Error Message** %FTD-3-713133: Mismatch: Overriding phase 2 DH Group (DH group DH group_id ) with phase 1 group (DH group DH group_number)

**Explanation** The configured Phase 2 PFS Group differed from the DH group that was negotiated for Phase 1.

**Recommended Action** None required.

713134

**Error Message** %FTD-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

**Explanation** The configured LAN-to-LAN proposal is different from the one accepted for the LAN-to-LAN connection. Depending on which side is the initiator, different proposals will be used.

**Recommended Action** None required.

713135

**Error Message** %FTD-5-713135: message received, redirecting tunnel to IP_address.

**Explanation** The tunnel is being redirected because of load balancing on the remote Firepower Threat Defense device. A REDIRECT_CONNECTION notify packet was received.

**Recommended Action** None required.

713136

**Error Message** %FTD-5-713136: IKE session establishment timed out [IKE_state_name], aborting!

**Explanation** The Reaper has detected an Firepower Threat Defense device stuck in an inactive state. The Reaper will try to remove the inactive Firepower Threat Defense device.

**Recommended Action** None required.

713137

**Error Message** %FTD-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!

**Explanation** An internal software error has occurred.

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

713138

**Error Message** %FTD-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
**Explanation** No group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Firepower Threat Defense device will fall back and try to use the default preshared key configured in one of the default groups. The default preshared key is not configured.

**Recommended Action** Verify the configuration of the preshared keys.

### 713139

**Error Message** %FTD-5-713139: group_name not found, using BASE GROUP default preshared key

**Explanation** No tunnel group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Firepower Threat Defense device will fall back and use the default preshared key configured in the default group.

**Recommended Action** None required.

### 713140

**Error Message** %FTD-3-713140: Split Tunneling Policy requires network list but none configured

**Explanation** The split tunneling policy is set to either split tunneling or to allow local LAN access. A split tunneling ACL must be defined to represent the information required by the VPN client.

**Recommended Action** Check the configuration of the ACLs.

### 713141

**Error Message** %FTD-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability_value

**Explanation** The Firepower Threat Defense device installed on the client does not match the configured required Firepower Threat Defense device. This message lists the actual and expected values, and whether the tunnel is terminated or allowed.

**Recommended Action** You may need to install a different personal Firepower Threat Defense device on the client or change the configuration on the Firepower Threat Defense device.

### 713142

**Error Message** %FTD-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value

**Explanation** The client did not report an Firepower Threat Defense device in use using ModeCfg, but one is required. The event lists the expected values and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all of the allowed products.

**Recommended Action** You may need to install a different personal Firepower Threat Defense device on the client or change the configuration on the Firepower Threat Defense device.
713143


**Explanation** Debugging information about the Firepower Threat Defense device installed on the client appears.

**Recommended Action** None required.

713144

**Error Message** `%FTD-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction`

**Explanation** Bad Firepower Threat Defense device information was received from the client.

**Recommended Action** Check the personal configuration on the client and the Firepower Threat Defense device.

713145

**Error Message** `%FTD-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: netmask`

**Explanation** A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Firepower Threat Defense device to make the remote network known to all the routers on the private side of the headend.

**Recommended Action** None required.

713146

**Error Message** `%FTD-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: netmask`

**Explanation** An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The routing table may be full, or a possible addressing error has occurred.

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

713147

**Error Message** `%FTD-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask: netmask`

**Explanation** A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

**Recommended Action** None required.
713148

**Error Message** %FTD-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: netmask

**Explanation** While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

**Recommended Action** Check the routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

713149

**Error Message** %FTD-3-713149: Hardware client security attribute attribute_name was enabled but not requested.

**Explanation** The headend Firepower Threat Defense device has the specified hardware client security attribute enabled, but the attribute was not requested by the VPN 3002 hardware client.

**Recommended Action** Check the configuration on the hardware client.

713152

**Error Message** %FTD-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.

**Explanation** The client is required to use CPP to provision its Firepower Threat Defense device, but the headend device was unable to obtain any ACLs to send to the client. This is probably due to a misconfiguration.

**Recommended Action** Check the ACLs specified for CPP in the group policy for the client.

713154

**Error Message** %FTD-4-713154: DNS lookup for peer_description Server [server_name ] failed!

**Explanation** This message appears when a DNS lookup for the specified server has not been resolved.

**Recommended Action** Check the DNS server configuration on the Firepower Threat Defense device. Also check the DNS server to ensure that it is operational and has hostname to IP address mapping.

713155

**Error Message** %FTD-5-713155: DNS lookup for Primary VPN Server [server_name ] successfully resolved after a previous failure. Resetting any Backup Server init.

**Explanation** A previous DNS lookup failure for the primary server might have caused the Firepower Threat Defense device to initialize a backup peer. This message indicates that a later DNS lookup on the primary server finally succeeded and is resetting any backup server initializations. A tunnel initiated after this point will be aimed at the primary server.

**Recommended Action** None required.
713156

**Error Message** %FTD-5-713156: Initializing Backup Server [server_name or IP_address ]

**Explanation** The client is failing over to a backup server, or a failed DNS lookup for the primary server caused the Firepower Threat Defense device to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.

**Recommended Action** None required.

713157

**Error Message** %FTD-4-713157: Timed out on initial contact to server [server_name or IP_address ] Tunnel could not be established.

**Explanation** The client tried to initiate a tunnel by sending out IKE MSG1, but did not receive a response from the Firepower Threat Defense device on the other end. If backup servers are available, the client will attempt to connect to one of them.

**Recommended Action** Verify connectivity to the headend Firepower Threat Defense device.

713158

**Error Message** %FTD-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP

**Explanation** The client is configured to use IPsec over TCP. The client rejected the attempt by the Firepower Threat Defense device to use IPsec over UDP.

**Recommended Action** If TCP is desired, no action is required. Otherwise, check the client configuration.

713159

**Error Message** %FTD-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

**Explanation** The TCP connection to the Firepower Threat Defense server was lost for a certain reason, such as the server has rebooted, a network problem has occurred, or an SSL mismatch has occurred.

**Recommended Action** If the server connection was lost after the initial connection was made, then the server and network connections must be checked. If the initial connection is lost immediately, this might indicate an SSL authentication problem.

713160

**Error Message** %FTD-7-713160: Remote user (session Id - id ) has been granted access by the Firewall Server

**Explanation** Normal authentication of the remote user to the Firepower Threat Defense server has occurred.

**Recommended Action** None required.
713161

**Error Message**  %FTD-3-713161: Remote user (session Id = id) network access has been restricted by the Firewall Server

**Explanation**  The Firepower Threat Defense server has sent the Firepower Threat Defense device a message indicating that this user must be restricted. There are several reasons for this, including Firepower Threat Defense software upgrades or changes in permissions. The Firepower Threat Defense server will transition the user back into full access mode as soon as the operation has been completed.

**Recommended Action**  No action is required unless the user is never transitioned back into full access state. If this does not happen, refer to the Firepower Threat Defense server for more information on the operation that is being performed and the state of the Firepower Threat Defense software running on the remote machine.

713162

**Error Message**  %FTD-3-713162: Remote user (session Id = id) has been rejected by the Firewall Server

**Explanation**  The Firepower Threat Defense server has rejected this user.

**Recommended Action**  Check the policy information on the Firepower Threat Defense server to make sure that the user is configured correctly.

713163

**Error Message**  %FTD-3-713163: Remote user (session Id = id) has been terminated by the Firewall Server

**Explanation**  The Firepower Threat Defense server has terminated this user session, which can occur if the integrity agent stops running on the client machine or if the security policy is modified by the remote user in any way.

**Recommended Action**  Verify that the Firepower Threat Defense software on the client machine is still running and that the policy is correct.

713164

**Error Message**  %FTD-7-713164: The Firewall Server has requested a list of active user sessions

**Explanation**  The Firepower Threat Defense server will request the session information if it detects that it has stale data or if it loses the session data (because of a reboot).

**Recommended Action**  None required.

713165

**Error Message**  %FTD-3-713165: Client IKE Auth mode differs from the group's configured Auth mode

**Explanation**  The client negotiated with preshared keys while its tunnel group points to a policy that is configured to use digital certificates.

**Recommended Action**  Check the client configuration.
713166

**Error Message** %FTD-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password

**Explanation** The hardware client has failed extended authentication. This is most likely a username and password problem or an authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server at the headend is operational.

713167

**Error Message** %FTD-3-713167: Remote peer has failed user authentication - check configured username and password

**Explanation** The remote user has failed to extend authentication. This is most likely a username or password problem, or an authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server being used to authenticate the remote user is operational.

713168

**Error Message** %FTD-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!

**Explanation** Reauthentication on rekeying has been enabled, but the tunnel authentication requires manual intervention.

**Recommended Action** If manual intervention is desired, no action is required. Otherwise, check the interactive authentication configuration.

713169

**Error Message** %FTD-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address , SA address: internal_SA_address , tunnelCnt: tunnel_count

**Explanation** IKE has received a delete message from the remote peer to delete its old IKE SA after a rekey has completed.

**Recommended Action** None required.

713170

**Error Message** %FTD-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address , centry address: internal_address , msgid: id

**Explanation** IKE has received a delete message from the remote peer to delete its old centry after Phase 2 rekeying is completed.

**Recommended Action** None required.
713171

**Error Message** %FTD-7-713171: NAT-Traversal sending NAT-Original-Address payload

**Explanation** UDP-Encapsulated-Transport was either proposed or selected during Phase 2. Send this payload for NAT-Traversal in this case.

**Recommended Action** None required.

---

713172

**Error Message** %FTD-6-713172: Automatic NAT Detection Status: Remote end *is* | *is not* behind a NAT device This end *is* | *is not* behind a NAT device

**Explanation** NAT-Traversal auto-detected NAT.

**Recommended Action** None required.

---

713174

**Error Message** %FTD-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

**Explanation** A hardware client is attempting to tunnel in using network extension mode, but network extension mode is not allowed.

**Recommended Action** Verify the configuration of the network extension mode versus PAT mode.

---

713176

**Error Message** %FTD-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored

**Explanation** The Firepower Threat Defense device is processing data intended to trigger an IPsec tunnel to the indicated peer. Because memory resources are at a critical state, it is not initiating any more tunnels. The data packet has been ignored and dropped.

**Recommended Action** If condition persists, verify that the Firepower Threat Defense device is efficiently configured. An Firepower Threat Defense device with increased memory may be required for this application.

---

713177

**Error Message** %FTD-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address , Protocol protocol , Port port

**Explanation** A Phase 2 ID payload containing an FQDN has been received from the peer.

**Recommended Action** None required.

---

713178

**Error Message** %FTD-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
Explanation  An internal software error has occurred.
Recommended Action  If the problem persists, contact the Cisco TAC.

713179

ErrorMessage  %FTD-5-713179: IKE AM Initiator received a packet from its peer without a payload_type  payload

Explanation  An internal software error has occurred.
Recommended Action  If the problem persists, contact the Cisco TAC.

713182

ErrorMessage  %FTD-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!

Explanation  An internal software error has occurred.
Recommended Action  If the problem persists, contact the Cisco TAC.

713184

ErrorMessage  %FTD-6-713184: Client Type: Client_type  Client Application Version: Application_version_string

Explanation  The client operating system and application version appear. If the information is not available, then N/A will be indicated.
Recommended Action  None required.

713185

ErrorMessage  %FTD-3-713185: Error: Username too long - connection aborted

Explanation  The client returned an invalid length username, and the tunnel was torn down.
Recommended Action  Check the username and make changes, if necessary.

713186

ErrorMessage  %FTD-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text  Character index (value ) is illegal

Explanation  An invalid secondary domain name list was received from an external RADIUS authentication server. When split tunnelling is used, this list identifies the domains that the client should resolve through the tunnel.
Recommended Action  Correct the specification of the Secondary-Domain-Name-List attribute (vendor-specific attribute 29) on the RADIUS server. The list must be specified as a comma-delimited list of domain names. Domain names may include only alphanumeric characters, a hyphen, an underscore, and a period.
713187

**Error Message** %FTD-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy
IKE peer address: IP_address, Remote peer address: IP_address

**Explanation** The IKE peer that is attempting to bring up this tunnel is not the one that is configured in the ISAKMP configuration that is bound to the received remote subnet.

**Recommended Action** Verify that L2L settings are correct on the headend and peer.

713189

**Error Message** %FTD-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.

**Explanation** The IP address from the pool is either the network or broadcast address for this subnet. This address will be marked as unavailable.

**Recommended Action** This error is generally benign, but the IP address pool configuration should be checked.

713190

**Error Message** %FTD-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)

**Explanation** The reference counter for this SA is invalid.

**Recommended Action** None required.

713191

**Error Message** %FTD-3-713191: Maximum concurrent IKE negotiations exceeded!

**Explanation** To minimize CPU-intensive cryptographic calculations, the Firepower Threat Defense device limits the number of connection negotiations in progress. When a new negotiation is requested and the Firepower Threat Defense device is already at its limit, the new negotiation is rejected. When an existing connection negotiation completes, new connection negotiation will again be permitted.

**Recommended Action** See the `crypto ikev1 limit max-in-negotiation-sa` command. Increasing the limit can degrade performance..

713193

**Error Message** %FTD-3-713193: Received packet with missing payload, Expected payload: payload_id

**Explanation** The Firepower Threat Defense device received an encrypted or unencrypted packet of the specified exchange type that had one or more missing payloads. This usually indicates a problem on the peer.

**Recommended Action** Verify that the peer is sending valid IKE messages.
713194

**Error Message** %FTD-3-713194: Sending IKE |IPsec Delete With Reason message: termination_reason

**Explanation** A delete message with a termination reason code was received.

**Recommended Action** None required.

713195

**Error Message** %FTD-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!

**Explanation** The originate-only peer can accept incoming connections only after it brings up the first P2 tunnel. At that point, data from either direction can initiate additional Phase 2 tunnels.

**Recommended Action** If a different behavior is desired, the originate-only configuration needs to be revised.

713196

**Error Message** %FTD-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!

**Explanation** The remote L2L peer has initiated a public-public tunnel. The remote L2L peer expects a response from the peer at the other end, but does not receive one, because of a possible misconfiguration.

**Recommended Action** Check the L2L configuration on both sides.

713197

**Error Message** %FTD-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.

**Explanation** The configured confidence interval in the group is outside of the valid range.

**Recommended Action** Check the confidence setting in the group to make sure it is within the valid range.

713198

**Error Message** %FTD-3-713198: User Authorization failed: user User authorization failed. Username could not be found in the certificate

**Explanation** A reason string that states that a username cannot be found in the certificate appears.

**Recommended Action** Check the group configuration and client authorization.

713199

**Error Message** %FTD-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter { counter_value }!

**Explanation** The Reaper corrected an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.
**713203**

**Error Message** %FTD-3-713203: IKE Receiver: Error reading from socket.

**Explanation** An error occurred while reading a received IKE packet. This is generally an internal error and might indicate a software problem.

**Recommended Action** This problem is usually benign, and the system will correct itself. If the problem persists, contact the Cisco TAC.

---

**713204**

**Error Message** %FTD-7-713204: Adding static route for client address: IP_address

**Explanation** This message indicates that a route to the peer-assigned address or to the networks protected by a hardware client was added to the routing table.

**Recommended Action** None required.

---

**713205**

**Error Message** %FTD-3-713205: Could not add static route for client address: IP_address

**Explanation** An attempt to add a route to the client-assigned address or to the networks protected by a hardware client failed. This might indicate duplicate routes in the routing table or a corrupted network address. The duplicate routes might be caused by routes that were not cleaned up correctly or by having multiple clients sharing networks or addresses.

**Recommended Action** Check the IP local pool configuration as well as any other IP address-assigning mechanism being used (for example, DHCP or RADIUS). Make sure that routes are being cleared from the routing table. Also check the configuration of networks and/or addresses on the peer.

---

**713206**

**Error Message** %FTD-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy

**Explanation** A tunnel was dropped because the allowed tunnel specified in the group policy was different from the allowed tunnel in the tunnel group configuration.

**Recommended Action** Check the tunnel group and group policy configuration.

---

**713207**

**Error Message** %FTD-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPSec

**Explanation** This syslog is displayed for ikev1 while terminating the connection if GW is an initiator and tunnel group type is L2TP over IPSEC.

**Recommended Action** None required.
713208

**Error Message** %FTD-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id

**Explanation** A failure occurred in creating the ACLs that trigger IKE and allow IPsec data to be processed properly. The failure was specific to the backup L2L configuration, which may indicate a configuration error, a capacity error, or an internal software error.

**Recommended Action** If the Firepower Threat Defense device is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, specifically the ACLs associated with the crypto maps.

713209

**Error Message** %FTD-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id

**Explanation** A failure occurred in deleting the ACLs that trigger IKE and allow IPsec data to be processed correctly. The failure was specific to the backup L2L configuration. This may indicate an internal software error.

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

713210

**Error Message** %FTD-3-713210: Cannot create dynamic map for Backup L2L entry rule_id

**Explanation** A failure occurred in creating a run-time instance of the dynamic crypto map associated with backup L2L configuration. This may indicate a configuration error, a capacity error, or an internal software error.

**Recommended Action** If the Firepower Threat Defense device is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, and specifically the ACLs associated with the crypto maps.

713212

**Error Message** %FTD-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask

**Explanation** The Firepower Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full routing table, or a failure of the Firepower Threat Defense device to remove previously used routes.

Check the routing table to make sure there is room for additional routes and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

713213

**Error Message** %FTD-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
Explanation The Firepower Threat Defense device is deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

Recommended Action None required.

713214

Error Message %FTD-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask

Explanation The Firepower Threat Defense device experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted, or an internal software error has occurred.

Recommended Action If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

713215

Error Message %FTD-6-713215: No match against Client Type and Version rules. Client: type version is /is not allowed by default

Explanation The client type and the version of a client did not match any of the rules configured on the Firepower Threat Defense device. The default action appears.

Recommended Action Determine what the default action and deployment requirements are, and make the applicable changes.

713216

Error Message %FTD-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed

Explanation The client type and the version of a client have matched one of the rules. The results of the match and the rule are displayed.

Recommended Action Determine what the deployment requirements are, and make the appropriate changes.

713217

Error Message %FTD-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version

Explanation A malformed client type and version rule exist. The required format is action client type | client version action. Either permit or deny client type and client version are displayed under Session Management. Only one wildcard per parameter (*) is supported.

Recommended Action Correct the rule.
713218

Error Message  %FTD-3-713218: Tunnel Rejected: Client Type or Version not allowed.

The client was denied access according to the configured rules.
None required.

713219

Error Message  %FTD-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.

Explanation Phase 2 messages are being enqueued after Phase 1 completes.
Recommended Action None required.

713220

Error Message  %FTD-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.

Explanation Queued Phase 2 messages are being processed.
Recommended Action None required.

713221

Error Message  %FTD-7-713221: Static Crypto Map check, checking map = crypto_map_tag , seq = seq_number...

Explanation The Firepower Threat Defense device is iterating through the crypto maps looking for configuration information.
Recommended Action None required.

713222

Error Message  %FTD-7-713222: Group group Username username IP ip  Static Crypto Map check, map = crypto_map_tag , seq = seq_number , ACL does not match proxy IDs src:source_address dst:dest_address

Explanation While iterating through the configured crypto maps, the Firepower Threat Defense device cannot match any of the associated ACLs. This generally means that an ACL was misconfigured.
Recommended Action Check the ACLs associated with this tunnel peer, and make sure that they specify the appropriate private networks from both sides of the VPN tunnel.

713223

Error Message  %FTD-7-713223: Static Crypto Map check, map = crypto_map_tag , seq = seq_number , no ACL configured

Explanation The crypto map associated with this peer is not linked to an ACL.
**Recommended Action** Make sure an ACL associated with this crypto map exists, and that the ACL includes the appropriate private addresses or network from both sides of the VPN tunnel.

**713224**

**Error Message** %FTD-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

**Explanation** The crypto map associated with this VPN tunnel is missing critical information.

**Recommended Action** Verify that the crypto map is configured correctly with both the VPN peer, a transform set, and an associated ACL.

**713225**

**Error Message** %FTD-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match

**Explanation** The Firepower Threat Defense device found a valid matching crypto map for this VPN tunnel.

**Recommended Action** None required.

**713226**

**Error Message** %FTD-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group

**Explanation** When the device is configured to use digital certificates, a trustpoint must be specified in the configuration. When the trustpoint is missing from the configuration, this message is generated to flag an error.

- **IP_address**—IP address of the peer
- **tunnel_group**—Tunnel group for which the trustpoint was missing in the configuration

**Recommended Action** The administrator of the device has to specify a trustpoint in the configuration.

**713227**

**Error Message** %FTD-3-713227: Rejecting new IPsec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address /Local_netmask, remote Proxy Remote_address /Remote_netmask

**Explanation** When establishing a Phase SA, the Firepower Threat Defense device will reject a new Phase 2 matching this proxy.

**Recommended Action** None required.

**713228**

**Error Message** %FTD-6-713228: Group = group, Username = uname, IP = remote_IP_address

Assigned private IP address assigned_private_IP to remote user

**Explanation** IKE obtained a private IP address for the client from DHCP or from the address pool.

- **group**—The name of the group
• **uname** — The name of the user
• **remote_IP_address** — The IP address of the remote client
• **assigned_private_IP** — The client IP address assigned by DHCP or from the local address pool

**Recommended Action** None required.

### 713229

**Error Message** %FTD-5-713229: Auto Update - Notification to client client_ip of update string: message_string.

**Explanation** A VPN remote access client is notified that updated software is available for download. The remote client user is responsible for choosing to update the client access software.

• **client_ip** — The IP address of the remote client
• **message_string** — The message text sent to the remote client

**Recommended Action** None required.

### 713230

**Error Message** %FTD-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type.

**Explanation** An internal error occurred, which is reporting that the IKE subsystem is attempting to lock memory that has already been locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

• **>type** — String that describes the type of semaphore that had a locking issue

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

### 713231

**Error Message** %FTD-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type.

**Explanation** An internal error has occurred, which is reporting that the IKE subsystem is attempting to unlock memory that is not currently locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

• **type** — String that describes the type of semaphore that had a locking issue

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

### 713232

**Error Message** %FTD-3-713232 SA lock refCnt = value, bitmask = hexvalue, pl_decrypt_cb = value, qm_decrypt_cb = value, qm_hash_cb = value, qm_spi_ok_cb = value, qm_dh_cb = value, qm_secret_key_cb = value, qm_encrypt_cb = value
**Explanation** All the IKE SA are locked, and a possible error has been detected. This message reports errors on semaphores that are used to protect memory violations for IKE SAs.

- >value —Decimal value
- >hexvalue —Hexadecimal value

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

---

**71323**

**Error Message** %FTD-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.

**Explanation** The remote network received during the Phase 2 negotiation was validated. The message indicates the results of the remote network check during Phase 2 negotiations for Network Extension Mode clients. This is part of an existing feature that prevents users from misconfiguring their hardware client network (for example, configuring overlapping networks or the same network on multiple clients).

- remote network —Subnet address and subnet mask from Phase 2 proxy

**Recommended Action** None required.

---

**71324**

**Error Message** %FTD-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).

**Explanation** The remote network received during the Phase 2 negotiation does not match the framed-ip-address and framed-subnet-mask that were returned from the AAA server for this session.

- remote network —Subnet address and subnet mask from Phase 2 proxy
- aaa network —Subnet address and subnet mask configured through AAA

**Recommended Action** Do one of the following:

- Check the address assignment for this user and group, then check the network configuration on the HW client, and correct any inconsistencies.
- Disable address assignment for this user and group.

---

**71325**

**Error Message** %FTD-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!

**Explanation** Normally, IKE packets should never be sent from the standby unit to the remote peer. If such an attempt is made, an internal logic error may have occurred. The packet never leaves the standby unit because of protective code. This message facilitates debugging.

**Recommended Action** None required.

---

**71326**

**Error Message** %FTD-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen
**Explaination** IKE sent or received various messages.

The following example shows the output when IKE receives a message with an 8-byte hash payload, an 11-byte notify payload, and two 13-byte vendor-specific payloads:

```
%FTD-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

**Recommended Action** None required.

---

**Error Message** %FTD-5-713237: ACL update (access_list ) received during re-key re-authentication will not be applied to the tunnel.

**Explanation** The Phase 1 rekey of a remote access IPsec tunnel appears under the following conditions:

- The tunnel is configured to reauthenticate the user when the tunnel is rekeyed.
- The RADIUS server returns an access list or a reference to a locally configured access list that is different from the one that was returned when the tunnel was first established.

**Recommended Action** Under these conditions, the Firepower Threat Defense device ignores the new access list and this message is generated.

- `>access_list` — Name associated with the static or dynamic access list, as displayed in the output of the `show access-list` command

IPsec users must reconnect for new user-specific access lists to take effect.

---

**Error Message** %FTD-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client.

**Explanation** The private side address of a network extension mode client came across as 0.0.0.0. This usually indicates that no IP address was set on the private interface of the hardware client.

**Recommended Action** Verify the configuration of the remote client.

---

**Error Message** %FTD-4-713239: IP_Address : Tunnel Rejected: The maximum tunnel count allowed has been reached.

**Explanation** An attempt to create a tunnel has occurred after the maximum number of tunnels allowed has been reached.

- `IP_Address` — The IP address of the peer

**Recommended Action** None required.

---

**Error Message** %FTD-4-713240: Received DH key with bad length: received length=rlength expected length=elength
Explanation  A Diffie-Hellman key with the incorrect length was received from the peer.

- rlength—The length of the DH key that was received
- elength—The expected length (based on the DH key size)

**Recommended Action** None required.

---

**713241**

**Error Message** %FTD-4-713241: IE Browser Proxy Method setting_number is Invalid

**Explanation** An invalid proxy setting was found during ModeCfg processing. P1 negotiation will fail.

**Recommended Action** Check the `msie-proxy method` command settings (a subcommand of the `group-policy` command), which should conform to one of the following: `[auto-detect | no-modify | no-proxy | use-server]` . Any other value or no value is incorrect. Try resetting the `msie-proxy method` command settings. If the problem persists, contact the Cisco TAC.

---

**713242**

**Error Message** %FTD-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.

**Explanation** The Firepower Threat Defense device has detected a request to start an IKE rekey for a tunnel configured to use Hybrid Xauth, but the rekey was not started. The Firepower Threat Defense device will wait for the client to detect and initiate an IKE rekey.

**Recommended Action** None required.

---

**713243**

**Error Message** %FTD-4-713243: META-DATA Unable to find the requested certificate

**Explanation** The IKE peer requested a certificate from the cert-req payload. However, no valid identity certificate issued by the requested DN was found.

**Recommended Action** Perform the following steps:

1. Check the identity certificates.
2. Enroll or import the desired certificate.
3. Enable certificate debugging for more details.

---

**713244**

**Error Message** %FTD-4-713244: META-DATA Received Legacy Authentication Method (LAM) type type is different from the last type received type .

**Explanation** The LAM attribute type received differs from the last type received. The type must be consistent throughout the user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- type—The LAM type

**Recommended Action** If the problem persists, contact the Cisco TAC.
713245

Error Message %FTD-4-713245: META-DATA Unknown Legacy Authentication Method (LAM) type type received.

Explanation An unsupported LAM type was received during the CRACK challenge or response user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

• type — The LAM type

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

713246

Error Message %FTD-4-713246: META-DATA Unknown Legacy Authentication Method (LAM) attribute type type received.

Explanation The Firepower Threat Defense device received an unknown LAM attribute type, which should not cause connectivity problems, but might affect the functionality of the peer.

• type — The LAM attribute type

Recommended Action None required.

713247

Error Message %FTD-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.

Explanation An unexpected error occurred during state processing.

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

713248

Error Message %FTD-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.

Explanation When an IKE SA is negotiated using the CRACK authentication method, the Phase 1 SA rekey timer at the headend expired before a successful rekey. Because the remote client is always the initiator of the exchange when using the CRACK authentication method, the headend will not initiate the rekey. Unless the remote peer initiates a successful rekey before the IKE SA expires, the connection will come down upon IKE SA expiration.

Recommended Action None required.

713249

Error Message %FTD-4-713249: META-DATA Received unsupported authentication results: result

Explanation While negotiating an IKE SA using the CRACK authentication method, the IKE subsystem received a result that is not supported during CRACK authentication from the authentication subsystem. The user authentication fails, and the VPN connection is torn down.
• **result** — The result returned from the authentication subsystem

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

### 713250

**Error Message** %FTD-5-713250: META-DATA Received unknown Internal Address attribute: attribute

**Explanation** The Firepower Threat Defense device received a request for an internal address attribute that is not recognizable. The attribute might be valid, but not currently supported, or the peer might be sending an illegal value. This should not cause connectivity problems, but might affect the functionality of the peer.

**Recommended Action** None required.

### 713251

**Error Message** %FTD-4-713251: META-DATA Received authentication failure message

**Explanation** The Firepower Threat Defense device received a notification message that indicated an authentication failure while an IKE SA is negotiated using the CRACK authentication method. The connection is torn down.

**Recommended Action** None required.

### 713252

**Error Message** %FTD-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.

**Explanation** When the group policy is configured to require the client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator depending on the failure policy configured. If the fail policy is to reject the client connection, this message is generated when a Zonelab Integrity Server is not connected to the Firepower Threat Defense device at the time the client is connecting.

- **group** — The tunnel group to which the remote access user is connecting
- **user** — The remote access user
- **ip** — The IP address of the remote access user

**Recommended Action** Check that the configurations on the concentrator and the Zonelab Integrity Server match. Then verify that communication exists between the concentrator and the Zonelab Integrity Server.

### 713253

**Error Message** %FTD-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.

**Explanation** When the group policy is configured to require a client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator, depending on the failure policy configured. If the failure policy is to accept the client connection, and provide unrestricted network access, this message is generated when a Zonelab Integrity Server is not connected to the Firepower Threat Defense device at the time the client is connecting.

- **group** — The tunnel group to which the remote access user is connecting
• user —The remote access user
• ip —The IP address of the remote access user

**Recommended Action** Check that the configurations on the Firepower Threat Defense device and the Zonelab Integrity Server match, and verify that communication exists between the Firepower Threat Defense device and the Zonelab Integrity Server.

---

### 713254

**ErrorMessage** %FTD-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPSec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPSec/NAT-T

**Explanation** You cannot use UDP port 4500 for IPSec/UDP connections, because it is reserved for IPSec or NAT-T connections. The CLI does not allow this configuration for local groups. This message should only occur for externally defined groups.

- **groupname** —The name of the user group
- **username** —The name of the user
- **peerip** —The IP address of the client
- **portnum** —The IPSec/UDP port number on the external server
- **minport** —The minimum valid port number for a user-configurable port, which is 4001
- **maxport** —The maximum valid port number for a user-configurable port, which is 49151

**Recommended Action** Change the IPSec or UDP port number on the external server to another port number. Valid port numbers are 4001 to 49151.

---

### 713255

**ErrorMessage** %FTD-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name

**Explanation** An unknown tunnel group was specified in ISAKMP Aggressive Mode message 1.

- **peer-ip** —The address of the peer
- **group-name** —The group name specified by the peer

**Recommended Action** Check the tunnel group and client configurations to make sure that they are valid.

---

### 713256

**ErrorMessage** %FTD-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.

**Explanation** When the peer specifies an invalid tunnel group, the Firepower Threat Defense device will still send message 2 to prevent the peer from gleaning tunnel group information.

- **peer-ip** —The address of the peer

**Recommended Action** None required.
**713257**

**Error Message** %FTD-5-713257: Phase var1 failure: Mismatched attribute types for class var2
: Rcv'd: var3 Cfg'd: var4

**Explanation** An Firepower Threat Defense device has acted as the responder in a LAN-to-LAN connection. It indicates that the Firepower Threat Defense crypto configuration does not match the configuration of the initiator. The message specifies during which phase the mismatch occurred, and which attributes both the responder and the initiator had that were different.

- var1 — The phase during which the mismatch occurred
- var2 — The class to which the attributes that do not match belong
- var3 — The attribute received from the initiator
- var4 — The attribute configured

**Recommended Action** Check the crypto configuration on both of the LAN-to-LAN devices for inconsistencies. In particular, if a mismatch between UDP-Tunnel (NAT-T) and something else is reported, check the crypto maps. If one configuration has NAT-T disabled on the matched crypto map and the other does not, this will cause a failure.

**713258**

**Error Message** %FTD-3-713258: IP = var1, Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.

**Explanation** The Firepower Threat Defense device tries to establish a Phase 2 tunnel on an interface, and a Phase 1 tunnel already exists on a different interface. The existing Phase 1 tunnel is torn down to allow the establishment of a new tunnel on the new interface.

- var1 — The IP address of the peer
- var2 — The interface on which the Firepower Threat Defense device is trying to establish a Phase 2 tunnel
- var3 — The interface on which the Phase 1 tunnel exists

**Recommended Action** Check whether or not the route of the peer has changed. If the route has not changed, a possible misconfiguration may exist.

**713259**

**Error Message** %FTD-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason

**Explanation** The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.

- groupname — The tunnel group of the session being terminated
- username — The username of the session being terminated
- peerIP — The peer address of the session being terminated
- reason — The RADIUS termination reason of the session being terminated. Reasons include the following:
  - Port Preempted (simultaneous logins)
  - Idle Timeout
713260

**Error Message** %FTD-3-713260: Output interface \#d to peer was not found

**Explanation** When trying to create a Phase 1 SA, the interface database could not be found for the interface ID.

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

713261

**Error Message** %FTD-3-713261: IPV6 address on output interface \#d was not found

**Explanation** When trying to create a Phase 1 SA, no IPv6 address is specified on the local interface.

**Recommended Action** For information about how to set up an IPv6 address on a desired interface, see the “Configuring IPv6 Addressing” section in the CLI configuration guide.

713262

**Error Message** %FTD-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address /Local_prefix_len, remote Proxy Remote_address /Remote_prefix_len

**Explanation** When establishing a Phase SA, the Firepower Threat Defense device will reject a new Phase 2 SA matching this proxy.

- **Peer_address** — The new address attempting to initiate Phase 2 with a proxy matching an existing negotiation
- **Local_address** — The address of the previous local peer currently negotiating Phase 2
- **Local_prefix_len** — The length of the subnet prefix according to CIDR notation
- **Remote_address** — The address of the proxy
- **Remote_prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

713263

**Error Message** %FTD-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port

**Explanation** The Firepower Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation
- **protocol** — The proxy protocol
**713264**

**Error Message** %FTD-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask/prefix_len, Protocol protocol, Port port ("Received remote IP Proxy Subnet data in ID Payload: Address $a, Mask/$d, Protocol $u, Port $u")

**Explanation** The Firepower Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation
- **protocol** — The proxy protocol
- **port** — The proxy port

**Recommended Action** None required.

---

**713265**

**Error Message** %FTD-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len

**Explanation** The Firepower Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

---

**713266**

**Error Message** %FTD-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len

**Explanation** The Firepower Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full IPv6 routing table, or a failure of the Firepower Threat Defense device to remove previously used routes.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** Check the IPv6 routing table to make sure there is room for additional routes, and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.
**713267**

**Error Message** %FTD-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len

**Explanation** The Firepower Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

---

**713268**

**Error Message** %FTD-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len

**Explanation** The Firepower Threat Defense device experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted, or an internal software error has occurred.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Also check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

---

**713269**

**Error Message** %FTD-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: /prefix_len

**Explanation** A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Firepower Threat Defense device to make the remote network known to all the routers on the private side of the headend.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

---

**713270**

**Error Message** %FTD-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: /prefix_len
Explanation An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The IPv6 routing table may be full, or a possible addressing error has occurred.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

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

---

**713271**

**Error Message** %FTD-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: **IP_address**, mask:**prefix_len**

**Explanation** A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

---

**713272**

**Error Message** %FTD-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: **IP_address**, mask:**prefix_len**

**Explanation** While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

- **IP_address** — The base IP address of the destination network of the peer
- **prefix_len** — The length of the subnet prefix according to CIDR notation

**Recommended Action** Check the IPv6 routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

---

**713273**

**Error Message** %FTD-7-713273: Deleting static route for client address: **IP_Address**, IP_Address address of client whose route is being removed

**Explanation** A route to the peer-assigned address or the networks protected by a hardware client were removed from the routing table.

**Recommended Action** None required.

---

**713274**

**Error Message** %FTD-3-713274: Could not delete static route for client address: **IP_Address**, IP_Address address of client whose route is being removed

**Explanation** While a tunnel to an IPsec client was being removed, its entry in the routing table could not be removed. This condition may indicate a networking or software problem.
Recommended Action Check the routing table to make sure that the route does not exist. If it does, it may need to be removed manually, but only if the tunnel has been closed successfully.

713275

Error Message %FTD-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s

Explanation This syslog is displayed for ikev1 when certificate key type is not of type ECDSA. Ensure that certificates of valid KEY type is installed on the GW.

Recommended Action None required.

713276

Error Message %FTD-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached

Explanation This syslog message is displayed for ikev1 in multi context when maximum in negotiation limit is reached.

Recommended Action None required.

713900

Error Message %FTD-1-713900: Descriptive_event_string.

Explanation A serious event or failure has occurred. For example, the Firepower Threat Defense device is trying to generate a Phase 2 deletion, but the SPI did not match any of the existing Phase 2 SAs.

Recommended Action In the example described, both peers are deleting Phase 2 SAs at the same time. In this case, it is a benign error and can be ignored. If the error is persistent and results in negative side effects such as dropped tunnels or device reboots, it may reflect a software failure. In this case, copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

713901

Error Message %FTD-2-713901: Descriptive_event_string.

Explanation An error has occurred, which may be the result of a configuration error on the headend or remote access client. The event string provides details about the error that occurred.

Recommended Action You may need to troubleshoot the message to determine what caused the error. Check the ISAKMP and crypto map configuration on both peers.

713902

Error Message % FTD-3-713902: Descriptive_event_string.

Explanation An error has occurred, which may be the result of a configuration error either on the headend or remote access client.
**Recommended Action** It might be necessary to troubleshoot the configuration to determine the cause of the error. Check the ISAKMP and crypto map configuration on both peers.

**713903**

**Error Message** %FTD-4-713903: IKE error message reason reason.

**Explanation** This syslog ID is used for IKE warning messages which can display multiple other syslogs.

**Recommended Action** None required.

**Examples:**
- %FTD-4-713903: Group = group policy, Username = user name, IP = remote IP, ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP
- %FTD-4-713903: IKE Receiver: Runt ISAKMP packet discarded on Port Port_Number from Source_URL
- %FTD-4-713903: IP = IP address, Header invalid, missing SA payload! (next payload = x)
- %FTD-4-713903: Group = DefaultRAGroup, IP = IP address, Error: Unable to remove PeerTblEntry

**713904**

**Error Message** %FTD-5-713904: Descriptive_event_string.

**Explanation** Notification status information appears, which is used to track events that have occurred.

**Recommended Action** None required.

**713905**

**Error Message** %FTD-6-713905: Descriptive_event_string.

**Explanation** Information status details appear, which are used to track events that have occurred.

**Example**
- %FTD-6-713905: IKE successfully unreserved UDP port 27910 on interface outside

**Recommended Action** None required.

**713906**

**Error Message** %FTD-7-713906: Descriptive_event_string.

**Explanation** Debugging status information appears, which is used to track events that have occurred.

**Recommended Action** None required.

**714001**

**Error Message** %FTD-7-714001: description_of_event_or_packet

**Explanation** A description of an IKE protocol event or packet was provided.

**Recommended Action** None required.
714002

**Error Message** %FTD-7-714002: IKE Initiator starting QM: msg id = message_number

**Explanation** The Firepower Threat Defense device has sent the first packet of the Quick mode exchange as the Phase 2 initiator.

**Recommended Action** None required.

714003

**Error Message** %FTD-7-714003: IKE Responder starting QM: msg id = message_number

**Explanation** The Firepower Threat Defense device has received the first packet of the Quick mode exchange as the Phase 2 responder.

**Recommended Action** None required.

714004

**Error Message** %FTD-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number

**Explanation** The protocol of the first Quick Mode packet was decoded.

**Recommended Action** None required.

714005

**Error Message** %FTD-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number

**Explanation** The protocol of the second Quick Mode packet was decoded.

**Recommended Action** None required.

714006

**Error Message** %FTD-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number

**Explanation** The protocol of the third Quick Mode packet was decoded.

**Recommended Action** None required.

714007

**Error Message** %FTD-7-714007: IKE Initiator sending Initial Contact

**Explanation** The Firepower Threat Defense device is building and sending the initial contact payload.

**Recommended Action** None required.

714011

**Error Message** %FTD-7-714011: Description of received ID values
**Explanation** The Firepower Threat Defense device received the displayed ID information during the negotiation.

**Recommended Action** None required.
Syslog Messages 715001 to 721019

This chapter contains the following sections:
- Messages 715001 to 715080, on page 289
- Messages 716001 to 716603, on page 301
- Messages 717001 to 717064, on page 320
- Messages 718001 to 719026, on page 333
- Messages 720001 to 721019, on page 355

Messages 715001 to 715080

This section includes messages from 715001 to 715080.

**715001**

**Error Message**: %FTD-7-715001: Descriptive statement

**Explanation**: A description of an event or problem encountered by the Firepower Threat Defense device appears.

**Recommended Action**: The action depends on the description.

**715004**

**Error Message**: %FTD-7-715004: subroutine name () Q Send failure: RetCode (return_code )

**Explanation**: An internal error occurred when attempting to put messages in a queue.

**Recommended Action**: This is often a benign condition. If the problem persists, contact the Cisco TAC.

**715005**

**Error Message**: %FTD-7-715005: subroutine name() Bad message code: Code (message_code )

**Explanation**: An internal subroutine received a bad message code.

**Recommended Action**: This is often a benign condition. If the problem persists, contact the Cisco TAC.
**715006**

**Error Message** %FTD-7-715006: IKE got SPI from key engine: SPI = SPI_value

**Explanation** The IKE subsystem received an SPI value from IPsec.

**Recommended Action** None required.

**715007**

**Error Message** %FTD-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value

**Explanation** IKE has completed tunnel negotiation and has successfully loaded the appropriate encryption and hashing keys for IPsec use.

**Recommended Action** None required.

**715008**

**Error Message** %FTD-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address

**Explanation** The calling subroutine cannot delete the IPsec SA. This might indicate a reference count problem.

**Recommended Action** If the number of stale SAs grows as a result of this event, contact the Cisco TAC.

**715009**

**Error Message** %FTD-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address

**Explanation** SA is being deleted with the listed proxy addresses.

**Recommended Action** None required.

**715013**

**Error Message** %FTD-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data

**Explanation** IKE is in the process of establishing a tunnel for this data. All packets to be protected by this tunnel will be dropped until the tunnel is fully established.

**Recommended Action** None required.

**715018**

**Error Message** %FTD-7-715018: IP Range type id was loaded: Direction %a, From: %a, Through: %a

**Explanation** This syslog message is generated while updating IPSEC SA details.

**Recommended Action** None required.
**715019**

**Error Message** %FTD-7-715019: Group group Username username IP ip IKEGetUserAttributes: 
Attribute name = name 

**Explanation** The `modecfg` attribute name and value pair being processed by the Firepower Threat Defense device appear.

**Recommended Action** None required.

**715020**

**Error Message** %FTD-7-715020: construct_cfg_set: Attribute name = name

**Explanation** The `modecfg` attribute name and value pair being transmitted by the Firepower Threat Defense device appear.

**Recommended Action** None required.

**715021**

**Error Message** %FTD-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

**Explanation** Quick mode processing is being delayed until all Phase 1 processing has been completed (for transaction mode).

**Recommended Action** None required.

**715022**

**Error Message** %FTD-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

**Explanation** Phase 1 processing has completed, and quick mode is being resumed.

**Recommended Action** None required.

**715027**

**Error Message** %FTD-7-715027: IPsec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPsec SA entry # crypto_map_index

**Explanation** The indicated IPsec SA proposal and transform were selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

**Recommended Action** None required.

**715028**

**Error Message** %FTD-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index

**Explanation** The indicated IKE SA transform was selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.
### 715031

**Error Message** %FTD-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)

**Explanation** This syslog is generated when the IP address is assigned by the IP util subsystem.

**Recommended Action** None required.

### 715032

**Error Message** %FTD-7-715032: Sending subnet mask (%s) to remote client

**Explanation** This syslog is generated when the IP address is assigned by the IP util subsystem.

**Recommended Action** None required.

### 715033

**Error Message** %FTD-7-715033: Processing CONNECTED notify (MsgId message_number )

**Explanation** The Firepower Threat Defense device is processing a message containing a notify payload with the notify type CONNECTED (16384). The CONNECTED notify type is used to complete the commit bit processing and should be included in the fourth overall quick mode packet, which is sent from the responder to the initiator.

**Recommended Action** None required.

### 715034

**Error Message** %FTD-7-715034: action IOS keep alive payload: proposal=time 1 /time 2 sec.

**Explanation** Processing for sending or receiving a keepalive payload message is being performed.

**Recommended Action** None required.

### 715035

**Error Message** %FTD-7-715035: Starting IOS keepalive monitor: seconds sec.

**Explanation** The keepalive timer will monitor for a variable number of seconds for keepalive messages.

**Recommended Action** None required.

### 715036

**Error Message** %FTD-7-715036: Sending keep-alive of type notify_type (seq number number )

**Explanation** Processing for sending a keepalive notify message is being performed.

**Recommended Action** None required.
715037

**Error Message** %FTD-7-715037: Unknown IOS Vendor ID version: major.minor.variance

**Explanation** The capabilities of this version of the Cisco IOS are not known.

**Recommended Action** There may be interoperability issues with features such as IKE keepalives. If the problem persists, contact the Cisco TAC.

715038

**Error Message** %FTD-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance , capabilities: value )

**Explanation** Processing for the Cisco IOS vendor ID payload has been performed. The action being performed might be Altiga spoofing the Cisco IOS.

**Recommended Action** None required.

715039

**Error Message** %FTD-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

**Explanation** An entry in the IKE tunnel table was never removed when the SA was freed. This indicates a defect in the state machine.

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

715040

**Error Message** %FTD-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle

**Error Message** The authentication handle was still active during SA deletion. This is part of cleanup recovery during the error condition.

**Recommended Action** None required.

715041

**Error Message** %FTD-7-715041: Received keep-alive of type keepalive_type , not the negotiated type

**Explanation** A keepalive of the type indicated in the message was received unexpectedly.

**Recommended Action** Check the keepalive configuration on both peers.

715042

**Error Message** %FTD-7-715042: IKE received response of type failure_type to a request from the IP_address utility
**Explanation** A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied. Variable text in the message string indicates more specifically what went wrong.

**Recommended Action** Check the IP address assignment configuration and adjust accordingly.

---

**715044**

**Error Message** %FTD-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

**Explanation** A Cisco IOS keepalive payload from a vendor was received without keepalive capabilities being set. The payload is ignored.

**Recommended Action** None required.

---

**715045**

**Error Message** %FTD-7-715045: ERROR: malformed Keepalive payload

**Explanation** A malformed keepalive payload has been received. The payload is ignored.

**Recommended Action** None required.

---

**715046**

**Error Message** %FTD-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload

**Explanation** An IP address from a remote client for a specific group and user shows details about the IKE payload being constructed.

**Recommended Action** None required.

---

**715047**

**Error Message** %FTD-7-715047: processing payload_description payload

**Explanation** Details of the IKE payload received and being processed appear.

**Recommended Action** None required.

---

**715048**

**Error Message** %FTD-7-715048: Send VID_type VID

**Explanation** The type of vendor ID payload being sent appears.

**Recommended Action** None required.

---

**715049**

**Error Message** %FTD-7-715049: Received VID_type VID

**Explanation** The type of vendor ID payload received appears.
**Recommended Action** None required.

**715050**

**Error Message** %FTD-7-715050: Claims to be IOS but failed authentication

**Explanation** The vendor ID received looks like a Cisco IOS VID, but does not match hmac_sha.

**Recommended Action** Check the vendor ID configuration on both peers. If this issue affects interoperability and the problem persists, contact the Cisco TAC.

**715051**

**Error Message** %FTD-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply

**Explanation** An unknown TLV was received in an Firepower Threat Defense record while an FWTYPE ModeCfg Reply was being processed. The TLV will be discarded. This might occur either because of packet corruption or because the connecting client supports a later version of the Firepower Threat Defense protocol.

**Recommended Action** Check the personal FW installed on the Cisco VPN client and the personal firewall configuration on the Firepower Threat Defense device. This may also indicate a version mismatch between the VPN client and the Firepower Threat Defense device.

**715052**

**Error Message** %FTD-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition entries

**Explanation** The old P1 SA is being deleted, but has no new SA to transition to because it was marked for deletion as well. This generally indicates that the two IKE peers are out-of-sync with each other and may be using different rekey times. The problem should correct itself, but there may be some small amount of data loss until a fresh P1 SA is reestablished.

**Recommended Action** None required.

**715053**

**Error Message** %FTD-7-715053: MODE_CFG: Received request for attribute_info !

**Explanation** The Firepower Threat Defense device received a mode configuration message requesting the specified attribute.

**Recommended Action** None required.

**715054**

**Error Message** %FTD-7-715054: MODE_CFG: Received attribute_name reply: value

**Explanation** The Firepower Threat Defense received a mode configuration reply message from the remote peer.

**Recommended Action** None required.
**715055**

**Error Message** %FTD-7-715055: Send attribute_name

**Explanation** The Firepower Threat Defense device sent a mode configuration message to the remote peer.

**Recommended Action** None required.

---

**715056**

**Error Message** %FTD-7-715056: Client is configured for TCP_transparency

**Explanation** Because the remote end (client) is configured for IPsec over TCP, the headend Firepower Threat Defense device must not negotiate IPsec over UDP or IPsec over NAT-T with the client.

**Recommended Action** The NAT transparency configuration may require adjustment of one of the peers if the tunnel does not come up.

---

**715057**

**Error Message** %FTD-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.

**Explanation** IPsec-over-UDP mode configuration information will not be exchanged because NAT-Traversal was detected.

**Recommended Action** None required.

---

**715058**

**Error Message** %FTD-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.

**Explanation** The remote end did not provide NAT-Discovery payloads required for NAT-Traversal after exchanging NAT-Traversal VIDs. At least two NAT-Discovery payloads must be received.

**Recommended Action** This may indicate a nonconforming NAT-T implementation. If the offending peer is a Cisco product and the problem persists, contact the Cisco TAC. If the offending peer is not a Cisco product, then contact the manufacturer support team.

---

**715059**

**Error Message** %FTD-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal

**Explanation** You need to use these modes instead of the usual transport and tunnel modes defined in the SA to successfully negotiate NAT-Traversal.

**Recommended Action** None required.

---

**715060**

**Error Message** %FTD-7-715060: Dropped received IKE fragment. Reason: reason
Explanation The reason for dropping the fragment appears.

Recommended Action The recommended action depends on the drop reason, but might indicate a problem with an intervening NAT device or a nonconforming peer.

715061

Error Message %FTD-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

Explanation A resend of the same packet occurred, but fragmented to a different MTU, or another packet altogether.

Recommended Action None required.

715062

Error Message %FTD-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

Explanation There is a gap in fragment numbers.

Recommended Action This might indicate a network problem. If the condition persists and results in dropped tunnels or prevents certain peers from negotiating with the Firepower Threat Defense device, contact the Cisco TAC.

715063

Error Message %FTD-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!

Explanation Assembly for a fragmented packet that was received was successful.

Recommended Action None required.

715064

Error Message %FTD-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true /false Aggressive Mode: true /false

Explanation The peer supports IKE fragmentation based on the information provided in the message.

Recommended Action None required.

715065

Error Message %FTD-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address ) state , event : state /event pairs

Explanation A Phase 1 error occurred and the state, event history pairs will be displayed in reverse chronological order.

Recommended Action Most of these errors are benign. If the problem persists, contact the Cisco TAC.
**715066**

**Error Message**  %FTD-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.

**Explanation**  The logical ID in the IKE SA is NULL. The Phase II negotiation will be torn down.

**Recommended Action**  An internal error has occurred. If the problem persists, contact the Cisco TAC.

---

**715067**

**Error Message**  %FTD-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

**Explanation**  The LAN-TO-LAN SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. This new SA will be deleted, because this is not a legal configuration.

**Recommended Action**  Check the LAN-TO-LAN configuration on all associated peers. Specifically, multiple peers should not be sharing private networks.

---

**715068**

**Error Message**  %FTD-7-715068: QM IsRekeyed: duplicate sa found by address , deleting old sa

**Explanation**  The remote access SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. The old SA will be deleted, because the peer may have changed its IP address.

**Recommended Action**  This may be a benign condition, especially if a client tunnel was terminated abruptly. If the problem persists, contact the Cisco TAC.

---

**715069**

**Error Message**  %FTD-7-715069: Invalid ESP SPI size of SPI_size

**Explanation**  The Firepower Threat Defense device received an IPsec SA proposal with an invalid ESP SPI size. This proposal will be skipped.

**Recommended Action**  Generally, this is a benign condition but might indicate that a peer may be nonconforming. If the problem persists, contact the Cisco TAC.

---

**715070**

**Error Message**  %FTD-7-715070: Invalid IPComp SPI size of SPI_size

**Explanation**  The Firepower Threat Defense device received an IPsec SA proposal with an invalid IPComp SPI size. This proposal will be skipped.

**Recommended Action**  Generally, this is a benign condition but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.
715071

Error Message %FTD-7-715071: AH proposal not supported
Explanation The IPsec AH proposal is not supported. This proposal will be skipped.
Recommended Action None required.

715072

Error Message %FTD-7-715072: Received proposal with unknown protocol ID protocol_ID
Explanation The Firepower Threat Defense device received an IPsec SA proposal with an unknown protocol ID. This proposal will be skipped.
Recommended Action Generally, this is a benign condition, but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.

715074

Error Message %FTD-7-715074: Could not retrieve authentication attributes for peer IP_address
Explanation The Firepower Threat Defense device cannot get authorization information for the remote user.
Recommended Action Make sure that authentication and authorization settings have been configured correctly. If the problem persists, contact the Cisco TAC.

715075

Error Message %FTD-7-715075: Group = group_name , IP = IP_address Received keep-alive of type message_type (seq number number )
Explanation This message is paired with DPD R-U-THERE message 715036, which logs the DPD sending messages.

- group_name—The VPN group name of the peer
- IP_address—IP address of the VPN peer
- message_type—The message type (DPD R-U-THERE or DPD R-U-THERE-ACK)
- number—The DPD sequence number

Two possible cases:
- Received peer sending DPD R-U-THERE message
- Received peer reply DPD R-U-THERE-ACK message

Be aware of the following:
- The DPD R-U-THERE message is received and its sequence number matches the outgoing DPD reply messages.

If the Firepower Threat Defense device sends a DPD R-U-THERE-ACK message without first receiving a DPD R-U-THERE message from the peer, it is likely experiencing a security breech.
- The received DPD R-U-THERE-ACK message's sequence number is matched with previously sent DPD messages.
If the Firepower Threat Defense device did not receive a DPD R-U-THERE-ACK message within a reasonable amount of time after sending a DPD R-U-THERE message to the peer, the tunnel is most likely down.

Recommended Action None required.

**715076**

**Error Message** %FTD-7-715076: Computing hash for ISAKMP

**Explanation** IKE computed various hash values.

This object will be prepended as follows:
Group = > groupname , Username = > username , IP = > ip_address ...

Recommended Action None required.

**715077**

**Error Message** %FTD-7-715077: Pitcher: msg string , spi spi

**Explanation** Various messages have been sent to IKE.

msg_string can be one of the following:
- Received a key acquire message
- Received SPI for nonexistent SA
- Received key delete msg
- Received KEY_UPDATE
- Received KEY_REKEY_IB
- Received KEY_REKEY_OB
- Received KEY_SA_ACTIVE
- Could not find IKE SA to activate IPSEC (OB)
- Could not find IKE SA to rekey IPSEC (OB)
- KEY_SA_ACTIVE no centry found
- KEY_ADD centry not found
- KEY_UPDATE centry not found

This object will be prepended as follows:
Group = > groupname , Username = > username , IP = > ip_address , ...

Recommended Action None required.

**715078**

**Error Message** %FTD-7-715078: Received %s LAM attribute

**Explanation** This syslog is generated during parsing of challenge/response payload.

Recommended Action None required.
715079

**Error Message** %FTD-7-715079: INTERNAL_ADDRESS: Received request for %s

**Explanation** This syslog is generated during processing of internal address payload.

**Recommended Action** None required.

715080

**Error Message** %FTD-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.

**Error Message** An IKE rekey timer has started.

**Recommended Action** None required.

Messages 716001 to 716603

This section includes messages from 716001 to 716603.

716001

**Error Message** %FTD-6-716001: Group group User user IP ip WebVPN session started.

**Explanation** The WebVPN session has started for the user in this group at the specified IP address. When the user logs in via the WebVPN login page, the WebVPN session starts.

**Recommended Action** None required.

716002

**Error Message** %FTD-6-716002: Group GroupPolicy User username IP ip WebVPN session terminated: User requested.

**Explanation** The WebVPN session has been terminated by a user request. Possible reasons include:

- Lost carrier
- Lost service
- Idle timeout
- Max time exceeded
- Administrator reset
- Administrator reboot
- Administrator shutdown
- Port error
- NAS error
- NAS request
- NAS reboot
- Port unneeded
• Port preempted. This reason indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.
• Port suspended
• Service unavailable
• Callback
• User error
• Host requested
• Bandwidth management error
• ACL parse error
• VPN simultaneous logins limit specified in the group policy
• Unknown

**Recommended Action** Unless the reason indicates a problem, then no action is required.

### 716003

**Error Message** %FTD-6-716003: Group group User user IP ip WebVPN access "GRANTED: url "

**Explanation** The WebVPN user in this group at the specified IP address has been granted access to this URL. The user access to various locations can be controlled using WebVPN-specific ACLs.

**Recommended Action** None required.

### 716004

**Error Message** %FTD-6-716004: Group group User user WebVPN access DENIED to specified location: url

**Explanation** The WebVPN user in this group has been denied access to this URL. The WebVPN user access to various locations can be controlled using WebVPN-specific ACLs. In this case, a particular entry is denying access to this URL.

**Recommended Action** None required.

### 716005

**Error Message** %FTD-6-716005: Group group User user WebVPN ACL Parse Error: reason

**Explanation** The ACL for the WebVPN user in the specified group failed to parse correctly.

**Recommended Action** Correct the WebVPN ACL.

### 716006

**Error Message** %FTD-6-716006: Group name User user WebVPN session terminated. Idle timeout.

**Explanation** The WebVPN session was not created for the user in the specified group because the VPN tunnel protocol is not set to WebVPN.

**Recommended Action** None required.
716007

**Error Message** %FTD-4-716007: Group group User user WebVPN Unable to create session.

**Explanation** The WebVPN session was not created for the user in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

**Recommended Action** None required.

716008

**Error Message** %FTD-7-716008: WebVPN ACL: action

**Explanation** The WebVPN ACL has begun performing an action (for example, begin parsing).

**Recommended Action** None required.

716009

**Error Message** %FTD-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.

**Explanation** The WebVPN session for the specified user in this group is not allowed because the associated ACL did not parse. The user will not be allowed to log in via WebVPN until this error has been corrected.

**Recommended Action** Correct the WebVPN ACL.

716010

**Error Message** %FTD-7-716010: Group group User user Browse network.

**Explanation** The WebVPN user in the specified group browsed the network.

**Recommended Action** None required.

716011

**Error Message** %FTD-7-716011: Group group User user Browse domain domain .

**Explanation** The WebVPN specified user in this group browsed the specified domain.

**Recommended Action** None required.

716012

**Error Message** %FTD-7-716012: Group group User user Browse directory directory .

**Explanation** The specified WebVPN user browsed the specified directory.

**Recommended Action** None required.
716013

**Error Message** %FTD-7-716013: Group group User user Close file filename.
**Explanation** The specified WebVPN user closed the specified file.
**Recommended Action** None required.

716014

**Error Message** %FTD-7-716014: Group group User user View file filename.
**Explanation** The specified WebVPN user viewed the specified file.
**Recommended Action** None required.

716015

**Error Message** %FTD-7-716015: Group group User user Remove file filename.
**Explanation** The WebVPN user in the specified group removed the specified file.
**Recommended Action** None required.

716016

**Error Message** %FTD-7-716016: Group group User user Rename file old_filename to new_filename.
**Explanation** The specified WebVPN user renamed the specified file.
**Recommended Action** None required.

716017

**Error Message** %FTD-7-716017: Group group User user Modify file filename.
**Explanation** The specified WebVPN user modified the specified file.
**Recommended Action** None required.

716018

**Error Message** %FTD-7-716018: Group group User user Create file filename.
**Explanation** The specified WebVPN user created the specified file.
**Recommended Action** None required.

716019

**Error Message** %FTD-7-716019: Group group User user Create directory directory.
**Explanation** The specified WebVPN user created the specified directory.
**716020**

**Recommended Action** None required.

**ErrorMessage** %FTD-7-716020: Group group User user Remove directory directory.

**Explanation** The specified WebVPN user removed the specified directory.

**Recommended Action** None required.

**716021**

**ErrorMessage** %FTD-7-716021: File access DENIED, filename.

**Explanation** The specified WebVPN user was denied access to the specified file.

**Recommended Action** None required.

**716022**

**ErrorMessage** %FTD-4-716022: Unable to connect to proxy server reason.

**Explanation** The WebVPN HTTP/HTTPS redirect failed for the specified reason.

**Recommended Action** Check the HTTP/HTTPS proxy configuration.

**716023**

**ErrorMessage** %FTD-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.

**Explanation** The user session cannot be established because the current number of sessions exceeds the maximum session load.

**Recommended Action** Increase the configured limit, if possible, to create a load-balanced cluster.

**716024**

**ErrorMessage** %FTD-7-716024: Group name User user Unable to browse the network.Error: description

**Explanation** The user was unable to browse the Windows network using the CIFS protocol, as indicated by the description. For example, “Unable to contact necessary server” indicates that the remote server is unavailable or unreachable. This might be a transient condition or may require further troubleshooting.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device.

**716025**

**ErrorMessage** %FTD-7-716025: Group name User user Unable to browse domain domain. Error: description
**Explanation** The user was unable to browse the remote domain using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Check the NetBIOS name server configuration on the Firepower Threat Defense device.

---

**716026**

**ErrorMessage**

```
%FTD-7-716026: Group name User user Unable to browse directory directory .
Error: description
```

**Explanation** The user was unable to browse the remote directory using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device.

---

**716027**

**ErrorMessage**

```
%FTD-7-716027: Group name User user Unable to view file filename . Error: description
```

**Explanation** The user was unable to view the remote file using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device.

---

**716028**

**ErrorMessage**

```
%FTD-7-716028: Group name User user Unable to remove file filename . Error: description
```

**Explanation** The user was unable to remove the remote file using the CIFS protocol, probably caused by a lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device and the file permissions.

---

**716029**

**ErrorMessage**

```
%FTD-7-716029: Group name User user Unable to rename file filename . Error: description
```

**Explanation** The user was unable to rename the remote file using the CIFS protocol, probably caused by lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device and the file permissions.
716030

**Error Message** %FTD-7-716030: Group name User user Unable to modify file filename. Error: description

**Explanation** A problem occurred when a user attempted to modify an existing file using the CIFS protocol, probably caused by a lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device and the file permissions.

716031

**Error Message** %FTD-7-716031: Group name User user Unable to create file filename. Error: description

**Explanation** A problem occurred when a user attempted to create a file using the CIFS protocol, probably caused by a file permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device and the file permissions.

716032

**Error Message** %FTD-7-716032: Group name User user Unable to create folder folder. Error: description

**Explanation** A problem occurred when a user attempted to create a folder using the CIFS protocol, probably caused by a file permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device and the file permissions.

716033

**Error Message** %FTD-7-716033: Group name User user Unable to remove folder folder. Error: description

**Explanation** A problem occurred when a user of the CIFS protocol attempted to remove a folder, which probably occurred because of a permissions problem or a problem communicating with the server on which the file resides.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Firepower Threat Defense device.

716034

**Error Message** %FTD-7-716034: Group name User user Unable to write to file filename.
Explanation A problem occurred when a user attempted to write to a file using the CIFS protocol, probably caused by a permissions problem or a problem communicating with the server on which the file resides.

Recommended Action None required.

Error Message %FTD-7-716035: Group name User user Unable to read file filename.

Explanation A problem occurred when a user of the CIFS protocol tried to read a file, probably caused by a file permissions problem.

Recommended Action Check the file permissions.

Error Message %FTD-7-716036: Group name User user File Access: User user logged into the server server.

Explanation A user successfully logged into the server using the CIFS protocol.

Recommended Action None required.

Error Message %FTD-7-716037: Group name User user File Access: User user failed to login into the server server.

Explanation A user attempted to log in to a server using the CIFS protocol, but was unsuccessful.

Recommended Action Verify that the user entered the correct username and password.

Error Message %FTD-6-716038: Group group User user IP ip Authentication: successful, Session Type: WebVPN.

Explanation Before a WebVPN session can start, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+).

Recommended Action None required.

Error Message %FTD-6-716039: Authentication: rejected, group = name user = user , Session Type: %s

Explanation Before a WebVPN session starts, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+). In this case, the user credentials (username and password) either did not match, or the user does not have permission to start a WebVPN session. The username is hidden when invalid or unknown, but appears when valid or the no logging hide username command has been configured.

• %s—The session type, which can be either WebVPN or admin
**Recommended Action** Verify the user credentials on the local or remote server and that WebVPN is configured for the user.

### 716040

**Error Message** `%FTD-6-716040: Reboot pending, new sessions disabled. Denied user login.`

**Explanation** A user was unable to log in to WebVPN because the Firepower Threat Defense device is in the process of rebooting.

- **user** — The session user

**Recommended Action** None required.

### 716041

**Error Message** `%FTD-6-716041: access-list acl_ID action url url hit_cnt count`

**Explanation** The WebVPN URL named `acl_ID` has been hit `count` times for location `url`, whose `action` is permitted or denied.

- **acl_ID** — The WebVPN URL ACL
- **count** — The number of times the URL was accessed
- **url** — The URL that was accessed
- **action** — The user action

**Recommended Action** None required.

### 716042

**Error Message** `%FTD-6-716042: access-list acl_ID action tcp source_interface /source_address (source_port) - dest_interface /dest_address (dest_port) hit_cnt count`

**Explanation** The WebVPN TCP named `acl_ID` has been hit `count` times for packet received on the source interface `source_interface/source_address` and source port `source_port` forwarded to `dest_interface/dest_address` destination `dest_port`, whose `action` is permitted or denied.

- **count** — The number of times the ACL was accessed
- **source_interface** — The source interface
- **source_address** — The source IP address
- **source_port** — The source port
- **dest_interface** — The destination interface
- **dest_address** — The destination IP address
- **action** — The user action

**Recommended Action** None required.

### 716043

**Error Message** `%FTD-6-716043 Group group-name, User user-name, IP IP_address : WebVPN Port Forwarding Java applet started. Created new hosts file mappings.`

**Explanation** The user has launched a TCP port-forwarding applet from a WebVPN session.
- **group-name**—Group name associated with the session
- **user-name**—Username associated with the session
- **IP_address**—Source IP address associated with the session

**Recommended Action** None required.

### 716044

**Error Message**  
% FTD-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.

**Explanation** The given parameter has a bad value.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address
- **param-name**—The name of the parameter
- **param-value**—The value of the parameter

**Recommended Action** Modify the configuration to correct the indicated parameter. If the parameter is vlan or nac-settings, verify that it is correctly configured on the AAA server and the Firepower Threat Defense device.

### 716045

**Error Message**  
% FTD-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.

**Explanation** The given parameter has a bad value. The value is not shown because it might be very long.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address
- **param-name**—The name of the parameter

**Recommended Action** Modify the configuration to correct the indicated parameter.

### 716046

**Error Message**  
% FTD-4-716046: Group group-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.

**Explanation** The specified ACL was not found on the Firepower Threat Defense device.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address
- **access-list-name**—The name of the ACL

**Recommended Action** Modify the configuration to add the specified ACL or to correct the ACL name.
716047

Error Message % FTD-4-716047: Group group-name User user-name IP IP_address User ACL access-list-name from AAA ignored, AV-PAIR ACL used instead.

Explanation The specified ACL was not used because a Cisco AV-PAIR ACL was used.

- group-name—The name of the group
- user-name—The name of the user
- IP_address—The IP address
- access-list-name—The name of the ACL

Recommended Action Determine the correct ACL to use and correct the configuration.

716048

Error Message % FTD-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.

Explanation There was not enough memory to parse the ACL.

- group-name—The name of the group
- user-name—The name of the user
- IP_address—The IP address

Recommended Action Purchase more memory, upgrade the Firepower Threat Defense device, or reduce the load on it.

716049

Error Message %FTD-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.

Explanation The ACL to be used by the client was empty.

- group-name—The name of the group
- user-name—The name of the user
- IP_address—The IP address

Recommended Action Determine the correct ACL to use and modify the configuration.

716050

Error Message %FTD-6-716050: Error adding to ACL: ace_command_line

Explanation The ACL entry had a syntax error.

- ace_command_line—The ACL entry that is causing the error

Recommended Action Correct the downloadable ACL configuration.

716051

Error Message %FTD-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
Explanation There is not enough memory to perform the action.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address

**Recommended Action** Purchase more memory, upgrade the Firepower Threat Defense device, or reduce the load on it.

**716052**

Error Message `%FTD-4-716052: Group group-name User user-name IP IP_address Pending session terminated.`

Explanation A user did not complete login and the pending session was terminated. This may be due to an SVC that was unable to connect.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address

**Recommended Action** Check the user PC for SVC compatibility.

**716053**

Error Message `%FTD-5-716053: SSO Server added: name: name Type: type`

Explanation The SSO server name of the specified type has been configured.

- **name**—The name of the server
- **type**—The type of the server (the only server type is SiteMinder)

**Recommended Action** None required.

**716054**

Error Message `%FTD-5-716054: SSO Server deleted: name: name Type: type`

Explanation The SSO server name of the specified type has been removed from the configuration.

- **name**—The name of the server
- **type**—The type of server (the only server type is SiteMinder)

**Recommended Action** None required.

**716055**

Error Message `%FTD-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded`

Explanation The WebVPN user has been successfully authenticated to the SSO server.

- **group-name**—The group name
- **user-name**—The username
 Syslog Messages 715001 to 721019

- **IP_address**—The IP address of the server
- **name**—The name of the server
- **type**—The type of server (the only server type is SiteMinder)

**Recommended Action** None required.

### 716056

**Error Message** `%FTD-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason`

**Explanation** The WebVPN user failed to authenticate to the SSO server.
- **group-name**—The group name
- **user-name**—The username
- **IP_address**—The IP address of the server
- **name**—The name of the server
- **type**—The type of server (the only server type is SiteMinder)
- **reason**—The reason for the authentication failure

**Recommended Action** Either the user or the Firepower Threat Defense administrator needs to correct the problem, depending on the reason for the failure.

### 716057

**Error Message** `%FTD-3-716057: Group group User user IP ip Session terminated, no type license available.`

**Explanation** A user has attempted to connect to the Firepower Threat Defense device using a client that is not licensed. This message may also occur if a temporary license has expired.
- **group**—The group policy that the user logged in with
- **user**—The name of the user
- **IP**—The IP address of the user
- **type**—The type of license requested, which can be one of the following:
  - AnyConnect Mobile
  - LinkSys Phone
  - The type of license requested by the client (if other than the AnyConnect Mobile or LinkSys Phone)
  - Unknown

**Recommended Action** A permanent license with the appropriate feature should be purchased and installed.

### 716058

**Error Message** `%FTD-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.`

**Explanation** The SSL tunnel was dropped and the AnyConnect session enters the inactive state, which can be caused by a hibernating host, a standby host, or a loss of network connectivity.
- **group**—The tunnel group name associated with the AnyConnect session
• **user** — The name of the user associated with the session
• **ip** — The source IP address of the session

**Recommended Action** None required.

### 716059

**Error Message** `%FTD-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2`.

**Explanation** An AnyConnect session resumed from the inactive state.

• **group** — The tunnel group name associated with the AnyConnect session
• **user** — The name of the user associated with the session
• **ip** — The source IP address of the session
• **ip2** — The source IP address of the host on which the session is resumed

**Recommended Action** None required.

### 716060

**Error Message** `%FTD-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.`

**Explanation** An AnyConnect session in the inactive state was logged out to allow a new incoming SSL VPN (AnyConnect or clientless) connection.

• **group** — The tunnel group name associated with the AnyConnect session
• **user** — The name of the user associated with the session
• **ip** — The source IP address of the session

**Recommended Action** None required.

### 716061

**Error Message** `%FTD-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection`.

**Explanation** The IPv6 VPN filter has been deprecated and if it is configured instead of a unified filter for IPv6 traffic access control, the connection will be terminated.

**Recommended Action** Configure a unified filter with IPv6 entries to control IPv6 traffic for the user.

### 716500

**Error Message** `%FTD-2-716500: internal error in: function : Fiber library cannot locate AK47 instance`.

**Explanation** The fiber library cannot locate the application kernel layer 4 to 7 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.
716501

**Error Message** %FTD-2-716501: internal error in: function : Fiber library cannot attach AK47 instance

**Explanation** The fiber library cannot attach the application kernel layer 4 to 7 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716502

**Error Message** %FTD-2-716502: internal error in: function : Fiber library cannot allocate default arena

**Explanation** The fiber library cannot allocate the default arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716503

**Error Message** %FTD-2-716503: internal error in: function : Fiber library cannot allocate fiber descriptors pool

**Explanation** The fiber library cannot allocate the fiber descriptors pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716504

**Error Message** %FTD-2-716504: internal error in: function : Fiber library cannot allocate fiber stacks pool

**Explanation** The fiber library cannot allocate the fiber stack pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716505

**Error Message** %FTD-2-716505: internal error in: function : Fiber has joined fiber in unfinished state

**Explanation** The fiber has joined fiber in an unfinished state.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716506

**Error Message** %FTD-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER

**Explanation** An internal fiber library was generated.

**Recommended Action** Contact the Cisco TAC.
716507

**Error Message** %FTD-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.

**Explanation** The Firepower Threat Defense device has experienced an unexpected error and has recovered.

**Recommended Action** Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.

---

716508

**Error Message** %FTD-1-716508: internal error in: function : Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating

**Explanation** The fiber scheduler is scheduling rotten fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

---

716509

**Error Message** %FTD-1-716509:internal error in: function : Fiber scheduler is scheduling alien fiber. Cannot continue terminating

**Explanation** The fiber scheduler is scheduling alien fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

---

716510

**Error Message** %FTD-1-716510:internal error in: function : Fiber scheduler is scheduling finished fiber. Cannot continue terminating

**Explanation** The fiber scheduler is scheduling finished fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

---

716512

**Error Message** %FTD-2-716512:internal error in: function : Fiber has joined fiber waited upon by someone else

**Explanation** The fiber has joined fiber that is waited upon by someone else.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

---

716513

**Error Message** %FTD-2-716513: internal error in: function : Fiber in callback blocked on other channel

**Explanation** The fiber in the callback was blocked on the other channel.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.
716515

**Error Message** %FTD-2-716515: internal error in: function : OCCAM failed to allocate memory for AK47 instance

**Explanation** The OCCAM failed to allocate memory for the AK47 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716516

**Error Message** %FTD-1-716516: internal error in: function : OCCAM has corrupted ROL array. Cannot continue terminating

**Explanation** The OCCAM has a corrupted ROL array, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716517

**Error Message** %FTD-2-716517: internal error in: function : OCCAM cached block has no associated arena

**Explanation** The OCCAM cached block has no associated arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716518

**Error Message** %FTD-2-716518: internal error in: function : OCCAM pool has no associated arena

**Explanation** The OCCAM pool has no associated arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716519

**Error Message** %FTD-1-716519: internal error in: function : OCCAM has corrupted pool list. Cannot continue terminating

**Explanation** The OCCAM has a corrupted pool list, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716520

**Error Message** %FTD-2-716520: internal error in: function : OCCAM pool has no block list

**Explanation** The OCCAM pool has no block list.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.
716521

**Error Message** %FTD-2-716521: internal error in: function : OCCAM no realloc allowed in named pool

**Explanation** The OCCAM did not allow reallocation in the named pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716522

**Error Message** %FTD-2-716522: internal error in: function : OCCAM corrupted standalone block

**Explanation** The OCCAM has a corrupted standalone block.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

716525

**Error Message** %FTD-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED

**Explanation** An internal SAL error has occurred.

**Recommended Action** Contact the Cisco TAC.

716526

**Error Message** %FTD-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL

**Explanation** A failure in the mounting of the permanent storage server directory occurred.

**Recommended Action** Contact the Cisco TAC.

716527

**Error Message** %FTD-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAIL

**Explanation** A failure in the mounting of the permanent storage file occurred.

**Recommended Action** Contact the Cisco TAC.

716528

**Error Message** %FTD-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition

**Explanation** The Firepower Threat Defense device has experienced an unexpected error and has recovered.

**Recommended Action** Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.
716600

**Error Message** %FTD-3-716600: Rejected size-recv KB Hostscan data from IP src-ip. Hostscan results exceed default | configured limit of size-conf KB.

**Explanation** When the size of the received Hostscan data exceeds the limit configured on the Firepower Threat Defense device, the data is discarded.

- **size-recv** — Size of received Hostscan data in kilobytes
- **src-ip** — Source IP address
- **default | configured** — Keyword specifying whether the value of the Hostscan data limit is the default or configured by the administrator
- **size-conf** — Configured upper limit on the size of the Hostscan data that the Firepower Threat Defense device accepts from clients

**Recommended Action** Contact Cisco TAC to increase the upper limit on the size of Hostscan data that the Firepower Threat Defense device accepts from clients.

716601

**Error Message** %FTD-3-716601: Rejected size-recv KB Hostscan data from IP src-ip. System-wide limit on the amount of Hostscan data stored on FTD exceeds the limit of data-max KB.

**Explanation** When the amount of Hostscan data stored on the Firepower Threat Defense device exceeds the limit, new Hostscan results are rejected.

- **size-recv** — Size of received Hostscan data in kilobytes
- **src-ip** — Source IP address
- **data-max** — Limit on the amount of Hostscan results to be stored by the Firepower Threat Defense device in kilobytes

**Recommended Action** Contact Cisco TAC to change the limit on stored Hostscan data.

716602

**Error Message** %FTD-3-716602: Memory allocation error. Rejected size-recv KB Hostscan data from IP src-ip.

**Explanation** An error occurred while memory was being allocated for Hostscan data.

- **size-recv** — Size of received Hostscan data in kilobytes
- **src-ip** — Source IP address

**Recommended Action** Set the Hostscan limit to the default value if it is configured. If the problem persists, contact Cisco TAC.

716603

**Error Message** %FTD-7-716603: Received size-recv KB Hostscan data from IP src-ip.

**Explanation** The Hostscan data of a specified size was successfully received.

- **size-recv** — Size of received Hostscan data in kilobytes
- **src-ip** — Source IP address
Recommended Action None required.

Messages 717001 to 717064

This section includes messages from 717001 to 717064.

717001

Error Message %FTD-3-717001: Querying keypair failed.
Explanation A required keypair was not found during an enrollment request.
Recommended Action Verify that a valid keypair exists in the trustpoint configuration, then resubmit the enrollment request.

717002

Error Message %FTD-3-717002: Certificate enrollment failed for trustpoint trustpoint_name.
Reason: reason_string.
Explanation An enrollment request for this trustpoint has failed.
• trustpoint name —Trustpoint name that the enrollment request was for
• reason_string —The reason the enrollment request failed
Recommended Action Check the CA server for the failure reason.

717003

Error Message %FTD-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
Explanation A certificate was successfully received from the CA for this trustpoint.
• trustpoint_name —Trustpoint name
Recommended Action None required

717004

Error Message %FTD-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
Explanation The trustpoint failed to export, because of one of the following: only a CA certificate exists, and an identity certificate does not exist for the trustpoint, or a required keypair is missing.
• trustpoint_name —Trustpoint name
Recommended Action Make sure that required certificates and keypairs are present for the given trustpoint.

717005

Error Message %FTD-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
Explanation The trustpoint was successfully exported.

- **trustpoint_name** — Trustpoint name

**Recommended Action** None required

---

**717006**

**Error Message** %FTD-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.

**Explanation** Import of the requested trustpoint failed to be processed.

- **trustpoint_name** — Trustpoint name

**Recommended Action** Verify the integrity of the imported data. Then make sure that the entire pkcs12 record is correctly pasted, and reimport the data.

---

**717007**

**Error Message** %FTD-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.

**Explanation** Import of the requested trustpoint was successfully completed.

- **trustpoint_name** — Trustpoint name

**Recommended Action** None required.

---

**717008**

**Error Message** %FTD-2-717008: Insufficient memory to process_requiring_memory.

**Explanation** An internal error occurred while attempting to allocate memory for the process that requires memory. Other processes may experience problems allocating memory and prevent further processing.

- **process_requiring_memory** — The specified process that requires memory

**Recommended Action** Collect memory statistics and logs for further debugging and reload the Firepower Threat Defense device.

---

**717009**

**Error Message** %FTD-3-717009: Certificate validation failed. Reason: reason_string.

**Explanation** A certificate validation failed, which might be caused by a validation attempt of a revoked certificate, invalid certificate attributes, or configuration issues.

- **reason_string** — The reason that the certificate validation failed

**Recommended Action** Make sure the configuration has a valid trustpoint configured for validation if the reason indicates that no suitable trustpoints were found. Check the Firepower Threat Defense device time to ensure that it is accurate relative to the certificate authority time. Check the reason for the failure and correct any issues that are indicated.
### 717010

**Error Message** \%FTD-3-717010: CRL polling failed for trustpoint trustpoint_name.

**Explanation** CRL polling has failed and may cause connections to be denied if CRL checking is required.

- **trustpoint_name**—The name of the trustpoint that requested the CRL

**Recommended Action** Verify that connectivity exists with the configured CRL distribution point and make sure that manual CRL retrieval also functions correctly.

### 717011

**Error Message** \%FTD-2-717011: Unexpected event event event_ID

**Explanation** An event that is not expected under normal conditions has occurred.

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

### 717012

**Error Message** \%FTD-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure

**Explanation** An attempt to refresh a cached CRL entry has failed for the specified trustpoint at the indicated time of failure. This may result in obsolete CRLs on the Firepower Threat Defense device, which may cause connections that require a valid CRL to be denied.

- **trustpoint_name**—The name of the trustpoint
- **time_of_failure**—The time of failure

**Recommended Action** Check connectivity issues to the server, such as a downed network or server. Try to retrieve the CRL manually using the `crypto ca crl retrieve` command.

### 717013

**Error Message** \%FTD-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer

**Explanation** When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. If the cache fills to the point where an incoming CRL cannot be accommodated, older CRLs will be removed until the required space is made available. This message is generated for each purged CRL.

- **issuer**—The name of the device that removes cached CRLs

**Recommended Action** None required.

### 717014

**Error Message** \%FTD-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated if a received CRL is too large to fit in the cache. Large CRLs are still supported even though they are not cached. This means that the CRL will be downloaded with each IPsec connection, which may affect performance during IPsec connection bursts.

Recommended Action None required.

717015

ErrorMessage %FTD-3-717015: CRL received from issuer is too large to process (CRL size = crl_size , maximum CRL size = max_crl_size )

Explanation An IPsec connection caused a CRL that is larger than the maximum permitted CRL size to be downloaded. This error condition causes the connection to fail. This message is rate limited to one message every 10 seconds.

Recommended Action Scalability is perhaps the most significant drawback to the CRL method of revocation checking. To solve this problem, the only options are to investigate a CA-based solution to reduce the CRL size or configure the Firepower Threat Defense device not to require CRL validation.

717016

ErrorMessage %FTD-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer

Explanation When the Firepower Threat Defense device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated when either the CA specified expiration time or the configured cache time has lapsed and the CRL is removed from the cache.

Recommended Action None required.

717017

ErrorMessage %FTD-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url

Explanation An error occurred when an attempt was made to authenticate a trustpoint by requesting a CA certificate from a certificate authority.

Recommended Action Make sure that an enrollment URL is configured with this trustpoint, ensure connectivity with the CA server, then retry the request.

717018

ErrorMessage %FTD-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries , maximum number allowed = max_allowed )

Explanation An IPsec connection caused a CRL that includes more revocation entries than can be supported to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every 10 seconds.

- issuer—The X.500 name of the CRLs issuer
• **number_of_entries**—The number of revocation entries in the received CRL
• **max_allowed**—The maximum number of CRL entries that the Firepower Threat Defense device supports

**Recommended Action** Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a CA-based solution to reduce the CRL size or configure the Firepower Threat Defense device not to require CRL validation.

**717019**

**Error Message** %FTD-3-717019: Failed to insert CRL for trustpoint trustpoint_name . Reason: failure_reason .

**Explanation** A CRL is retrieved, but found to be invalid and cannot be inserted into the cache because of the failure_reason.

• **trustpoint_name**—The name of the trustpoint that requested the CRL
• **failure_reason**—The reason that the CRL failed to be inserted into cache

**Recommended Action** Make sure that the current Firepower Threat Defense device time is correct relative to the CA time. If the NextUpdate field is missing, configure the trustpoint to ignore the NextUpdate field.

**717020**

**Error Message** %FTD-3-717020: Failed to install device certificate for trustpoint label . Reason: reason_string .

**Explanation** A failure occurred while trying to enroll or import an enrolled certificate into a trustpoint.

• **label**—Label of the trustpoint that failed to install the enrolled Firepower Threat Defense certificate
• **reason_string**—The reason that the certificate cannot be verified

**Recommended Action** Use the failure reason to remedy the cause of failure and retry the enrollment. Common failures are due to invalid certificates being imported into the Firepower Threat Defense device or a mismatch of the public key included in the enrolled certificate with the keypair referenced in the trustpoint.

**717021**

**Error Message** %FTD-3-717021: Certificate data could not be verified. Locate Reason: reason_string serial number: serial_number , subject name: subject_name , key length key_length_bits.

**Explanation** An attempt to verify the certificate that is identified by the serial number and subject name was unsuccessful for the specified reason. When verifying certificate data using the signature, several errors can occur that should be logged, including invalid key types and unsupported key size.

• **reason_string**—The reason that the certificate cannot be verified
• **serial_number**—Serial number of the certificate that is being verified
• **subject_name**—Subject name included in the certificate that is being verified
• **key_length**—The number of bits in the key used to sign this certificate

**Recommended Action** Check the specified certificate to ensure that it is valid, that it includes a valid key type, and that it does not exceed the maximum supported key size.
717022

Error Message %FTD-6-717022: Certificate was successfully validated. certificate_identifiers

Explanation The identified certificate was successfully validated.

- certificate_identifiers — Information to identify the certificate that was validated successfully, which might include a reason, serial number, subject name, and additional information

Recommended Action None required.

717023

Error Message %FTD-3-717023: SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason_string.

Explanation A failure occurred while trying to set an Firepower Threat Defense certificate for the given trustpoint for authenticating the SSL connection.

- trustpoint name — Name of the trustpoint for which SSL failed to set an Firepower Threat Defense certificate
- reason_string — Reason indicating why the Firepower Threat Defense certificate cannot be set

Recommended Action Resolve the issue indicated by the reason reported for the failure by doing the following:

- Make sure that the specified trustpoint is enrolled and has an Firepower Threat Defense certificate.
- Make sure the Firepower Threat Defense certificate is valid.
- Reenroll the trustpoint, if required.

717024

Error Message %FTD-7-717024: Checking CRL from trustpoint: trustpoint name for purpose

Explanation A CRL is being retrieved.

- trustpoint name — Name of the trustpoint for which the CRL is being retrieved
- purpose — Reason that the CRL is being retrieved

Recommended Action None required.

717025

Error Message %FTD-7-717025: Validating certificate chain containing number of certs certificate(s).

Explanation A certificate chain is being validated.

- >number of certs — Number of certificates in the chain

Recommended Action None required.

717026

Error Message %FTD-4-717026: Name lookup failed for hostname hostname during PKI operation.
Explanation The given hostname cannot be resolved while attempting a PKI operation.
  • \texttt{>hostname} — The hostname that failed to resolve

Recommended Action Check the configuration and the DNS server entries for the given hostname to make sure that it can be resolved. Then retry the operation.

717027

Error Message \texttt{%FTD-3-717027: Certificate chain failed validation. reason\_string}. 

Explanation A certificate chain cannot be validated.
  • \texttt{reason\_string} — Reason for the failure to validate the certificate chain. The reasons could be non reachability of a CA server, trustpoint not being available, the validity period for the certificate identity has elapsed, or when the certificate is revoked.

Recommended Action Resolve the issue noted by the reason and retry the validation attempt by performing any of the following actions:
  • Make sure that connectivity to a CA is available if CRL checking is required.
  • Make sure that a trustpoint is authenticated and available for validation.
  • Make sure that the identity certificate within the chain is valid based on the validity dates.
  • Make sure that the certificate is not revoked.

717028

Error Message \texttt{%FTD-6-717028: Certificate chain was successfully validated additional\_info}. 

Explanation A certificate chain was successfully validated.
  • \texttt{additional\_info} — More information for how the certificate chain was validated (for example, “with warning” indicates that a CRL check was not performed)

Recommended Action None required.

717029

Error Message \texttt{%FTD-7-717029: Identified client certificate within certificate chain. serial\_number: serial\_number, subject name: subject\_name}. 

Explanation The certificate specified as the client certificate is identified.
  • \texttt{serial\_number} — Serial number of the certificate that is identified as the client certificate
  • \texttt{subject\_name} — Subject name included in the certificate that is identified as the client certificate

Recommended Action None required.

717030

Error Message \texttt{%FTD-7-717030: Found a suitable trustpoint trustpoint\_name to validate certificate}. 

Explanation A suitable or usable trustpoint is found that can be used to validate the certificate.
• **trustpoint name** — Trustpoint that will be used to validate the certificate

**Recommended Action** None required.

---

**717031**

**Error Message** FTD-4-717031: Failed to find a suitable trustpoint for the issuer: *issuer*

**Reason:** *reason_string*

**Explanation** A usable trustpoint cannot be found. During certificate validation, a suitable trustpoint must be available in order to validate a certificate.

- >*issuer* — Issuer of the certificate that was being validated
- *reason_string* — The reason that a suitable trustpoint cannot be found

**Recommended Action** Resolve the issue indicated in the reason by checking the configuration to make sure that a trustpoint is configured, authenticated, and enrolled. Also make sure that the configuration allows for specific types of certificates, such as identity certificates.

---

**717033**

**Error Message** FTD-6-717033: OCSP response status - Successful.

**Explanation** An OCSP status check response was received successfully.

**Recommended Action** None required.

---

**717034**

**Error Message** FTD-7-717034: No-check extension found in certificate. OCSP check bypassed.

**Explanation** An OCSP responder certificate was received that includes an “id-pkix-ocsp-nocheck” extension, which allows this certificate to be validated without an OCSP status check.

**Recommended Action** None required.

---

**717035**

**Error Message** FTD-4-717035: OCSP status is being checked for certificate. *certificate_identifier*.

**Explanation** The certificate for which an OCSP check occurs is identified.

- *certificate_identifier* — Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** None required.

---

**717036**

**Error Message** FTD-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with *certificate_identifier*.
**Explanation** The peer certificate identified by the certificate identifier is being processed through the configured certificate maps to attempt a possible tunnel group match.

- *certificate_identifier* — Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** None required.

---

**717037**

**Error Message** %FTD-4-717037: Tunnel group search using certificate maps failed for peer certificate: *certificate_identifier*.

**Explanation** The peer certificate identified by the certificate identifier was processed through the configured certificate maps to attempt a possible tunnel group match, but no match can be found.

- *certificate_identifier* — Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** Make sure that the warning is expected based on the received peer certificate and the configured crypto CA certificate map rules.

---

**717038**

**Error Message** %FTD-7-717038: Tunnel group match found. Tunnel Group: *tunnel_group_name*, Peer certificate: *certificate_identifier*.

**Explanation** The peer certificate identified by the certificate identifier was processed by the configured certificate maps, and a match was found to the tunnel group.

- *certificate_identifier* — Information that identifies the certificate being processed by the certificate map rules
- *tunnel_group_name* — The name of the tunnel group matched by the certificate map rules

**Recommended Action** None required.

---

**717050**

**Error Message** %FTD-5-717050: SCEP Proxy: Processed request type *type* from IP *client_ip_address*, User *username*, TunnelGroup *tunnel_group_name*, GroupPolicy *group-policy_name* to CA IP *ca_ip_address*.

**Explanation** The SCEP proxy received a message and relayed it to the CA. The response from the CA is relayed back to the client.

- *type* — The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- *client_ip_address* — The source IP address of the request received
- *username* — The username that is associated with the VPN session in which the SCEP request is received
- *tunnel-group name* — The tunnel group that is associated with the VPN session in which the SCEP request is received
- *group-policy name* — The group policy that is associated with the VPN session in which the SCEP request is received
- *ca_ip_address* — The IP address of the CA that is configured in the group policy
Recommended Action None required.

717051

Error Message %FTD-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address, User username, TunnelGroup tunnel group name, GroupPolicy group policy name to CA ca ip address. Reason: msg

Explanation The SCEP proxy denied processing of the request, which may be caused by a misconfiguration, an error condition in the proxy, or an invalid request.

- type — The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- client ip address — The source IP address of the request received
- username — The username that is associated with the VPN session in which the SCEP request is received
- tunnel-group name — The tunnel group that is associated with the VPN session in which the SCEP request is received
- group-policy name — The group policy that is associated with the VPN session in which the SCEP request is received
- ca ip address — The IP address of the CA that is configured in the group policy
- msg — The reason string that explains the reason or error for why the request processing is denied

Recommended Action Identify the cause from the reason printed. If the reason indicates that the request is invalid, check the CA URL configuration. Otherwise, confirm that the tunnel group is enabled for SCEP enrollment and debug further by using the debug crypto ca scep-proxy command.

717052

Error Message %FTD-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number

Explanation Periodic certificate authentication failed, and the session was disconnected.

- group name — The name of the group policy to which the session belongs
- user name — The username of the session
- IP — The public IP address of the session
- id subject name — The subject name in the ID certificate of the session
- id issuer name — The issuer name in the ID certificate of the session
- id serial number — The serial number in the ID certificate of the session

Recommended Action None required.

717053

SSP-whole topic

Error Message %FTD-5-717053: Group group name User user name IP IP Address Periodic certificate authentication succeeded. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number

Explanation Periodic certificate authentication succeeded.
• **group name** — The name of the group policy to which the session belongs
• **user name** — The username of the session
• **id subject name** — The subject name in the ID certificate of the session
• **id issuer name** — The issuer name in the ID certificate of the session
• **id serial number** — The serial number in the ID certificate of the session

**Recommended Action** None required.

---

**717054**

SSP-whole topic

**ErrorMessage** %FTD-1-717054: The type certificate in the trustpoint *tp name* is due to expire in *number* days. Expiration date and time Subject Name *subject name* Issuer Name *issuer name* Serial Number *serial number*

**Explanation** The specified certificate in the trustpoint is about to expire.

• **type** — The type of certificate: CA or ID
• **tp name** — The name of the trustpoint to which the certificate belongs
• **number** — The number of days until expiration
• **date and time** — The expiration date and time
• **subject name** — The subject name in the certificate
• **issuer name** — The issuer name in the certificate
• **serial number** — The serial number in the certificate

**Recommended Action** Renew the certificate.

---

**717055**

**ErrorMessage** %FTD-1-717055: The type certificate in the trustpoint *tp name* has expired.

**Explanation** The specified certificate in the trustpoint has expired.

• **type** — The type of certificate: CA or ID
• **tp name** — The name of the trustpoint to which the certificate belongs
• **date and time** — The expiration date and time
• **subject name** — The subject name in the certificate
• **issuer name** — The issuer name in the certificate
• **serial number** — The serial number in the certificate

**Recommended Action** Renew the certificate.

---

**717056**

Only heading title SSP

**ErrorMessage** %FTD-6-717056: Attempting type revocation check from *Src Interface :Src IP /Src Port* to *Dst IP /Dst Port* using *protocol*

**Explanation** The CA was attempting to download a CRL or send an OCSP revocation check request.
Syslog Messages 715001 to 721019

- **type** — Type of revocation check, which can be OCSP or CRL
- **Src Interface** — Name of the interface from which the revocation checking is being done
- **Src IP** — IP address from which the revocation checking is being done
- **Src Port** — Port number from which the revocation checking is being done
- **Dst IP** — IP address of the server to which the revocation checking request is being sent
- **Dst Port** — Port number of the server to which the revocation checking request is being sent
- **Protocol** — Protocol being used for revocation checking, which can be HTTP, LDAP, or SCEP

**Recommended Action** None required.

**717057**

**Error Message** %FTD-3-717057: Automatic import of trustpool certificate bundle has failed. 
Maximum retry attempts reached. Failed to reach CA server | Cisco root bundle signature validation failed | Failed to update trustpool bundle in flash | Failed to install trustpool bundle in memory

**Explanation** This syslog is generated with one of these error messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages especially in cases of failure. Details of each error are present in the debug output.

**Recommended Action** Verify CA accessibility and make space on flash CA root certificate.

**717058**

**Error Message** %FTD-6-717058: Automatic import of trustpool certificate bundle is successful: 
No change in trustpool bundle | Trustpool updated in flash.

**Explanation** This syslog is generated with one of these success messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages, especially in cases of failure. Details of each error are present in the debug output.

**Recommended Action** None.

**717059**

**Error Message** %FTD-6-717059: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> matched the configured certificate map <map_name>

**Explanation** This log is generated when an ASDM connection is authenticated via certificates and allowed based on the configured certificate map rules.

**Recommended Action** None required.

**717060**

**Error Message** %FTD-3-717060: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> failed to match the configured certificate map <map_name>

**Explanation** This log is generated when an ASDM connection is authenticated via certificates and not allowed based on the configured certificate map rules.

---

Cisco Firepower Threat Defense Syslog Messages 331
**Recommended Action** If the peer certificate referenced in the log is supposed to be allowed, check certificate map configuration for the referenced map_name and correct the map to allow the connection as needed.

### 717061

**SSP-only heading title**

**Error Message** `%FTD-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name. Request Type type Mode mode`

**Explanation** A CMP enrollment request has been triggered.

- `tpname` — Name of the trustpoint being enrolled
- `ca` — CA hostname or IP address as provided in the CMP configuration
- `type` — CMP request type: Initialization Request, Certification Request, and Key Update Request
- `mode` — Enrollment trigger: Manual or Automatic
- `protocol` — Enrollment protocol: CMP

**Recommended Action** None required.

### 717062

**Error Message** `%FTD-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial`

**Explanation** CMP enrollment request succeeded. New certificate received.

- `tpname` — Name of the trustpoint being enrolled
- `ca` — CA hostname or IP address as provided in the CMP configuration
- `subject` — Subject Name from the received certificate
- `issuer` — Issuer Name from the received certificate
- `serial` — Serial Number from the received certificate
- `protocol` — Enrollment protocol: CMP

**Recommended Action** None required.

### 717063

**SSP Only heading title**

**Error Message** `%FTD-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca`

**Explanation** CMP enrollment request failed.

- `tpname` — Name of the trustpoint being enrolled
- `ca` — CA hostname or IP address as provided in the CMP configuration
- `protocol` — Enrollment protocol: CMP

**Recommended Action** Use the CMP debug traces to fix the enrollment failure.
**Error Message** %FTD-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal

**Explanation** The keypair in the trustpoint is regenerated for certificate enrollment using CMP.

- **tpname** — Name of the trustpoint being enrolled
- **keyname** — Name of the keypair in the trustpoint
- **mode** — Enrollment trigger: Manual or Automatic
- **protocol** — Enrollment protocol: CMP

**Recommended Action** None required.

**Messages 718001 to 719026**

This section includes messages from 718001 to 719026.

**718001**

**Error Message** %FTD-7-718001: Internal interprocess communication queue send failure: code error_code

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

**718002**

**Error Message** %FTD-5-718002: Create peer IP_address failure, already at maximum of number_of_peers

**Explanation** The maximum number of load-balancing peers has been exceeded. The new peer is ignored.

**Recommended Action** Check your load balancing and network configuration to ensure that the number of load-balancing peers does not exceed the maximum allowed.

**718003**

**Error Message** %FTD-6-718003: Got unknown peer message message_number from IP_address , local version version_number , remote version version_number

**Explanation** An unrecognized load-balancing message was received from one of the load-balancing peers. This may indicate a version mismatch between peers, but is most likely caused by an internal software error.

**Recommended Action** Verify that all load-balancing peers are compatible. If they are and this condition persists or is linked to undesirable behavior, contact the Cisco TAC.
718004

**Error Message**  %FTD-6-718004: Got unknown internal message message_number

**Explanation**  An internal software error occurred.

**Recommended Action**  This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718005

**Error Message**  %FTD-5-718005: Fail to send to IP_address , port port

**Explanation**  An internal software error occurred during packet transmission on the load-balancing socket. This might indicate a network problem.

**Recommended Action**  Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

718006

**Error Message**  %FTD-5-718006: Invalid load balancing state transition [cur-state_number ][event=event_number ]

**Explanation**  A state machine error has occurred. This might indicate an internal software error.

**Recommended Action**  This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718007

**Error Message**  %FTD-5-718007: Socket open failure failure_code

**Explanation**  An error occurred when the load-balancing socket tried to open. This might indicate a network problem or an internal software error.

**Recommended Action**  Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

718008

**Error Message**  %FTD-5-718008: Socket bind failure failure_code

**Explanation**  An error occurred when the Firepower Threat Defense device tried to bind to the load-balancing socket. This might indicate a network problem or an internal software error.

**Recommended Action**  Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

718009

**Error Message**  %FTD-5-718009: Send HELLO response failure to IP_address
**Explanation** An error occurred when the Firepower Threat Defense device tried to send a hello response message to one of the load-balancing peers. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

**718010**

**Error Message** `%FTD-5-718010: Sent HELLO response to IP_address`

**Explanation** The Firepower Threat Defense device transmitted a hello response message to a load-balancing peer.

**Recommended Action** None required.

**718011**

**Error Message** `%FTD-5-718011: Send HELLO request failure to IP_address`

**Explanation** An error occurred when the Firepower Threat Defense device tried to send a hello request message to one of the load-balancing peers. This may indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

**718012**

**Error Message** `%FTD-5-718012: Sent HELLO request to IP_address`

**Explanation** The Firepower Threat Defense device transmitted a hello request message to a load-balancing peer.

**Recommended Action** None required.

**718013**

**Error Message** `%FTD-6-718013: Peer IP_address is not answering HELLO`

**Explanation** The load-balancing peer is not answering a hello request message.

**Recommended Action** Check the status of the load-balancing SSF peer and the network connections.

**718014**

**Error Message** `%FTD-5-718014: Master peer IP_address is not answering HELLO`

**Explanation** The load balancing master peer is not answering the hello request message.

**Recommended Action** Check the status of the load balancing SSF master peer and the network connections.
718015

**ErrorMessage**  %FTD-5-718015: Received HELLO request from IP_address

**Explanation** The Firepower Threat Defense device received a hello request message from the load balancing peer.

**Recommended Action** None required.

718016

**ErrorMessage**  %FTD-5-718016: Received HELLO response from IP_address

**Explanation** The Firepower Threat Defense device received a Hello Response packet from a load balancing peer.

**Recommended Action** None required.

718017

**ErrorMessage**  %FTD-7-718017: Got timeout for unknown peer IP_address msg type message_type

**Explanation** The Firepower Threat Defense device processed a timeout for an unknown peer. The message was ignored because the peer may have already been removed from the active list.

**Recommended Action** If the message persists or is linked to undesirable behavior, check the load balancing peers and verify that all are configured correctly.

718018

**ErrorMessage**  %FTD-7-718018: Send KEEPALIVE request failure to IP_address

**Explanation** An error has occurred while attempting to send a Keepalive Request message to one of the load balancing peers. This indicates a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

718019

**ErrorMessage**  %FTD-7-718019: Sent KEEPALIVE request to IP_address

**Explanation** The Firepower Threat Defense device transmitted a Keepalive Request message to a load balancing peer.

**Recommended Action** None required.

718020

**ErrorMessage**  %FTD-7-718020: Send KEEPALIVE response failure to IP_address
**718021**

**Error Message** %FTD-7-718021: Sent KEEPALIVE response to IP_address

**Explanation** The Firepower Threat Defense device transmitted a Keepalive Response message to a load balancing peer.

**Recommended Action** None required.

**718022**

**Error Message** %FTD-7-718022: Received KEEPALIVE request from IP_address

**Explanation** The Firepower Threat Defense device received a Keepalive Request message from a load balancing peer.

**Recommended Action** None required.

**718023**

**Error Message** %FTD-7-718023: Received KEEPALIVE response from IP_address

**Explanation** The Firepower Threat Defense device received a Keepalive Response message from a load balancing peer.

**Recommended Action** None required.

**718024**

**Error Message** %FTD-5-718024: Send CFG UPDATE failure to IP_address

**Explanation** An error has occurred while attempting to send a Configuration Update message to one of the load balancing peers. This may indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

**718025**

**Error Message** %FTD-7-718025: Sent CFG UPDATE to IP_address

**Explanation** The Firepower Threat Defense device transmitted a Configuration Update message to a load balancing peer.

**Recommended Action** None required.
Error Message %FTD-7-718026: Received CFG UPDATE from IP_address
Explanation The Firepower Threat Defense device received a Configuration Update message from a load balancing peer.
Recommended Action None required.

Error Message %FTD-6-718027: Received unexpected KEEPALIVE request from IP_address
Explanation The Firepower Threat Defense device received an unexpected Keepalive request message from a load balancing peer.
Recommended Action If the problem persists or is linked with undesirable behavior, verify that all load balancing peers are configured and discovered correctly.

Error Message %FTD-5-718028: Send OOS indicator failure to IP_address
Explanation An error has occurred while attempting to send an OOS indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.
Recommended Action Check the network-based configuration on the Firepower Threat Defense device and verify that interfaces are active and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

Error Message %FTD-7-718029: Sent OOS indicator to IP_address
Explanation The Firepower Threat Defense device transmitted an OOS indicator message to a load balancing peer.
Recommended Action None required.

Error Message %FTD-6-718030: Received planned OOS from IP_address
Explanation The Firepower Threat Defense device received a planned OOS message from a load balancing peer.
Recommended Action None required.

Error Message %FTD-5-718031: Received OOS obituary for IP_address
Explanation The Firepower Threat Defense device received an OOS obituary message from a load balancing peer.

Recommended Action None required.

718032

Error Message %FTD-5-718032: Received OOS indicator from IP_address

Explanation The Firepower Threat Defense device received an OOS indicator message from a load balancing peer.

Recommended Action None required.

718033

Error Message %FTD-5-718033: Send TOPOLOGY indicator failure to IP_address

Explanation An error has occurred while attempting to send a Topology indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Firepower Threat Defense device. Verify that interfaces are active, and protocol data is flowing through the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

718034

Error Message %FTD-7-718034: Sent TOPOLOGY indicator to IP_address

Explanation The Firepower Threat Defense device sent a Topology indicator message to a load balancing peer.

Recommended Action None required.

718035

Error Message %FTD-7-718035: Received TOPOLOGY indicator from IP_address

Explanation The Firepower Threat Defense device received a Topology indicator message from a load balancing peer.

Recommended Action None required.

718036

Error Message %FTD-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address

Explanation The Firepower Threat Defense device processed a peer timeout.

Recommended Action Verify that the peer should have been timed out. If not, check the load balancing peer configuration and the network connection between the peer and the Firepower Threat Defense device.
Error Message  %FTD-6-718037: Master processed number_of_timeouts timeouts
Explanation The Firepower Threat Defense device in the master role processed the specified number of peer timeouts.
Recommended Action Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Firepower Threat Defense device.

Error Message  %FTD-6-718038: Slave processed number_of_timeouts timeouts
Explanation The Firepower Threat Defense device in the slave role processed the specified number of peer timeouts.
Recommended Action Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Firepower Threat Defense device.

Error Message  %FTD-6-718039: Process dead peer IP_address
Explanation The Firepower Threat Defense device has detected a dead peer.
Recommended Action Verify that the dead peer detection is legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Firepower Threat Defense device.

Error Message  %FTD-6-718040: Timed-out exchange ID exchange_ID not found
Explanation The Firepower Threat Defense device has detected a dead peer, but the exchange ID is not recognized.
Recommended Action None required.

Error Message  %FTD-7-718041: Timeout [msgType-type] processed with no callback
Explanation The Firepower Threat Defense device has detected a dead peer, but a callback was not used in the processing.
Recommended Action None required.

Error Message  %FTD-5-718042: Unable to ARP for IP_address
Explanation The Firepower Threat Defense device experienced an ARP failure when attempting to contact a peer.
Recommended Action Verify that the network is operational and that all peers can communicate with each other.

718043

ErrorMessage %FTD-5-718043: Updating/removing duplicate peer entry IP_address
Explanation The Firepower Threat Defense device found and is removing a duplicate peer entry.
Recommended Action None required.

718044

ErrorMessage %FTD-5-718044: Deleted peer IP_address
Explanation The Firepower Threat Defense device is deleting a load balancing peer.
Recommended Action None required.

718045

ErrorMessage %FTD-5-718045: Created peer IP_address
Explanation The Firepower Threat Defense device has detected a load balancing peer.
Recommended Action None required.

718046

ErrorMessage %FTD-7-718046: Create group policy policy_name
Explanation The Firepower Threat Defense device has created a group policy to securely communicate with the load balancing peers.
Recommended Action None required.

718047

ErrorMessage %FTD-7-718047: Fail to create group policy policy_name
Explanation The Firepower Threat Defense device experienced a failure when attempting to create a group policy for securing the communication between load balancing peers.
Recommended Action Verify that the load balancing configuration is correct.

718048

ErrorMessage %FTD-5-718048: Create of secure tunnel failure for peer IP_address
Explanation The Firepower Threat Defense device experienced a failure when attempting to establish an IPsec tunnel to a load balancing peer.
Recommended Action Verify that the load balancing configuration is correct and that the network is operational.
718049

**Error Message** %FTD-7-718049: Created secure tunnel to peer IP_address

**Explanation** The Firepower Threat Defense device successfully established an IPsec tunnel to a load balancing peer.

**Recommended Action** None required.

718050

**Error Message** %FTD-5-718050: Delete of secure tunnel failure for peer IP_address

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to terminate an IPsec tunnel to a load balancing peer.

**Recommended Action** Verify that the load balancing configuration is correct and that the network is operational.

718051

**Error Message** %FTD-6-718051: Deleted secure tunnel to peer IP_address

**Explanation** The Firepower Threat Defense device successfully terminated an IPsec tunnel to a load balancing peer.

**Recommended Action** None required.

718052

**Error Message** %FTD-5-718052: Received GRAT-ARP from duplicate master MAC_address

**Explanation** The Firepower Threat Defense device received a gratuitous ARP from a duplicate master.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

718053

**Error Message** %FTD-5-718053: Detected duplicate master, mastership stolen MAC_address

**Explanation** The Firepower Threat Defense device detected a duplicate master and a stolen master.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

718054

**Error Message** %FTD-5-718054: Detected duplicate master MAC_address and going to SLAVE

**Explanation** The Firepower Threat Defense device detected a duplicate master and is switching to slave mode.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.
718055

**Error Message** %FTD-5-718055: Detected duplicate master MAC_address and staying MASTER

**Explanation** The Firepower Threat Defense device detected a duplicate master and is staying in slave mode.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

718056

**Error Message** %FTD-7-718056: Deleted Master peer, IP IP_address

**Explanation** The Firepower Threat Defense device deleted the load balancing master from its internal tables.

**Recommended Action** None required.

718057

**Error Message** %FTD-5-718057: Queue send failure from ISR, msg type failure_code

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue from an Interrupt Service Routing.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718058

**Error Message** %FTD-7-718058: State machine return code: action_routine, return_code

**Explanation** The return codes of action routines belonging to the load balancing finite state machine are being traced.

**Recommended Action** None required.

718059

**Error Message** %FTD-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine

**Explanation** The events and states of the load balancing finite state machine are being traced.

**Recommended Action** None required.

718060

**Error Message** %FTD-5-718060: Inbound socket select fail: context=context_ID

**Explanation** The socket select call returned an error and the socket cannot be read. This might indicate an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.
718061

**Error Message** %FTD-5-718061: Inbound socket read fail: context=\context_ID\.

**Explanation** The socket read failed after data was detected through the select call. This might indicate an internal software error.

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

718062

**Error Message** %FTD-5-718062: Inbound thread is awake (context=\context_ID\).

**Explanation** The load balancing process is awakened and begins processing.

**Recommended Action** None required.

718063

**Error Message** %FTD-5-718063: Interface \interface_name\ is down.

**Explanation** The load balancing process found the interface down.

**Recommended Action** Check the interface configuration to make sure that the interface is operational.

718064

**Error Message** %FTD-5-718064: Admin. interface \interface_name\ is down.

**Explanation** The load balancing process found the administrative interface down.

**Recommended Action** Check the administrative interface configuration to make sure that the interface is operational.

718065

**Error Message** %FTD-5-718065: Cannot continue to run {public-up /down , private-up /down , enable-LB_state , master-IP_address , session-Enable /Disable }.

**Explanation** The load balancing process can not run because all prerequisite conditions have not been met. The prerequisite conditions are two active interfaces and load balancing enabled.

**Recommended Action** Check the interface configuration to make sure at least two interfaces are operational and load balancing is enabled.

718066

**Error Message** %FTD-5-718066: Cannot add secondary address to interface \interface_name\, ip \IP_address\.

**Explanation** Load balancing requires a secondary address to be added to the outside interface. A failure occurred in adding that secondary address.
**Recommended Action** Check the address being used as the secondary address and make sure that it is valid and unique. Check the configuration of the outside interface.

**718067**

**Error Message** %FTD-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.

**Explanation** The deletion of the secondary address failed, which might indicate an addressing problem or an internal software error.

**Recommended Action** Check the addressing information of the outside interface and make sure that the secondary address is valid and unique. If the problem persists, contact the Cisco TAC.

**718068**

**Error Message** %FTD-5-718068: Start VPN Load Balancing in context context_ID.

**Explanation** The load balancing process has been started and initialized.

**Recommended Action** None required.

**718069**

**Error Message** %FTD-5-718069: Stop VPN Load Balancing in context context_ID.

**Explanation** The load balancing process has been stopped.

**Recommended Action** None required.

**718070**

**Error Message** %FTD-5-718070: Reset VPN Load Balancing in context context_ID.

**Explanation** The LB process has been reset.

**Recommended Action** None required.

**718071**

**Error Message** %FTD-5-718071: Terminate VPN Load Balancing in context context_ID.

**Explanation** The LB process has been terminated.

**Recommended Action** None required.

**718072**

**Error Message** %FTD-5-718072: Becoming master of Load Balancing in context context_ID.

**Explanation** The Firepower Threat Defense device has become the LB master.

**Recommended Action** None required.
718073

**Error Message** %FTD-5-718073: Becoming slave of Load Balancing in context context_ID.

**Explanation** The Firepower Threat Defense device has become the LB slave.

**Recommended Action** None required.

718074

**Error Message** %FTD-5-718074: Fail to create access list for peer context_ID.

**Explanation** ACLs are used to create secure tunnels over which the LB peers can communicate. The Firepower Threat Defense device was unable to create one of these ACLs. This might indicate an addressing problem or an internal software problem.

**Recommended Action** Check the addressing information of the inside interface on all peers and ensure that all peers are discovered correctly. If the problem persists, contact the Cisco TAC.

718075

**Error Message** %FTD-5-718075: Peer IP_address access list not set.

**Explanation** While removing a secure tunnel, the Firepower Threat Defense device detected a peer entry that did not have an associated ACL.

**Recommended Action** None required.

718076

**Error Message** %FTD-5-718076: Fail to create tunnel group for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when trying to create a tunnel group for securing the communication between load balancing peers.

**Recommended Action** Verify that the load balancing configuration is correct.

718077

**Error Message** %FTD-5-718077: Fail to delete tunnel group for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to delete a tunnel group for securing the communication between load balancing peers.

**Recommended Action** None required.

718078

**Error Message** %FTD-5-718078: Fail to create crypto map for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to create a crypto map for securing the communication between load balancing peers.

**Recommended Action** Verify that the load balancing configuration is correct.
718079

**Error Message** %FTD-5-718079: Fail to delete crypto map for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to delete a crypto map for securing the communication between load balancing peers.

**Recommended Action** None required.

718080

**Error Message** %FTD-5-718080: Fail to create crypto policy for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to create a transform set to be used in securing the communication between load balancing peers. This might indicate an internal software problem.

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

718081

**Error Message** %FTD-5-718081: Fail to delete crypto policy for peer IP_address.

**Explanation** The Firepower Threat Defense device experienced a failure when attempting to delete a transform set used in securing the communication between load balancing peers.

**Recommended Action** None required.

718082

**Error Message** %FTD-5-718082: Fail to create crypto ipsec for peer IP_address.

**Explanation** When cluster encryption for VPN load balancing is enabled, the VPN load balancing device creates a set of site-to-site tunnels for every other device in the load balancing cluster. For each tunnel, a set of crypto parameters (access list, crypto maps, and transform set) is created dynamically. One or more crypto parameters failed to be created or configured.

- **IP_address**—The IP address of the remote peer

**Recommended Action** Examine the message for other entries specific to the type of crypto parameters that failed to be created.

718083

**Error Message** %FTD-5-718083: Fail to delete crypto ipsec for peer IP_address.

**Explanation** When the local VPN load balancing device is removed from the cluster, crypto parameters are removed. One or more crypto parameters failed to be deleted.

- **IP_address**—The IP address of the remote peer

**Recommended Action** Examine the message for other entries specific to the type of crypto parameters that failed to be deleted.
718084

Error Message %FTD-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address

Explanation The cluster IP address is not on the same network as the outside interface of the Firepower Threat Defense device.

Recommended Action Make sure that both the cluster (or virtual) IP address and the outside interface address are on the same network.

718085

Error Message %FTD-5-718085: Interface interface_name has no IP address defined.

Explanation The interface does not have an IP address configured.

Recommended Action Configure an IP address for the interface.

718086

Error Message %FTD-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.

Explanation The Firepower Threat Defense device experienced a failure when attempting to create a SoftNP ACL rule to be used in securing the communication between load balancing peers. This may indicate an internal software problem.

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

718087

Error Message %FTD-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.

Explanation The Firepower Threat Defense device experienced a failure when attempting to delete the SoftNP ACL rule used in securing the communication between load balancing peers.

Recommended Action None required.

718088

Error Message %FTD-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.

Explanation The presence of a duplicate master indicates that one of the load balancing peers may be misconfigured.

Recommended Action Check the load balancing configuration on all peers, but pay special attention to the peer identified.
719001

**Error Message** %FTD-6-719001: Email Proxy session could not be established: session limit of *maximum_sessions* has been reached.

**Explanation** The incoming e-mail proxy session cannot be established because the maximum session limit has been reached.

- *maximum_sessions*—The maximum session number

**Recommended Action** None required.

719002

**Error Message** %FTD-3-719002: Email Proxy session pointer from *source_address* has been terminated due to *reason* error.

**Explanation** The session has been terminated because of an error. The possible errors are failure to add a session to the session database, failure to allocate memory, and failure to write data to a channel.

- *pointer*—The session pointer
- *source_address*—The e-mail proxy client IP address
- *reason*—The error type

**Recommended Action** None required.

719003

**Error Message** %FTD-6-719003: Email Proxy session pointer resources have been freed for *source_address*.

**Explanation** The dynamic allocated session structure has been freed and set to NULL after the session terminated.

- *pointer*—The session pointer
- *source_address*—The e-mail proxy client IP address

**Recommended Action** None required.

719004

**Error Message** %FTD-6-719004: Email Proxy session pointer has been successfully established for *source_address*.

**Explanation** A new incoming e-mail client session has been established.

**Recommended Action** None required.

719005

**Error Message** %FTD-7-719005: FSM NAME has been created using *protocol* for session pointer from *source_address*.

**Explanation** The FSM has been created for an incoming new session.
• NAME—The FSM instance name for the session
• protocol—The e-mail protocol type (for example, POP3, IMAP, and SMTP)
• pointer—The session pointer
• source_address—The e-mail proxy client IP address

Recommended Action None required.

719006

Error Message %FTD-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.

Explanation Network congestion is occurring, and data cannot be sent to either an e-mail client or an e-mail server. This condition starts the block timer. After the block timer is timed out, the session expires.
• pointer—The session pointer
• source_address—The e-mail proxy client IP address

Recommended Action Retry the operation after a few minutes.

719007

Error Message %FTD-7-719007: Email Proxy session pointer cannot be found for source_address.

Explanation A matching session cannot be found in the session database. The session pointer is bad.
• pointer—The session pointer
• source_address—The e-mail proxy client IP address

Recommended Action None required.

719008

Error Message %FTD-3-719008: Email Proxy service is shutting down.

Explanation The e-mail proxy is disabled. All resources are cleaned up, and all threads are terminated.

Recommended Action None required.

719009

Error Message %FTD-7-719009: Email Proxy service is starting.

Explanation The e-mail proxy is enabled.

Recommended Action None required.

719010

Error Message %FTD-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
**Explanation** The e-mail proxy feature is disabled on a specific entry point, invoked from the CLI. This is the main off switch for the user. When all protocols are turned off for all interfaces, the main shut-down routine is invoked to clean up global resources and threads.

- **protocol** — The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface name** — The Firepower Threat Defense interface name

**Recommended Action** None required.

### 719011

**Error Message** %FTD-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.

**Explanation** The e-mail proxy feature is enabled on a specific entry point, invoked from the CLI. This is the main on switch for the user. When it is first used, the main startup routine is invoked to allocate global resources and threads. Subsequent calls only need to start listening threads for the particular protocol.

- **protocol** — The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface name** — The Firepower Threat Defense interface name

**Recommended Action** None required.

### 719012

**Error Message** %FTD-6-719012: Email Proxy server listening on port port for mail protocol protocol.

**Explanation** A listening channel is opened for a specific protocol on a configured port and has added it to a TCP select group.

- **port** — The configured port number
- **protocol** — The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

**Recommended Action** None required.

### 719013

**Error Message** %FTD-6-719013: Email Proxy server closing port port for mail protocol protocol.

**Explanation** A listening channel is closed for a specific protocol on a configured port and has removed it from the TCP select group.

- **port** — The configured port number
- **protocol** — The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

**Recommended Action** None required.

### 719014

**Error Message** %FTD-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.

---

Cisco Firepower Threat Defense Syslog Messages
**Explanation** A change is signaled in the listening port for the specified protocol. All enabled interfaces for that port have their listening channels closed and have restarted listening on the new port. This action is invoked from the CLI.

- **old_port**—The previously configured port number
- **new_port**—The newly configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

**Recommended Action** None required.

---

**Error Message** %FTD-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user , vpnuser = VPN_user , mailserver = server

**Explanation** The username string is received from the client in the format vpnuser (name delimiter) mailuser (server delimiter) mailserver (for example: xxx:yyy@cisco.com). The name delimiter is optional. When the delimiter is not there, the VPN username and mail username are the same. The server delimiter is optional. When it is not present, the default configured mail server will be used.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address
- **mail_user**—The e-mail account username
- **VPN_user**—The WebVPN username
- **server**—The e-mail server

**Recommended Action** None required.

---

**Error Message** %FTD-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******

**Explanation** The password string is received from the client in the format vpnpass (name delimiter) mailpass (for example: xxx:yyy). The name delimiter is optional. When it is not present, the VPN password and mail password are the same.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

**Recommended Action** None required.

---

**Error Message** %FTD-6-719017: WebVPN user: vpnuser invalid dynamic ACL.

**Explanation** The WebVPN session is aborted because the ACL has failed to parse for this user. The ACL determines what the user restrictions are on e-mail account access. The ACL is downloaded from the AAA server. Because of this error, it is unsafe to proceed with login.

- **vpnuser**—The WebVPN username

**Recommended Action** Check the AAA server and fix the dynamic ACL for this user.
719018

Error Message %FTD-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found

Explanation The ACL cannot be found at the local maintained ACL list. The ACL determines what the user restrictions are on e-mail account access. The ACL is configured locally. Because of this error, you cannot be authorized to proceed.

- vpnuser—The WebVPN username
- acl_ID—The local configured ACL identification string

Recommended Action Check the local ACL configuration.

719019

Error Message %FTD-6-719019: WebVPN user: vpnuser authorization failed.

Explanation The ACL determines what the user restrictions are on e-mail account access. The user cannot access the e-mail account because the authorization check fails.

- vpnuser—The WebVPN username

Recommended Action None required.

719020

Error Message %FTD-6-719020: WebVPN user: vpnuser authorization completed successfully.

Explanation The ACL determines what the user restrictions are on e-mail account access. The user is authorized to access the e-mail account.

- vpnuser—The WebVPN username

Recommended Action None required.

719021

Error Message %FTD-6-719021: WebVPN user: vpnuser is not checked against ACL.

Explanation The ACL determines what the user restrictions are on e-mail account access. The authorization checking using the ACL is not enabled.

- vpnuser—The WebVPN username

Recommended Action Enable the ACL checking feature, if necessary.

719022

Error Message %FTD-6-719022: WebVPN user: vpnuser has been authenticated.

Explanation The username is authenticated by the AAA server.

- vpnuser—The WebVPN username

Recommended Action None required.
719023

Error Message %FTD-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.

Explanation The username is denied by the AAA server. The session will be aborted. The user is not allowed to access the e-mail account.

- vpnuser — The WebVPN username

Recommended Action None required.

719024

Error Message %FTD-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser
addr=source_address

Explanation The Piggyback authentication is using an established WebVPN session to verify the username and IP address matching in the WebVPN session database. This is based on the assumption that the WebVPN session and e-mail proxy session are initiated by the same user, and a WebVPN session is already established. Because the authentication has failed, the session will be aborted. The user is not allowed to access the e-mail account.

- pointer — The session pointer
- vpnuser — The WebVPN username
- source_address — The client IP address

Recommended Action None required.

719025

Error Message %FTD-6-719025: Email Proxy DNS name resolution failed for hostname.

Explanation The hostname cannot be resolved with the IP address because it is not valid, or no DNS server is available.

- hostname — The hostname that needs to be resolved

Recommended Action Check DNS server availability and whether or not the configured mail server name is valid.

719026

Error Message %FTD-6-719026: Email Proxy DNS name hostname resolved to IP_address.

Explanation The hostname has successfully been resolved with the IP address.

- hostname — The hostname that needs to be resolved
- IP_address — The IP address resolved from the configured mail server name

Recommended Action None required.
Messages 720001 to 721019

This section includes messages from 720001 to 721019.

720001

**ErrorMessage** %FTD-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.

**Explanation** The VPN failover subsystem fails to initialize with the memory buffer management subsystem. A system-wide problem has occurred, and the VPN failover subsystem cannot be started.

- **unit**—Either Primary or Secondary

**Recommended Action** Examine the messages for any sign of system-level initialization problems.

720002

**ErrorMessage** %FTD-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...

**Explanation** The VPN failover subsystem is starting and booting up.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720003

**ErrorMessage** %FTD-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully

**Explanation** The VPN failover subsystem initialization is completed at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720004

**ErrorMessage** %FTD-6-720004: (VPN-unit) VPN failover main thread started.

**Explanation** The VPN failover main processing thread is started at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720005

**ErrorMessage** %FTD-6-720005: (VPN-unit) VPN failover timer thread started.

**Explanation** The VPN failover timer processing thread is started at boot time.

- **unit**—Either Primary or Secondary
**720006**

**ErrorMessage** %FTD-6-720006: (VPN-unit) VPN failover sync thread started.

**Explanation** The VPN failover bulk synchronization processing thread is started at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

**720007**

**ErrorMessage** %FTD-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.

**Explanation** The set of preallocated memory buffers is running out. The Firepower Threat Defense device has a resource issue. The Firepower Threat Defense device may be under heavy load when too many messages are being processed.

- **unit**—Either Primary or Secondary

**Recommended Action** This condition may be improved later when the VPN failover subsystem processes outstanding messages and frees up previously allocated memory.

**720008**

**ErrorMessage** %FTD-4-720008: (VPN-unit) Failed to register to High Availability Framework.

**Explanation** The VPN failover subsystem failed to register to the core failover subsystem. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

**Recommended Action** Search the message for any sign of system-wide initialization problems.

**720009**

**ErrorMessage** %FTD-4-720009: (VPN-unit) Failed to create version control block.

**Explanation** The VPN failover subsystem failed to create a version control block. This step is required for the VPN failover subsystem to find out the backward compatible firmware versions for the current release. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

**Recommended Action** Search the message for any sign of system-wide initialization problems.

**720010**

**ErrorMessage** %FTD-6-720010: (VPN-unit) VPN failover client is being disabled

**Explanation** An operator enabled failover without defining a failover key. In order to use a VPN failover, a failover key must be defined.
Recommended Action Use the `failover key` command to define a shared secret key between the active and standby units.

720011

**Error Message** `%FTD-4-720011: (VPN-unit ) Failed to allocate memory`  
**Explanation** The VPN failover subsystem cannot allocate a memory buffer, which indicates a system-wide resource problem. The Firepower Threat Defense device may be under heavy load.

- **unit**—Either Primary or Secondary

**Recommended Action** This condition may be improved later when you reduce the load on the Firepower Threat Defense device by reducing incoming traffic. By reducing incoming traffic, memory allocated for processing the existing work load will be available, and the Firepower Threat Defense device may return to normal operation.

720012

**Error Message** `%FTD-6-720012: (VPN-unit ) Failed to update IPsec failover runtime data on the standby unit.`  
**Explanation** The VPN failover subsystem cannot update IPsec-related runtime data because the corresponding IPsec tunnel has been deleted on the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720013

**Error Message** `%FTD-4-720013: (VPN-unit ) Failed to insert certificate in trustpoint trustpoint_name`  
**Explanation** The VPN failover subsystem tried to insert a certificate in the trustpoint.

- **unit**—Either Primary or Secondary
- **trustpoint_name**—The name of the trustpoint

**Recommended Action** Check the certificate content to determine if it is invalid.

720014

**Error Message** `%FTD-6-720014: (VPN-unit ) Phase 2 connection entry (msg_id=message_number , my cookie=mine , his cookie=his ) contains no SA list.`  
**Explanation** No security association is linked to the Phase 2 connection entry.

- **unit**—Either Primary or Secondary
- **message_number**—The message ID of the Phase 2 connection entry
- **mine**—The My Phase 1 cookie
- **his**—The peer Phase 1 cookie
Recommended Action None required.

720015

Error Message %FTD-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry {msg_id=message_number ,my cookie=mine , his cookie=his }.

Explanation The corresponding Phase 1 security association for the given Phase 2 connection entry cannot be found.

- unit—Either Primary or Secondary
- message_number—The message ID of the Phase 2 connection entry
- mine—The My Phase 1 cookie
- his—The peer Phase 1 cookie

Recommended Action None required.

720016

Error Message %FTD-5-720016: (VPN-unit) Failed to initialize default timer #index .

Explanation The VPN failover subsystem failed to initialize the given timer event. The VPN failover subsystem cannot be started at boot time.

- unit—Either Primary or Secondary
- index—The internal index of the timer event

Recommended Action Search the message for any sign of system-wide initialization problems.

720017

Error Message %FTD-5-720017: (VPN-unit) Failed to update LB runtime data

Explanation The VPN failover subsystem failed to update the VPN load balancing runtime data.

- unit—Either Primary or Secondary

Recommended Action None required.

720018

Error Message %FTD-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.

Explanation The Firepower Threat Defense device may be under heavy load. The VPN failover subsystem failed to obtain a failover buffer.

- unit—Either Primary or Secondary
- code—The error code returned by the high-availability subsystem

Recommended Action Decrease the amount of incoming traffic to improve the current load condition. With decreased incoming traffic, the Firepower Threat Defense device will free up memory allocated for processing the incoming load.
720019

**Error Message** %FTD-5-720019: (VPN-unit) Failed to update cTCP statistics.

**Explanation** The VPN failover subsystem failed to update the IPsec/cTCP-related statistics.
- **unit**—Either Primary or Secondary

**Recommended Action** None required. Updates are sent periodically, so the standby unit IPsec/cTCP statistics should be updated with the next update message.

720020

**Error Message** %FTD-5-720020: (VPN-unit) Failed to send type timer message.

**Explanation** The VPN failover subsystem failed to send a periodic timer message to the standby unit.
- **unit**—Either Primary or Secondary
- **type**—The type of timer message

**Recommended Action** None required. The periodic timer message will be resent during the next timeout.

720021

**Error Message** %FTD-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number. HA error code.

**Explanation** The VPN failover subsystem failed to send a nonblock message. This is a temporary condition caused by the Firepower Threat Defense device being under load or out of resources.
- **unit**—Either Primary or Secondary
- **message_number**—The ID number of the peer message
- **code**—The error return code

**Recommended Action** The condition will improve as more resources become available to the Firepower Threat Defense device.

720022

**Error Message** %FTD-4-720022: (VPN-unit) Cannot find trustpoint trustpoint

**Explanation** An error occurred when the VPN failover subsystem tried to look up a trustpoint by name.
- **unit**—Either Primary or Secondary
- **trustpoint**—The name of the trustpoint.

**Recommended Action** The trustpoint may be deleted by an operator.

720023

**Error Message** %FTD-6-720023: (VPN-unit) HA status callback: Peer is not present.

**Explanation** The VPN failover subsystem is notified by the core failover subsystem when the local Firepower Threat Defense device detected that a peer is available or becomes unavailable.
- **unit**—Either Primary or Secondary
- **not**—Either “not” or left blank

**Recommended Action** None required.

### 720024

**Error Message** %FTD-6-720024: (VPN-unit) HA status callback: Control channel is status.

**Explanation** The failover control channel is either up or down. The failover control channel is defined by the failover link and show failover commands, which indicate whether the failover link channel is up or down.

- **unit**—Either Primary or Secondary
- **status**—Up or Down

**Recommended Action** None required.

### 720025

**Error Message** %FTD-6-720025: (VPN-unit) HA status callback: Data channel is status.

**Explanation** The failover data channel is up or down.

- **unit**—Either Primary or Secondary
- **status**—Up or Down

**Recommended Action** None required.

### 720026

**Error Message** %FTD-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.

**Explanation** An operator or other external condition has occurred and has caused the current failover progression to abort before the failover peer agrees on the role (either active or standby). For example, when the failover active command is entered on the standby unit during the negotiation, or when the active unit is being rebooted.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

### 720027

**Error Message** %FTD-6-720027: (VPN-unit) HA status callback: My state state.

**Explanation** The state of the local failover device is changed.

- **unit**—Either Primary or Secondary
- **state**—Current state of the local failover device

**Recommended Action** None required.
720028

**Error Message** %FTD-6-720028: (VPN-unit) HA status callback: Peer state state.

**Explanation** The current state of the failover peer is reported.

- **unit**—Either Primary or Secondary
- **state**—Current state of the failover peer

**Recommended Action** None required.

720029

**Error Message** %FTD-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.

**Explanation** The active unit is ready to send all the state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720030

**Error Message** %FTD-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.

**Explanation** The active unit finished sending all the state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720031

**Error Message** %FTD-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.

**Explanation** The VPN failover subsystem received an invalid callback event from the underlying failover subsystem.

- **unit**—Either Primary or Secondary
- **event_ID**—The invalid event ID received

**Recommended Action** None required.

720032

**Error Message** %FTD-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence_, grp=group
, event=event , op=operand , my-my_state , peer-peer_state.

**Explanation** The VPN failover subsystem indicated that a status update was notified by the underlying failover subsystem.

- **unit**—Either Primary or Secondary
- **ID**—Client ID number
- **sequence_**—Sequence number
720033

Error Message  %FTD-4-720033: (VPN-unit) Failed to queue add to message queue.

Explanation System resources may be running low. An error occurred when the VPN failover subsystem tried to queue an internal message. This may be a temporary condition indicating that the Firepower Threat Defense device is under heavy load, and the VPN failover subsystem cannot allocate resource to handle incoming traffic.

• unit—Either Primary or Secondary

Recommended Action This error condition may disappear if the current load of the Firepower Threat Defense device is reduced, and additional system resources become available for processing new messages again.

720034

Error Message  %FTD-7-720034: (VPN-unit) Invalid type (type) for message handler.

Explanation An error occurred when the VPN failover subsystem tried to process an invalid message type.

• unit—Either Primary or Secondary

Recommended Action None required.

720035

Error Message  %FTD-5-720035: (VPN-unit) Fail to look up CTCP flow handle

Explanation The cTCP flow may be deleted on the standby unit before the VPN failover subsystem tries to do a lookup.

• unit—Either Primary or Secondary

Recommended Action Look for any sign of cTCP flow deletion in the message to determine the reason (for example, idle timeout) why the flow was deleted.

720036

Error Message  %FTD-5-720036: (VPN-unit) Failed to process state update message from the active peer.

Explanation An error occurred when the VPN failover subsystem tried to process a state update message received by the standby unit.

• unit - Either Primary or Secondary
Recommended Action None required. This may be a temporary condition because of the current load or low system resources.

720037

Error Message %FTD-6-720037: (VPN-unit) HA progression callback: id=\id\,seq=sequence_number, grp=group, event=event, op=operand, my=my_state, peer=peer_state.

Explanation The status of the current failover progression is reported.

- unit—Either Primary or Secondary
- id—Client ID
- sequence_number—Sequence number
- group—Group ID
- event—Current event
- operand—Current operand
- my_state—Current state of the Firepower Threat Defense device
- peer_state—Current state of the peer

Recommended Action None required.

720038

Error Message %FTD-4-720038: (VPN-unit) Corrupted message from active unit.

Explanation The standby unit received a corrupted message from the active unit. Messages from the active unit are corrupted, which may be caused by incompatible firmware running between the active and standby units. The local unit has become the active unit of the failover pair.

- unit—Either Primary or Secondary

Recommended Action None required.

720039

Error Message %FTD-6-720039: (VPN-unit) VPN failover client is transitioning to active state.

Explanation The local unit has become the active unit of the failover pair.

- unit—Either Primary or Secondary

Recommended Action None required.

720040

Error Message %FTD-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.

Explanation The local unit has become the standby unit of the failover pair.

- unit—Either Primary or Secondary

Recommended Action None required.
720041

**Error Message**  %FTD-7-720041: (VPN-unit) Sending type message id to standby unit

**Explanation** A message has been sent from the active unit to the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** None required.

720042

**Error Message**  %FTD-7-720042: (VPN-unit) Receiving type message id from active unit

**Explanation** A message has been received from the active unit by the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** None required.

720043

**Error Message**  %FTD-4-720043: (VPN-unit) Failed to send type message id to standby unit

**Explanation** An error occurred when the VPN failover subsystem tried to send a message from the active unit to the standby unit. The error may be caused by message 720018, in which the core failover subsystem runs out of failover buffer or the failover LAN link is down.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** Use the `show failover` command to see if the failover pair is running correctly and the failover LAN link is up.

720044

**Error Message**  %FTD-4-720044: (VPN-unit) Failed to receive message from active unit

**Explanation** An error occurred when the VPN failover subsystem tried to receive a message on the standby unit. The error may be caused by a corrupted message or an inadequate amount of memory allocated for storing the incoming message.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the `show failover` command and look for receive errors to determine if this is a VPN failover-specific problem or a general failover issue. Corrupted messages may be caused by incompatible firmware versions running on the active and standby units. Use the `show memory` command to determine if a low memory condition exists.
720045

**Error Message** %FTD-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.

**Explanation** The standby unit has been notified to start receiving bulk synchronization information from the active unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720046

**Error Message** %FTD-6-720046: (VPN-unit) End bulk syncing of state information on standby unit.

**Explanation** The standby unit has been notified that bulk synchronization from the active unit is completed.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

720047

**Error Message** %FTD-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to synchronize a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.

- **unit**—Either Primary or Secondary
- **IP_address**—IP address of the server

**Recommended Action** Use the **dir** command to display the flash contents. The node secret file has the filename, *ip*.sdi.

720048

**Error Message** %FTD-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.

**Explanation** A VPN failover subsystem finite state machine function has started.

- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **function**—Current executing function

**Recommended Action** None required.
720049

**Error Message** %FTD-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.

**Explanation** A VPN failover subsystem finite state machine function has finished.
- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **return**—Return code
- **function**—Current executing function

**Recommended Action** None required.

720050

**Error Message** %FTD-7-720050: (VPN-unit) Failed to remove timer. ID = id.

**Explanation** A timer cannot be removed from the timer processing thread.
- **unit**—Either Primary or Secondary
- **id**—Timer ID

**Recommended Action** None required.

720051

**Error Message** %FTD-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to add a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.
- **unit**—Either Primary or Secondary
- **id**—IP address of the SDI server

**Recommended Action** Use the `dir` command to display the flash contents. The node secret file has the filename, `ip.sdi`.

720052

**Error Message** %FTD-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to delete a node secret file on the active unit. The node secret file being deleted may not exist in the flash file system, or there was problem reading the flash file system.
- **unit**—Either Primary or Secondary
- **IP_address**—IP address of the SDI server
**Recommended Action** Use the dir command to display the flash contents. The node secret file has the filename, ip.sdi.

---

**720053**

**Error Message** %FTD-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer-IP_address, port-port

**Explanation** An error occurred when the VPN failover subsystem tried to load a cTCP IKE rule on the standby unit during bulk synchronization. The standby unit may be under heavy load, and the new IKE rule request may time out before completion.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** None required.

---

**720054**

**Error Message** %FTD-4-720054: (VPN-unit) Failed to add new cTCP record, peer-IP_address, port-port.

**Explanation** A cTCP record is replicated to the standby unit and cannot be updated. The corresponding IPsec over cTCP tunnel may not be functioning after failover. The cTCP database may be full, or a record with the same peer IP address and port number exists already.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** This may be a temporary condition and may improve when the existing cTCP tunnel is restored.

---

**720055**

**Error Message** %FTD-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.

**Explanation** The VPN subsystem does not start unless it is running in single (nontransparent) mode.

- **unit**—Either Primary or Secondary

**Recommended Action** Configure the Firepower Threat Defense device for the appropriate mode to support VPN failover and restart the Firepower Threat Defense device.

---

**720056**

**Error Message** %FTD-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.

**Explanation** The VPN failover subsystem main message processing thread is disabled when you have tried to enable failover, but a failover key is not defined. A failover key is required for VPN failover.
720057

**Error Message**  
%FTD-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.

**Explanation** The VPN failover subsystem main message processing thread is enabled when failover is enabled and a failover key is defined.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

---

720058

**Error Message**  
%FTD-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.

**Explanation** The VPN failover subsystem main timer processing thread is disabled when the failover key is not defined and failover is enabled.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

---

720059

**Error Message**  
%FTD-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.

**Explanation** The VPN failover subsystem main timer processing thread is enabled when the failover key is defined and failover is enabled.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

---

720060

**Error Message**  
%FTD-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.

**Explanation** The VPN failover subsystem main bulk synchronization processing thread is disabled when failover is enabled, but the failover key is not defined.

- **unit**—Either Primary or Secondary.

**Recommended Action** None required.

---

720061

**Error Message**  
%FTD-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.

**Explanation** The VPN failover subsystem main bulk synchronization processing thread is enabled when failover is enabled and the failover key is defined.

- **unit**—Either Primary or Secondary
Recommended Action None required.

**720062**

**Error Message** %FTD-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.

**Explanation** The VPN failover subsystem active unit has started bulk synchronization of state information to the standby unit.

• **unit**—Either Primary or Secondary

Recommended Action None required.

**720063**

**Error Message** %FTD-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.

**Explanation** The VPN failover subsystem active unit has completed bulk synchronization of state information to the standby unit.

• **unit**—Either Primary or Secondary

Recommended Action None required.

**720064**

**Error Message** %FTD-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.

**Explanation** An error occurred while the VPN failover subsystem attempted to update an existing cTCP record during bulk synchronization. The cTCP record may have been deleted from the cTCP database on the standby unit and cannot be found.

• **unit**—Either Primary or Secondary
• **IP_address**—Peer IP address
• **port**—Peer port number

Recommended Action Search in the message.

**720065**

**Error Message** %FTD-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.

**Explanation** An error occurred when the VPN failover subsystem tried to add a new IKE rule for the cTCP database entry on the standby unit. The Firepower Threat Defense device may be under heavy load, and the request for adding a cTCP IKE rule timed out and was never completed.

• **unit**—Either Primary or Secondary
• **IP_address**—Peer IP address
• **port**—Peer port number
**Recommended Action** This may be a temporary condition.

**720066**

**Error Message** %FTD-4-720066: (VPN-unit) Failed to activate IKE database.

**Explanation** An error occurred when the VPN failover subsystem tried to activate the IKE security association database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the IKE security association database from activating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the `show failover` command to see if the failover pair is still working correctly and/or look for other IKE-related errors in the message.

**720067**

**Error Message** %FTD-4-720067: (VPN-unit) Failed to deactivate IKE database.

**Explanation** An error occurred when the VPN failover subsystem tried to deactivate the IKE security association database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the IKE security association database from deactivating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the `show failover` command to see if the failover pair is still working correctly and/or look for IKE-related errors in the message.

**720068**

**Error Message** %FTD-4-720068: (VPN-unit) Failed to parse peer message.

**Explanation** An error occurred when the VPN failover subsystem tried to parse a peer message received on the standby unit. The peer message received on the standby unit cannot be parsed.

- **unit**—Either Primary or Secondary

**Recommended Action** Make sure that both active and standby units are running the same version of firmware. Also, use the `show failover` command to ensure that the failover pair is still working correctly.

**720069**

**Error Message** %FTD-4-720069: (VPN-unit) Failed to activate cTCP database.

**Explanation** An error occurred when the VPN failover subsystem tried to activate the cTCP database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the cTCP database from activating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the `show failover` command to see if the failover pair is still working correctly and/or look for other cTCP related errors in the message.
720070

**Error Message** %FTD-4-720070: (VPN-unit) Failed to deactivate cTCP database.

**Explanation** An error occurred when the VPN failover subsystem tried to deactivate the cTCP database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the cTCP database from deactivating.

- **unit**—Either Primary or Secondary.

**Recommended Action** Use the `show failover` command to see if the failover pair is still working correctly and/or look for cTCP related errors in the message.

720071

**Error Message** %FTD-5-720071: (VPN-unit) Failed to update cTCP dynamic data.

**Explanation** An error occurred while the VPN failover subsystem tried to update cTCP dynamic data.

- **unit**—Either Primary or Secondary.

**Recommended Action** This may be a temporary condition. Because this is a periodic update, wait to see if the same error recurs. Also, look for other failover-related messages in the message.

720072

**Error Message** %FTD-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.

**Explanation** The Zonelab Integrity Server cannot reestablish a connection before timeout. In an active/standby failover setup, the SSL connection between a Zonelab Integrity Server and the Firepower Threat Defense device needs to be reestablished after a failover.

- **interface**—The interface to which the Zonelab Integrity Server is connected
- **ip**—The IP address of the Zonelab Integrity Server

**Recommended Action** Check that the configuration on the Firepower Threat Defense device and the Zonelab Integrity Server match, and verify communication between the Firepower Threat Defense device and the Zonelab Integrity Server.

720073

**Error Message** %FTD-4-720073: VPN Session failed to replicate - ACL acl_name not found

**Explanation** When replicating VPN sessions to the standby unit, the standby unit failed to find the associated filter ACL.

- **acl_name**—The name of the ACL that was not found

**Recommended Action** Verify that the configuration on the standby unit has not been modified while in standby state. Resynchronize the standby unit by issuing the `write standby` command on the active unit.
721001

Error Message %FTD-6-721001: (device) WebVPN Failover SubSystem started successfully. (device) either WebVPN-primary or WebVPN-secondary.

Explanation The WebVPN failover subsystem in the current failover unit, either primary or secondary, has been started successfully.

- (device) — Either the WebVPN primary or the WebVPN secondary device

Recommended Action None required.

721002

Error Message %FTD-6-721002: (device) HA status change: event event , my state my_state , peer state peer .

Explanation The WebVPN failover subsystem receives status notification from the core HA component periodically. The incoming event, the new state of the local Firepower Threat Defense device, and the new state of the failover peer are reported.

- (device) — Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- event — New HA event
- my_state — The new state of the local Firepower Threat Defense device
- peer — The new state of the peer

Recommended Action None required.

721003

Error Message %FTD-6-721003: (device) HA progression change: event event , my state my_state , peer state peer .

Explanation The WebVPN failover subsystem transitions from one state to another state based on the event notified by the core HA component. The incoming event, the new state of the local Firepower Threat Defense device, and the new state of the failover peer are being reported.

- (device) — Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- event — New HA event
- my_state — The new state of the local Firepower Threat Defense device
- peer — The new state of the peer

Recommended Action None required.

721004

Error Message %FTD-6-721004: (device) Create access list list_name on standby unit.

Explanation A WebVPN-specific access list is replicated from the active unit to the standby unit. A successful installation of the WebVPN access list on the standby unit has occurred.

- (device) — Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- list_name — The access list name
**Recommended Action** None required.

### 721005

**Error Message** `%FTD-6-721005: (device) Fail to create access list list_name on standby unit.`

**Explanation** When a WebVPN-specific access list is installed on the active unit, a copy is installed on the standby unit. The access list failed to be installed on the standby unit. The access list may have existed on the standby unit already.

- *(device)*—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- *list_name*—Name of the access list that failed to install on the standby unit

**Recommended Action** Use the `show access-list` command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.

### 721006

**Error Message** `%FTD-6-721006: (device) Update access list list_name on standby unit.`

**Explanation** The content of the access list has been updated on the standby unit.

- *(device)*—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- *list_name*—Name of the access list that was updated

**Recommended Action** None required.

### 721007

**Error Message** `%FTD-4-721007: (device) Fail to update access list list_name on standby unit.`

**Explanation** An error occurred while the standby unit tried to update a WebVPN-specific access list. The access list cannot be located on the standby unit.

- *(device)*—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- *list_name*—Name of the access list that was not updated

**Recommended Action** Use a `show access-list` command on both the active and standby units. Compare the content of the output and determine whether or not there is any discrepancy. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.

### 721008

**Error Message** `%FTD-6-721008: (device) Delete access list list_name on standby unit.`

**Explanation** When a WebVPN-specific access list is removed from the active unit, a message is sent to the standby unit requesting that the same access list be removed. As a result, a WebVPN-specific access list has been removed from the standby unit.

- *(device)*—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- *list_name*—Name of the access list that was removed

**Recommended Action** None required.
721009

**Error Message** \%FTD-6-721009: (device) Fail to delete access list list_name on standby unit.

**Explanation** When a WebVPN-specific access list is removed on the active unit, a message is sent to the standby unit requesting the same access list be removed. An error condition occurred when an attempt was made to remove the corresponding access list on the standby unit. The access list did not exist on the standby unit.

- (device)—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- list_name—Name of the access list that was deleted

**Recommended Action** Use a `show access-list` command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.

721010

**Error Message** \%FTD-6-721010: (device) Add access list rule list_name , line line_no on standby unit.

**Explanation** When an access list rule is added to the active unit, the same rule is added on the standby unit. A new access list rule was added successfully on the standby unit.

- (device)—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- list_name—Name of the access list that was deleted
- line_no—Line number of the rule added to the access list

**Recommended Action** None required.

721011

**Error Message** \%FTD-4-721011: (device) Fail to add access list rule list_name , line line_no on standby unit.

**Explanation** When an access list rule is added to the active unit, an attempt is made to add the same access list rule to the standby unit. An error occurred when an attempt is made to add a new access list rule to the standby unit. The same access list rule may exist on the standby unit.

- (device)—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- list_name—Name of the access list that was deleted
- line_no—Line number of the rule added to the access list

**Recommended Action** Use a `show access-list` command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.

721012

**Error Message** \%FTD-6-721012: (device) Enable APCF XML file file_name on the standby unit.

**Explanation** When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file was installed successfully on the standby unit. Use the `dir` command on the standby unit to show that the XML file exists in the flash file system.
Syslog Messages 715001 to 721019

721013

Error Message  %FTD-4-721013: (device ) Fail to enable APCF XML file file_name on the standby unit.

Explanation When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file failed to install on the standby unit.

Recommended Action Use a dir command on both the active and standby unit. Compare the directory listing and determine if there is any discrepancy. Resynchronize the standby unit, if needed, by using the write standby command on the active unit.

721014

Error Message  %FTD-6-721014: (device ) Disable APCF XML file file_name on the standby unit.

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An APCF XML file was removed from the standby unit successfully.

Recommended Action None required.

721015

Error Message  %FTD-4-721015: (device ) Fail to disable APCF XML file file_name on the standby unit.

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An error occurred when an attempt was made to remove an APCF XML file from the standby unit. The file may not be installed on the standby unit.

Recommended Action Use a show running-config webvpn command to make sure the APCF XML file of interest is not enabled. As long as it is not enabled, you may ignore this message. Otherwise, try to disable the file by using the no apcf file_name command in the webvpn configuration submode.

721016

Error Message  %FTD-6-721016: (device ) WebVPN session for client user user_name , IP ip_address has been created.
Explanation A remote WebVPN user has logged in successfully and the login information has been installed on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

**Recommended Action** None required.

721017

**Error Message** %FTD-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.

**Explanation** When a WebVPN user logs into the active unit, the login information is replicated to the standby unit. An error occurred while replicating the login information to the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

**Recommended Action** Use the `show vpn-sessiondb detail webvpn` command for a regular WebVPN user, or the `show vpn-sessiondb detail svc` command for a WebVPN SVC user on both the active and standby units. Compare the entries and determine whether the same user session record appears on both Firepower Threat Defense devices. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.

721018

**Error Message** %FTD-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.

**Explanation** When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. A WebVPN user record was removed from the standby unit successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

**Recommended Action** None required.

721019

**Error Message** %FTD-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.

**Explanation** When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. An error occurred when an attempt was made to remove a WebVPN user record from the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Firepower Threat Defense device
- **user_name**—Name of the user
• **ip_address**—IP address of the remote user

**Recommended Action** Use the `show vpn-sessiondb detail webvpn` command for a regular WebVPN user, or the `show vpn-sessiondb detail svc` command for a WebVPN SVC user on both the active and standby units. Check whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the `write standby` command on the active unit.
Syslog Messages 722001 to 776254

This chapter contains the following sections:

- Messages 722001 to 722056, on page 379
- Messages 723001 to 736001, on page 391
- Messages 737001 to 776254, on page 412

Messages 722001 to 722056

This section includes messages from 722001 to 722056.

722001

Error Message %FTD-4-722001: IP IP_address Error parsing SVC connect request.

Explanation The request from the SVC was invalid.

Recommended Action Research as necessary to determine if this error was caused by a defect in the SVC, an incompatible SVC version, or an attack against the device.

722002

Error Message %FTD-4-722002: IP IP_address Error consolidating SVC connect request.

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722003

Error Message %FTD-4-722003: IP IP_address Error authenticating SVC connect request.

Explanation The user took too long to download and connect.

Recommended Action Increase the timeouts for session idle and maximum connect time.
722004

Error Message %FTD-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
Explanation There is not enough memory to perform the action.
Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722005

Error Message %FTD-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.
Explanation There is not enough memory to perform the action.
Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722006

Error Message %FTD-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.
Explanation An invalid address was assigned to the user.
Recommended Action Verify and correct the address assignment, if possible. Otherwise, notify your network administrator or escalate this issue according to your security policy. For additional assistance, contact the Cisco TAC.

722007

Error Message %FTD-3-722007: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message
Explanation The SVC issued a message.
  - type-num—A number from 0 to 31 indicating a message type. Message types are as follows:
    - 0—Normal
    - 16—Logout
    - 17—Closed due to error
    - 18—Closed due to rekey
    - 1-15, 19-31—Reserved and unused
  - message—A text message from the SVC
Recommended Action None required.

722008

Error Message %FTD-3-722008: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message
**Explaination** The SVC issued a message.

- **type-num** — A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message** — A text message from the SVC

**Recommended Action** None required.

---

**722009**

**Error Message** `%FTD-3-722009: Group group User user-name IP IP_address SVC Message: type-num /
/ERROR: message`

**Explanation** The SVC issued a message.

- **type-num** — A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message** — A text message from the SVC

**Recommended Action** None required.

---

**722010**

**Error Message** `%FTD-5-722010: Group group User user-name IP IP_address SVC Message: type-num /
/NOTICE: message`

**Explanation** The SVC issued a message.

- **type-num** — A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message** — A text message from the SVC

**Recommended Action** None required.
722011

**Error Message** %FTD-5-722011: Group group User user-name IP IP_address SVC Message: type-num

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

722012

**Error Message** %FTD-5-722012: Group group User user-name IP IP_address SVC Message: type-num

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

722013

**Error Message** %FTD-6-722013: Group group User user-name IP IP_address SVC Message: type-num

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
- 1-15, 19-31—Reserved and unused
  • message—A text message from the SVC

**Recommended Action** None required.

### 722014

**Error Message**

%FTD-6-722014: Group group User user-name IP IP_address SVC Message: type-num
/INFO: message

**Explanation** The SVC issued a message.

• type-num—A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal.
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
  • message—A text message from the SVC

**Recommended Action** None required.

### 722015

**Error Message**

%FTD-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num

**Explanation** The SVC sent an invalid frame type to the device, which might be caused by an SVC version incompatibility.

• type-num—The number identifier of the frame type

**Recommended Action** Verify the SVC version.

### 722016

**Error Message**

%FTD-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length

**Explanation** The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

**Recommended Action** Verify the SVC version.

### 722017

**Error Message**

%FTD-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
Explanation The SVC sent a badly framed datagram, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722018

Error Message %FTD-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version

Explanation The SVC sent a version unknown to the device, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722019

Error Message %FTD-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length

Explanation The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722020

Error Message %FTD-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection

Explanation Address assignment failed for the AnyConnect session. No IP addresses are available.

• tunnel_group — The name of the tunnel group that the user was assigned to or used to log in
• group_policy — The name of the group policy that the user was assigned to
• user-name — The name of the user with which this message is associated
• IP_address — The public IP (Internet) address of the client machine

Recommended Action Check the configuration listed in the ip local ip command to see if enough addresses exist in the pools that have been assigned to the tunnel group and the group policy. Check the DHCP configuration and status. Check the address assignment configuration. Enable IPAA syslog messages to determine why the AnyConnect client cannot obtain an IP address.

722028

Error Message %FTD-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.

Explanation An unused SVC connection was closed.

Recommended Action None required. However, the client may be having trouble connecting if multiple connections are established. The SVC log should be examined.
**722029**

**Error Message** %FTD-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets

**Explanation** The number of connections, reconnections, and resets that have occurred are reported. If connections is greater than 1 or the number of DPD_conns, compression_resets, or decompression_resets is greater than 0, it may indicate network reliability problems, which may be beyond the control of the Firepower Threat Defense administrator. If there are many connections or DPD connections, the user may be having problems connecting and may experience poor performance.

- **connections**—The total number of connections during this session (one is normal)
- **DPD_conns**—The number of reconnections due to DPD
- **compression_resets**—The number of compression history resets
- **decompression_resets**—The number of decompression history resets

**Recommended Action** The SVC log should be examined. You may want to research and take appropriate action to resolve possible network reliability problems.

**722030**

**Error Message** %FTD-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops

**Explanation** End-of-session statistics are being recorded.

- **data_bytes**—The number of inbound (from SVC) data bytes
- **ctrl_bytes**—The number of inbound control bytes
- **data_pkts**—The number of inbound data packets
- **ctrl_pkts**—The number of inbound control packets
- **drop_pkts**—The number of inbound packets that were dropped

**Recommended Action** None required.

**722031**

**Error Message** %FTD-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops

**Explanation** End-of-session statistics are being recorded.

- **data_bytes**—The number of outbound (to SVC) data bytes
- **ctrl_bytes**—The number of outbound control bytes
- **data_pkts**—The number of outbound data packets
- **ctrl_pkts**—The number of outbound control packets
- **ctrl_pkts**—The number of outbound packets that were dropped

**Recommended Action** None required.
Error Message %FTD-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.

Explanation A new SVC connection is replacing an existing one. You may be having trouble connecting.

Recommended Action Examine the SVC log.

Error Message %FTD-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.

Explanation The first SVC connection was established for the SVC session.

Recommended Action None required.

Error Message %FTD-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.

Explanation A reconnection attempt has occurred. An SVC connection is replacing a previously closed connection. There is no existing connection for this session because the connection was already dropped by the SVC or the Firepower Threat Defense device. You may be having trouble connecting.

Recommended Action Examine the Firepower Threat Defense device log and SVC log.

Error Message %FTD-3-722035: Group group User user-name IP IP_address Received large packet length (threshold num).

Explanation A large packet was received from the client.

• length—The length of the large packet
• num—The threshold

Recommended Action Enter the anyconnect ssl df-bit-ignore enable command under the group policy to allow the Firepower Threat Defense device to fragment the packets arriving with the DF bit set.

Error Message %FTD-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).

Explanation A large packet was sent to the client. The source of the packet may not be aware of the MTU of the client. This could also be due to compression of non-compressible data.

• length—The length of the large packet
• num—The threshold

Recommended Action Turn off SVC compression, otherwise, none required.
722037

**Error Message** %FTD-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.

**Explanation** An SVC connection was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.
- **reason**—The reason that the SVC connection was terminated

**Recommended Action** Examine the SVC log.

722038

**Error Message** %FTD-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.

**Explanation** An SVC session was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.
- **reason**—The reason that the SVC session was terminated

**Recommended Action** Examine the SVC log if the reason for termination was unexpected.

722041

**Error Message** %FTD-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection.

**Explanation** An IPv6 address was not available for assignment to the remote SVC client.
- **n**—The SVC connection identifier

**Recommended Action** Augment or create an IPv6 address pool, if desired.

722042

**Error Message** %FTD-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.

**Explanation** An invalid SVC or AnyConnect client is trying to connect.
- **group**—The name of the group policy with which the user is trying to connect
- **user**—The name of the user who is trying to connect
- **ip**—The IP address of the user who is trying to connect

**Recommended Action** Validate that the SVC or AnyConnect client is compatible with the Firepower Threat Defense device.

722043

**Error Message** %FTD-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.
Explanation The DTLS (UDP transport) cannot be established. The SSL encryption configuration was probably changed.

- **group** — The name of the group policy with which the user is trying to connect
- **user** — The name of the user who is trying to connect
- **ip** — The IP address of the user who is trying to connect

**Recommended Action** Revert the SSL encryption configuration. Make sure there is at least one block cipher (AES, DES, or 3DES) in the SSL encryption configuration.

**722044**

**ErrorMessage** %FTD-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.

**Explanation** An IP address cannot be requested because of low memory on the Firepower Threat Defense device.

- **group** — The name of the group policy with which the user is trying to connect
- **user** — The name of the user who is trying to connect
- **ip** — The IP address of the user who is trying to connect
- **ver** — Either IPv4 or IPv6, based on the IP address version being requested

**Recommended Action** Reduce the load on the Firepower Threat Defense device or add more memory.

**722045**

**ErrorMessage** %FTD-3-722045: Connection terminated: no SSL tunnel initialization data.

**Explanation** Data to establish a connection is missing. This is a defect in the Firepower Threat Defense software.

**Recommended Action** Contact the Cisco TAC for assistance.

**722046**

**ErrorMessage** %FTD-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.

**Explanation** The Firepower Threat Defense device cannot set up connection parameters. This is a defect in the Firepower Threat Defense software.

- **group** — The name of the group policy with which the user is trying to connect
- **user** — The name of the user who is trying to connect
- **ip** — The IP address of the user who is trying to connect

**Recommended Action** Contact the Cisco TAC for assistance.

**722047**

**ErrorMessage** %FTD-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
**Explanation** The user logged in via the web browser and tried to start the SVC or AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the SVC globally using the `svc enable` command. Validate the integrity of versions of the SVC images by reloading new images using the `svc image` command.

---

**722048**

**Error Message** `%FTD-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.`

**Explanation** The user logged in via the web browser, and tried to start the SVC or AnyConnect client. The SVC service is not enabled for this user. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the service for this user using the `group-policy` and `username` commands.

---

**722049**

**Error Message** `%FTD-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.`

**Explanation** The user logged in via the AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the SVC globally using the `svc-enable` command. Validate the integrity and versions of the SVC images by reloading new images using the `svc image` command.

---

**722050**

**Error Message** `%FTD-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.`

**Explanation** The user logged in through the AnyConnect client. The SVC service is not enabled for this user. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the service for this user using the `group-policy` and `username` commands.
722051

**Error Message** %FTD-6-722051: Group group-policy User username IP public-ip IPv4 Address assigned-ip IPv6 Address assigned-ip assigned to session

**Explanation** The specified address has been assigned to the given user.

- **group-policy** — The group policy that allowed the user to gain access
- **username** — The name of the user
- **public-ip** — The public IP address of the connected client
- **assigned-ip** — The IPv4 or IPv6 address that is assigned to the client

**Recommended Action** None required.

722053

**Error Message** %FTD-6-722053: Group g User u IP ip Unknown client user-agent connection.

**Explanation** An unknown or unsupported SSL VPN client has connected to the Firepower Threat Defense device. Older clients include the Cisco SVC and the Cisco AnyConnect client earlier than Version 2.3.1.

- **g** — The group policy under which the user logged in
- **u** — The name of the user
- **ip** — The IP address of the client
- **user-agent** — The user agent (usually includes the version) received from the client

**Recommended Action** Upgrade to a supported Cisco SSL VPN client.

722054

**Error Message** %FTD-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP

**Explanation** An error occurred for an AnyConnect VPN connection when a redirect URL was installed, and the ACL was received from the ISE, but the redirect ACL does not exist on the Firepower Threat Defense device.

- **group policy** — The group policy that allowed the user to gain access
- **user name** — Username of the requester for the remote access
- **remote IP** — Remote IP address that the connection request is coming from
- **redirect URL** — The URL for the HTTP traffic redirection
- **assigned IP** — The IP address that is assigned to the user

**Recommended Action** Configure the redirect ACL on the Firepower Threat Defense device.

722055

**Error Message** %FTD-6-722055: Group group-policy User username IP public-ip Client Type: user-agent

**Explanation** The indicated user is attempting to connect with the given user-agent.
- **group-policy** — The group policy that allowed the user to gain access
- **username** — The name of the user
- **public-ip** — The public IP address of the connected client
- **user-agent** — The user-agent string provided by the connecting client. Usually includes the AnyConnect version and host operating system for AnyConnect clients.

**Recommended Action** None required.

---

**722056**

**Error Message** `%FTD-4-722055: Unsupported AnyConnect client connection rejected from ip address. Client info: user-agent string. Reason: reason`

**Explanation** This syslog indicates that an AnyConnect client connection is rejected. The reason for this is provided in the syslog along with the client information.

- **ip address** — IP address from which a connection with the old client is attempted,
- **user-agent string** — User-Agent header in the client request. Usually includes the AnyConnect version and host operating system for AnyConnect clients
- **reason** — Reason for rejection

**Recommended Action** Use the client information and reason provided in the syslog to resolve the issue.

---

**Messages 723001 to 736001**

This section includes messages from 723001 to 736001.

**723001**

**Error Message** `%FTD-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.`

**Explanation** The Citrix connection is up.

- **group-name** — The name of the Citrix group
- **user-name** — The name of the Citrix user
- **IP_address** — The IP address of the Citrix user
- **connection** — The Citrix connection identifier

**Recommended Action** None required.

**723002**

**Error Message** `%FTD-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.`

**Explanation** The Citrix connection is down.

- **group-name** — The name of the Citrix group
- **user-name** — The name of the Citrix user
- **IP_address** — The IP address of the Citrix user
Recommended Action No action is required when the Citrix ICA connection is terminated intentionally by the client, the server, or the Firepower Threat Defense administrator. However, if this is not the case, verify that the WebVPN session in which the Citrix ICA connection is set up is still active. If it is inactive, then receiving this message is normal. If the WebVPN session is still active, verify that the ICA client and Citrix server both work correctly and that there is no error displayed. If not, bring either or both up or respond to any error. If this message is still received, contact the Cisco TAC and provide the following information:

- Network topology
- Delay and packet loss
- Citrix server configuration
- Citrix ICA client information
- Steps to reproduce the problem
- Complete text of all associated messages

### 723003

**Error Message** %FTD-7-723003: No memory for WebVPN Citrix ICA connection.

**Explanation** The Firepower Threat Defense device is running out of memory. The Citrix connection was rejected.

**Recommended Action** Verify that the Firepower Threat Defense device is working correctly. Pay special attention to memory and buffer usage. If the Firepower Threat Defense device is under heavy load, buy more memory and upgrade the Firepower Threat Defense device or reduce the load on the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

### 723004

**Error Message** %FTD-7-723004: WebVPN Citrix encountered bad flow control.

**Explanation** The Firepower Threat Defense device encountered an internal flow control mismatch, which can be caused by massive data flow, such as might occur during stress testing or with a high volume of ICA connections.

**Recommended Action** Reduce ICA connectivity to the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

### 723005

**Error Message** %FTD-7-723005: No channel to set up WebVPN Citrix ICA connection.

**Explanation** The Firepower Threat Defense device was unable to create a new channel for Citrix.

**Recommended Action** Verify that the Citrix ICA client and the Citrix server are still alive. If not, bring them back up and retest. Check the Firepower Threat Defense device load, paying special attention to memory and buffer usage. If the Firepower Threat Defense device is under heavy load, upgrade the Firepower Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.
723006

**Error Message**  %FTD-7-723006: WebVPN Citrix SOCKS errors.

**Explanation**  An internal Citrix SOCKS error has occurred on the Firepower Threat Defense device.

**Recommended Action**  Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the Citrix ICA client and the Firepower Threat Defense device, paying attention to packet loss. Resolve any abnormal network conditions. If the problem persists, contact the Cisco TAC.

723007

**Error Message**  %FTD-7-723007: WebVPN Citrix ICA connection list is broken.

**Explanation**  The Firepower Threat Defense device internal Citrix connection list is broken.

- **connection**—The Citrix connection identifier

**Recommended Action**  Verify that the Firepower Threat Defense device is working correctly, paying special attention to memory and buffer usage. If the Firepower Threat Defense device is under heavy load, upgrade the Firepower Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723008

**Error Message**  %FTD-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.

**Explanation**  An attempt was made to access a Citrix Socks server that does not exist.

- **server**—The Citrix server identifier

**Recommended Action**  Verify that the Firepower Threat Defense device is working correctly. Note whether or not there is any memory or buffer leakage. If this issue occurs frequently, capture information about memory usage, network topology, and the conditions during which this message is received. Send this information to the Cisco TAC for review. Make sure that the WebVPN session is still up while this message is being received. If not, determine the reason that the WebVPN session is down. If the Firepower Threat Defense device is under heavy load, upgrade the Firepower Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723009

**Error Message**  %FTD-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection.

**Explanation**  Data was received on a Citrix connection that does not exist.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection**—The Citrix connection identifier

**Recommended Action**  The original published Citrix application connection was probably terminated, and the remaining active published applications lost connectivity. Restart all published applications to generate a
new Citrix ICA tunnel. If the Firepower Threat Defense device is under heavy load, upgrade the Firepower Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

### 723010

**Error Message**  
%FTD-7-723010: Group group-name, User user-name, IP IP_address : WebVPN

Citrix received closing channel channel for invalid connection connection.

**Explanation** An abort was received on a nonexistent Citrix connection, which can be caused by massive data flow (such as stress testing) or a high volume of ICA connections, especially during network delay or packet loss.

- group-name—The name of the Citrix group
- user-name—The name of the Citrix user
- IP_address—The IP address of the Citrix user
- channel—The Citrix channel identifier
- connection—The Citrix connection identifier

**Recommended Action** Reduce the number of ICA connections to the Firepower Threat Defense device, obtain more memory for the Firepower Threat Defense device, or resolve the network problems.

### 723011

**Error Message**  
%FTD-7-723011: Group group-name, User user-name, IP IP_address : WebVPN

Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.

**Explanation** The Citrix SOCKS message length is incorrect.

- group-name—The name of the Citrix group
- user-name—The name of the Citrix user
- IP_address—The IP address of the Citrix user

**Recommended Action** Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Firepower Threat Defense device, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

### 723012

**Error Message**  
%FTD-7-723012: Group group-name, User user-name, IP IP_address : WebVPN

Citrix received bad SOCKS socks message format.

**Explanation** The Citrix SOCKS message format is incorrect.

- group-name—The name of the Citrix group
- user-name—The name of the Citrix user
- IP_address—The IP address of the Citrix user

**Recommended Action** Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Firepower Threat Defense device, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.
723013

**Error Message** %FTD-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.

**Explanation** The Firepower Threat Defense internal Citrix timer has expired, and the Citrix connection is invalid.

- **connection**—The Citrix connection identifier

**Recommended Action** Check the network connection between the Citrix ICA client and the Firepower Threat Defense device, and between the Firepower Threat Defense device and the Citrix server. Resolve any abnormal network conditions, especially delay and packet loss. Verify that the Firepower Threat Defense device works correctly, paying special attention to memory or buffer problems. If the Firepower Threat Defense device is under heavy load, obtain more memory, upgrade the Firepower Threat Defense device, or reduce the load. If the problem persists, contact the Cisco TAC.

723014

**Error Message** %FTD-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.

**Explanation** The Firepower Threat Defense internal Citrix Secure Gateway is connected to the Citrix server.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection**—The connection name
- **server**—The Citrix server identifier
- **channel**—The Citrix channel identifier (hexadecimal)

**Recommended Action** None required.

724001

**Error Message** %FTD-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.

**Explanation** The session was not allowed because an error occurred during processing of the CSD Host Integrity Check results on the Firepower Threat Defense device.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address

**Recommended Action** Determine whether the client firewall is truncating long URLs. Uninstall CSD from the client and reconnect to the Firepower Threat Defense device.

724002

**Error Message** %FTD-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
Explanation CSD is not running on the client machine.

- **group-name** — The name of the group
- **user-name** — The name of the user
- **IP_address** — The IP address

**Recommended Action** Verify that the end user can install and run CSD on the client machine.

---

**725001**

**Error Message** %FTD-6-725001: Starting SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol session.

**Explanation** The SSL handshake has started with the remote device, which can be a client or server.

- **peer-type** — Either the server or the client, depending on the device that initiated the connection
- **interface** — The interface name that the SSL session is using
- **source-ip** — The source IPv4 or IPv6 address
- **src-port** — The source port number
- **dst-ip** — The destination IP address
- **dst-port** — The destination port number
- **protocol** — The SSL version used for the SSL handshake

**Recommended Action** None required.

---

**725002**

**Error Message** %FTD-6-725002: Device completed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol-version session.

**Explanation** The SSL handshake has completed successfully with the remote device.

- **peer-type** — Either the server or the client, depending on the device that initiated the connection
- **interface** — The interface name that the SSL session is using
- **source-ip** — The source IPv4 or IPv6 address
- **src-port** — The source port number
- **dst-ip** — The destination IP address
- **dst-port** — The destination port number
- **protocol-version** — The version of the SSL protocol being used: SSLv3, TLSv1, DTLSv1, TLSv1.1 or TLSv1.2

**Recommended Action** None required.

---

**725003**

**Error Message** %FTD-6-725003: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port request to resume previous session.

**Explanation** The remote device is trying to resume a previous SSL session.

- **peer-type** — Either the server or the client, depending on the device that initiated the connection
- **interface** — The interface name that the SSL session is using
725004

**Error Message** %FTD-6-725004: Device requesting certificate from SSL peer-type interface :src-ip /src-port to dst-ip /dst-port for authentication.

**Explanation** The Firepower Threat Defense device has requested a client certificate for authentication.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IP address
- **dst-port**—The destination port number

**Recommended Action** None required.

725005

**Error Message** %FTD-6-725005: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port requesting our device certificate for authentication.

**Explanation** The server has requested the certificate of the Firepower Threat Defense device for authentication.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IP address
- **dst-port**—The destination port number

**Recommended Action** None required.

725006

**Error Message** %FTD-6-725006: Device failed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port

**Explanation** The SSL handshake with the remote device has failed.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IP address
- **dst-port**—The destination port number
**Recommended Action** Look for syslog message 725014, which indicates the reason for the failure.

**725007**

**Error Message** %FTD-6-725007: SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port terminated.

**Explanation** The SSL session has terminated.
- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip** —The destination IP address
- **dst-port** —The destination port number

**Recommended Action** None required.

**725008**

**Error Message** %FTD-7-725008: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port proposes the following n cipher(s).

**Explanation** The number of ciphers proposed by the remote SSL device are listed.
- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip** —The destination IP address
- **dst-port** —The destination port number
- **n** —The number of supported ciphers

**Recommended Action** None required.

**725009**

**Error Message** %FTD-7-725009 Device proposes the following n cipher(s) peer-type interface :src-ip /src-port to dst-ip /dst-port.

**Explanation** The number of ciphers proposed to the SSL server are listed.
- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip** —The destination IP address
- **dst-port** —The destination port number
- **n** —The number of supported ciphers

**Recommended Action** None required.
725010

**Error Message** %FTD-7-725010: Device supports the following n cipher(s).

**Explanation** The number of ciphers supported by the Firepower Threat Defense device for an SSL session are listed.

- n—The number of supported ciphers

**Recommended Action** None required.

725011

**Error Message** %FTD-7-725011 Cipher[order ]: cipher_name

**Explanation** Always following messages 725008, 725009, and 725010, this message indicates the cipher name and its order of preference.

- order—The order of the cipher in the cipher list
- cipher_name—The name of the OpenSSL cipher from the cipher list

**Recommended Action** None required.

725012

**Error Message** %FTD-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port.

**Explanation** The cipher that was chosen by the Cisco device for the SSL session is listed.

- cipher—The name of the OpenSSL cipher from the cipher list
- peer-type—Either the server or the client, depending on the device that initiated the connection
- interface—The interface name that the SSL session is using
- source-ip—The source IPv4 or IPv6 address
- src-port—The source port number
- dst-ip —The destination IP address
- dst-port —The destination port number

**Recommended Action** None required.

725013

**Error Message** %FTD-7-725013 SSL peer-type interface :src-ip /src-port to dst-ip /dst-port chooses cipher cipher

**Explanation** The cipher that was chosen by the server for the SSL session is identified.

- peer-type—Either the server or the client, depending on the device that initiated the connection
- interface—The interface name that the SSL session is using
- source-ip—The source IPv4 or IPv6 address
- src-port—The source port number
- dst-ip —The destination IP address
- dst-port —The destination port number
• cipher—The name of the OpenSSL cipher from the cipher list

Recommended Action None required.

725014

Error Message %FTD-7-725014 SSL lib error. Function: function Reason: reason

Explanation The reason for failure of the SSL handshake is indicated.

• function—The function name where the failure is reported
• reason—The description of the failure condition

Recommended Action Include this message when reporting any SSL-related issue to the Cisco TAC.

725015

Error Message %FTD-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.

Explanation The verification of an SSL client certificate failed because of an unsupported (large) key size.

Recommended Action Use client certificates with key sizes that are less than or equal to 4096 bits.

725016

Error Message %FTD-6-725016: Device selects trust-point trustpoint for peer-type interface :src-ip /src-port to dst-ip /dst-port

Explanation With server-name indication (SNI), the certificate used for a given connection may not be the certificate configured on the interface. There is also no indication of which certificate trustpoint has been selected. This syslog gives an indication of the trustpoint used by the connection (given by interface :src-ip /src-port).

• trustpoint—The name of the configured trustpoint that is being used for the specified connection
• interface—The name of the interface on the Firepower Threat Defense device
• src-ip—The IP address of the peer
• src-port—The port number of the peer
• dst-ip—The IP address of the destination
• dst-port—The port number of the destination

Recommended Action None required.

725017

Error Message %FTD-7-725017: No certificates received during the handshake with %s %s :%B/%d to %B/%d for %s session

Explanation A remote client has not sent a valid certificate.

• remote_device—Identifies whether a handshake is performed with the client or server
• ctm->interface—The interface name on which the handshake is sent
• ctm->src_ip—The IP address of the SSL server, which will communicate with the client
• ctm->src_port — The port of the SSL server, which will communicate with the client
• ctm->dst_ip — The IP address of the client
• ctm->dst_port — The port of the client through which it responds
• s->method->version — The protocol version involved in the transaction (SSLv3, TLSv1, or DTLSv1)

**Recommended Action** None required.

### 726001

**Error Message** `%FTD-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc :/sip /sport to dest_ifc :/dip /dport Action: action Matched Class class_map_id class_map_name`

**Explanation** An IM inspection was performed on an IM message and the specified criteria were satisfied. The configured action is taken.

- `im_protocol` — MSN IM or Yahoo IM
- `im_service` — The IM services, such as chat, conference, file transfer, voice, video, games, or unknown
- `im_client_1, im_client_2` — The client peers that are using the IM service in the session: `client_login_name` or `?`
- `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
- `action` — The action taken: reset connection, dropped connection, or received
- `class_map_id` — The matched class-map ID
- `class_map_name` — The matched class-map name

**Recommended Action** None required.

### 733100

**Error Message** `%FTD-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt`

**Explanation** The specified object in the message has exceeded the specified burst threshold rate or average threshold rate. The object can be a drop activity of a host, TCP/UDP port, IP protocol, or various drops caused by potential attacks. The Firepower Threat Defense device may be under attack.

- `Object` — The general or particular source of a drop rate count, which might include the following:
  - Firewall
  - Bad pkts
  - Rate limit
  - DoS attck
  - ACL drop
- Conn limit
- ICMP attk
- Scanning
- SYN attk
- Inspect
- Interface

(A citation of a particular interface object might take a number of forms. For example, you might see 80/HTTP, which would signify port 80, with the well-known protocol HTTP.)

- rate_ID — The configured rate that is being exceeded. Most objects can be configured with up to three different rates for different intervals.
- rate_val — A particular rate value.
- total_cnt — The total count since the object was created or cleared.

The following three examples show how these variables occur:

- For an interface drop caused by a CPU or bus limitation:

  %FTD-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654.”

- For a scanning drop caused by potential attacks:

  %FTD-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_max configured rate is 10; Current average rate is 245 per second_max configured rate is 5; Cumulative total count is 147409 (35 instances received)

- For bad packets caused by potential attacks:

  %FTD-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933

- Because of the scanning rate configured and the threat-detection rate scanning-rate 3600 average-rate 15 command:

  %FTD-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0 per second, max configured rate is 8; Current average rate is 5 per second, max configured rate is 4; Cumulative total count is 38086

Perform the following steps according to the specified object type that appears in the message:

1. If the object in the message is one of the following:
   - Firewall
   - Bad pkts
   - Rate limit
   - DoS attck
   - ACL drop
   - Conn limit
   - ICMP attck
   - Scanning
• SYN attack
• Inspect
• Interface

**Recommended Action** Check whether the drop rate is acceptable for the running environment.

1. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate `xxx` command, where `xxx` is one of the following:
   - acl-drop
   - bad-packet-drop
   - conn-limit-drop
   - dos-drop
   - fw-drop
   - icmp-drop
   - inspect-drop
   - interface-drop
   - scanning-threat
   - syn-attack

2. If the object in the message is a TCP or UDP port, an IP address, or a host drop, check whether or not the drop rate is acceptable for the running environment.

3. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate `bad-packet-drop` command.

---

**Note**

If you do not want the drop rate exceed warning to appear, you can disable it by using the `no threat-detection basic-threat` command.

---

**733101**

**Error Message** `%FTD-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.`

**Explanation** The Firepower Threat Defense device detected that a specific host (or several hosts in the same 1024-node subnet) is either scanning the network (attacking), or is being scanned (targeted).

- `object` — Attacker or target (a specific host or several hosts in the same 1024-node subnet)
- `objectIP` — The IP address of the scanning attacker or scanned target
- `rate_val` — A particular rate value
- `total_cnt` — The total count

The following two examples show how these variables occur:

- `%FTD-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per second, max configured rate is 0; Current average rate is 0 per second, max configured rate is 0; Cumulative total count is 2028.`
- `%FTD-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per second, max configured rate is 0; Current average rate is 0 per second, max configured rate is 0; Cumulative total count is 2024`
**Recommended Action** For the specific host or subnet, use the `show threat-detection statistics host ip-address ip-mask` command to check the overall situation and then adjust the threshold rate of the scanning threat to the appropriate value. After the appropriate value is determined, an optional action can be taken to shun those host attackers (not subnet attacker) by configuring the `threat-detection scanning-threat-shun-host` command. You may specify certain hosts or object groups in the shun-host except list. For more information, see the CLI configuration guide. If scanning detection is not desirable, you can disable this feature by using the `no threat-detection scanning` command.

---

**733102**

**Error Message** %FTD-4-733102: Threat-detection adds host %I to shun list

**Explanation** A host has been shunned by the threat detection engine. When the `threat-detection scanning-threat shun` command is configured, the attacking hosts will be shunned by the threat detection engine.

- %I — A particular hostname

The following message shows how this command was implemented:

%FTD-4-733102: Threat-detection add host 11.1.1.40 to shun list

**Recommended Action** To investigate whether the shunned host is an actual attacker, use the `threat-detection statistics host ip-address` command. If the shunned host is not an attacker, you can remove the shunned host from the threat detection engine by using the `clear threat-detection shun ip address` command. To remove all shunned hosts from the threat detection engine, use the `clear shun` command.

If you receive this message because an inappropriate threshold rate has been set to trigger the threat detection engine, then adjust the threshold rate by using the `threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z` command.

---

**733103**

**Error Message** %FTD-4-733103: Threat-detection removes host %I from shun list

**Explanation** A host has been shunned by the threat detection engine. When you use the `clear-threat-detection shun` command, the specified host will be removed from the shunned list.

- %I — A particular hostname

The following message shows how this command is implemented:

%FTD-4-733103: Threat-detection removes host 11.1.1.40 from shun list

**Recommended Action** None required.

---

**733104**

**Error Message** %FTD-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED

**Explanation** The Firepower Threat Defense device is under Syn flood attack and protected by the TCP intercept mechanism, if the average rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

**Recommended Action** Write an ACL to filter out the attacks.
733105

**ErrorMessage** %FTD-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED

**Explanation** The Firepower Threat Defense device is under Syn flood attack and protected by the TCP intercept mechanism, if the burst rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

**Recommended Action** Write an ACL to filter out the attacks.

734001

**ErrorMessage** %FTD-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names

**Explanation** The DAP records that were selected for the connection are listed.

- **user** — The authenticated username
- **ipaddr** — The IP address of the remote client
- **connection** — The type of client connection, which can be one of the following:
  - IPsec
  - AnyConnect
  - Clientless (web browser)
  - Cut-Through-Proxy
  - L2TP
- **DAP record names** — The comma-separated list of the DAP record names

**Recommended Action** None required.

734002

**ErrorMessage** %FTD-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names

**Explanation** The DAP records that terminated the connection are listed.

- **user** — The authenticated username
- **ipaddr** — The IP address of the remote client
- **DAP record names** — The comma-separated list of the DAP record names

**Recommended Action** None required.

734003

**ErrorMessage** %FTD-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value

**Explanation** The AAA and endpoint session attributes that are associated with the connection are listed.

- **user** — The authenticated username
- **ipaddr** — The IP address of the remote client
- attr/value — The AAA or endpoint attribute name and value

**Recommended Action** None required.

### 734004

**ErrorMessage** %FTD-3-734004: DAP: Processing error: internal error code

**Explanation** A DAP processing error occurred.

- internal error code — The internal error string

**Recommended Action** Enable the debug dap errors command and re-run DAP processing for further debugging information. If this does not resolve the issue, contact the Cisco TAC and provide the internal error code and any information about the conditions that generated the error.

### 735001

**ErrorMessage** %FTD-1-735001 IPMI: Cooling Fan var1 : OK

**Explanation** A cooling fan has been restored to normal operation.

- var1 — The device number markings

**Recommended Action** None required.

### 735002

**ErrorMessage** %FTD-1-735002 IPMI: Cooling Fan var1 : Failure Detected

**Explanation** A cooling fan has failed.

- var1 — The device number markings

**Recommended Action** Perform the following steps:

1. Check for obstructions that would prevent the fan from rotating.
2. Replace the cooling fan.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

### 735003

**ErrorMessage** %FTD-1-735003 IPMI: Power Supply var1 : OK

**Explanation** A power supply has been restored to normal operation.

- var1 — The device number markings

**Recommended Action** None required.

### 735004

**ErrorMessage** %FTD-1-735004 IPMI: Power Supply var1 : Failure Detected

**Explanation** AC power has been lost, or the power supply has failed.
• var1 —The device number markings

**Recommended Action** Perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

### 735005

**Error Message** %FTD-1-735005 IPMI: Power Supply Unit Redundancy OK

**Explanation** Power supply unit redundancy has been restored.

**Recommended Action** None required.

### 735006

**Error Message** %FTD-1-735006 IPMI: Power Supply Unit Redundancy Lost

**Explanation** A power supply failure occurred. Power supply unit redundancy has been lost, but the Firepower Threat Defense device is functioning normally with minimum resources. Any further failures will result in an Firepower Threat Defense device shutdown.

**Recommended Action** To regain full redundancy, perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

### 735007

**Error Message** %FTD-1-735007 IPMI: CPU var1: Temp: var2 var3, Critical

**Explanation** The CPU has reached a critical temperature.

• var1 —The device number markings
• var2 —The temperature value
• var3 —Temperature value units (C, F)

**Recommended Action** Record the message as it appears and contact the Cisco TAC.

### 735008

**Error Message** %FTD-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical

**Explanation** A chassis ambient temperature sensor has reached a critical level.

• var1 —The device number markings
• var2 —The temperature value
• var3 —Temperature value units (C, F)

**Recommended Action** Record the message as it appears and contact the Cisco TAC.
735009

**Error Message**  %FTD-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.

**Explanation** Environment monitoring has experienced a fatal error during initialization and was unable to continue.

**Recommended Action** Collect the output of the `show environment` and `debug ipmi` commands. Record the message as it appears and contact the Cisco TAC.

735010

**Error Message**  %FTD-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.

**Explanation** Environment monitoring has experienced an error that temporarily prevented it from updating one or more of its records.

**Recommended Action** If this message appears repeatedly, collect the output from the `show environment` driver and `debug ipmi` commands. Record the message as it appears and contact the Cisco TAC.

735011

**Error Message**  %FTD-1-735011: Power Supply `var1`: Fan OK

**Explanation** The power supply fan has returned to a working operating state.

- `var1` — Fan number

**Recommended Action** None required.

735012

**Error Message**  %FTD-1-735012: Power Supply `var1`: Fan Failure Detected

**Explanation** The power supply fan has failed.

- `var1` — Fan number

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735013

**Error Message**  %FTD-1-735013: Voltage Channel `var1`: Voltage OK

**Explanation** A voltage channel has returned to a normal operating level.

- `var1` — Voltage channel number

**Recommended Action** None required.
735014

**Error Message** %FTD-1-735014: Voltage Channel var1: Voltage Critical

**Explanation** A voltage channel has changed to a critical level.

- **var1** — Voltage channel number

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735015

**Error Message** %FTD-4-735015: CPU var1 : Temp: var2 var3 , Warm

**Explanation** The CPU temperature is warmer than the normal operating range.

- **var1** — CPU Number
- **var2** — Temperature Value
- **var3** — Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

735016

**Error Message** %FTD-4-735016: Chassis Ambient var1 : Temp: var2 var3 , Warm

**Explanation** The chassis temperature is warmer than the normal operating range.

- **var1** — Chassis Sensor Number
- **var2** — Temperature Value
- **var3** — Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

735017

**Error Message** %FTD-1-735017: Power Supply var1 : Temp: var2 var3 , OK

**Explanation** The power supply temperature has returned to a normal operating temperature.

- **var1** — Power Supply Number
- **var2** — Temperature Value
- **var3** — Units

**Recommended Action** None required.

735018

**Error Message** %FTD-4-735018: Power Supply var1 : Temp: var2 var3 , Critical

**Explanation** The power supply has reached a critical operating temperature.
• var1 — Power Supply Number
• var2 — Temperature Value
• var3 — Units

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735019

**Error Message** %FTD-4-735019: Power Supply var1: Temp: var2 var3 , Warm

**Explanation** The power supply temperature is warmer than the normal operating range.

• var1 — Power Supply Number
• var2 — Temperature Value
• var3 — Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

735020

**Error Message** %FTD-1-735020: CPU var1: Temp: var2 var3 OK

**Explanation** The CPU temperature has returned to the normal operating temperature.

• var1 — CPU Number
• var2 — Temperature Value
• var3 — Units

**Recommended Action** None required.

735021

**Error Message** %FTD-1-735021: Chassis var1: Temp: var2 var3 OK

**Explanation** The chassis temperature has returned to the normal operating temperature.

• var1 — Chassis Sensor Number
• var2 — Temperature Value
• var3 — Units

**Recommended Action** None required.

735022

**Error Message** %FTD-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.

**Explanation** The Firepower Threat Defense device has detected a CPU running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.
**735023**

**Error Message** %FTD-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.

**Explanation** At boot time, the Firepower Threat Defense device detected a shutdown that occurred because a CPU was running beyond the maximum safe operating temperature. Using the `show environment` command will indicate that this event has occurred.

**Recommended Action** The chassis need to be inspected immediately for ventilation issues.

---

**735024**

**Error Message** %FTD-1-735024: IO Hub var1 : Temp: var2 var3 , OK

**Explanation** The IO hub temperature has returned to the normal operating temperature.

- `var1` - IO hub number
- `var2` - Temperature value
- `var3` - Units

**Recommended Action** None required.

---

**735025**

**Error Message** %FTD-1-735025: IO Hub var1 : Temp: var2 var3 , Critical

**Explanation** The IO hub temperature has a critical temperature.

- `var1` - IO hub number
- `var2` - Temperature value
- `var3` - Units

**Recommended Action** Record the message as it appears and contact the Cisco TAC.

---

**735026**

**Error Message** %FTD-4-735026: IO Hub var1 : Temp: var2 var3 , Warm

**Explanation** The IO hub temperature is warmer than the normal operating range.

- `var1` - IO hub number
- `var2` - Temperature value
- `var3` - Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.
735027

**Error Message** %FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.

**Explanation** The Firepower Threat Defense device has detected a CPU voltage regulator running beyond the maximum thermal operating temperature, and shuts down immediately after detection.

• cpu_num — The number to identify which CPU voltage regulator experienced the thermal event

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.

735028

**Error Message** %FTD-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.

**Explanation** At boot time, the Firepower Threat Defense device detected a shutdown that occurred because of a CPU voltage regulator running beyond the maximum safe operating temperature. Enter the show environment command to indicate that this event has occurred.

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.

735029

**Error Message** %FTD-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.

**Explanation** The Firepower Threat Defense device has detected that the IO hub is running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

**Recommended Action** The chassis and IO hub need to be inspected immediately for ventilation issues.

736001

**Error Message** %FTD-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.

**Explanation** Insufficient memory has been detected when jumbo frame support was being configured. As a result, jumbo-frame support was disabled.

**Recommended Action** Try reenabling jumbo frame support using the jumbo-frame reservation command. Save the running configuration and reboot the Firepower Threat Defense device. If the problem persists, contact the Cisco TAC.

Messages 737001 to 776254

This section includes messages from 737001 to 776254.
737001

**Error Message** %FTD-7-737001: IPAA: Received message message-type

**Explanation** The IP address assignment process received a message.

- **message-type** — The message received by the IP address assignment process

**Recommended Action** None required.

737002

**Error Message** %FTD-3-737002: IPAA: Session= session, Received unknown message num variables

**Explanation** The IP address assignment process received a message.

- **session** — The session is the VPN session ID in hexadecimal.
- **num** — The identifier of the message received by the IP address assignment process

**Recommended Action** None required.

737003

**Error Message** %FTD-5-737003: IPAA: Session= session, DHCP configured, no viable servers found for tunnel-group tunnel-group

**Explanation** The DHCP server configuration for the given tunnel group is not valid.

- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

737004

**Error Message** %FTD-5-737004: IPAA: Session= session, DHCP configured, request failed for tunnel-group 'tunnel-group'

**Explanation** The DHCP server configuration for the given tunnel group is not valid.

- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

737005

**Error Message** %FTD-6-737005: IPAA: Session= session, DHCP configured, request succeeded for tunnel-group tunnel-group

**Explanation** The DHCP server request has succeeded.
- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** None required.

### 737006

**Error Message** `%FTD-6-737006: IPAA: Session= session, Local pool request succeeded for tunnel-group tunnel-group`

**Explanation** The local pool request has succeeded.
- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** None required.

### 737007

**Error Message** `%FTD-5-737007: IPAA: Session= session, Local pool request failed for tunnel-group tunnel-group`

**Explanation** The local pool request has failed. The pool assigned to the tunnel group may be exhausted.
- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the IP local pool configuration by using the `show ip local pool` command.

### 737008

**Error Message** `%FTD-5-737008: IPAA: Session= session, 'tunnel-group' not found`

**Explanation** The tunnel group was not found when trying to acquire an IP address for configuration. A software defect may cause this message to be generated.
- **session** — The session is the VPN session ID in hexadecimal.
- **tunnel-group** — The tunnel group that IP address assignment is using for configuration

**Recommended Action** Check the tunnel group configuration. Contact the Cisco TAC and report the issue.

### 737009

**Error Message** `%FTD-6-737009: IPAA: Session= session, AAA assigned address ip-address , request failed`

**Explanation** The remote access client software requested the use of a particular address. The request to the AAA server to use this address failed. The address may be in use.
- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address that the client requested
Recommended Action Check the AAA server status and the status of IP local pools.

737010

Error Message %FTD-6-737010: IPAA: Session= session, AAA assigned address ip-address, request succeeded

Explanation The remote access client software requested the use of a particular address and successfully received this address.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address that the client requested

Recommended Action None required.

737011

Error Message %FTD-5-737011: IPAA: Session= session, AAA assigned ip-address, not permitted, retrying

Explanation The remote access client software requested the use of a particular address. The `vpn-addr-assign` `aaa` command is not configured. An alternatively configured address assignment method will be used.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address that the client requested

Recommended Action If you want to permit clients to specify their own address, enable the `vpn-addr-assign` `aaa` command.

737012

Error Message %FTD-4-737012: IPAA: Session= session, Address assignment failed

Explanation The remote access client software request of a particular address failed.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IP address that the client requested

Recommended Action If using IP local pools, validate the local pool configuration. If using AAA, validate the configuration and status of the AAA server. If using DHCP, validate the configuration and status of the DHCP server. Increase the logging level (use notification or informational) to obtain additional messages to identify the reason for the failure.

737013

Error Message %FTD-4-737013: IPAA: Session= session, Error freeing address ip-address, not found

Explanation The Firepower Threat Defense device tried to free an address, but it was not on the allocated list because of a recent configuration change.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address to be released

**Recommended Action** Validate your address assignment configuration. If this message recurs, it might be due to a software defect. Contact the Cisco TAC and report the issue.

### 737014

**Error Message** %FTD-6-737014: IPAA: Session= session, Freeing AAA address ip-address

**Explanation** The Firepower Threat Defense device successfully released the IP address assigned through AAA.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address to be released

**Recommended Action** None required.

### 737015

**Error Message** %FTD-6-737015: IPAA: Session= session, Freeing DHCP address ip-address

**Explanation** The Firepower Threat Defense device successfully released the IP address assigned through DHCP.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IP address to be released

**Recommended Action** None required.

### 737016

**Error Message** %FTD-6-737016: IPAA: Session= session, Freeing local pool pool-name address ip-address

**Explanation** The Firepower Threat Defense device successfully released the IP address assigned through local pools.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IPv4 or IPv6 address to be released
- **pool-name** — The pool to which the address is being returned to

**Recommended Action** None required.

### 737017

**Error Message** %FTD-6-737017: IPAA: Session= session, DHCP request attempt num succeeded

**Explanation** The Firepower Threat Defense device successfully sent a request to a DHCP server.

- **session** — The session is the VPN session ID in hexadecimal.
- **num** — The attempt number

**Recommended Action** None required.
**737018**

**Error Message** %FTD-5-737018: IPAA: Session= session, DHCP request attempt num failed

**Explanation** The Firepower Threat Defense device failed to send a request to a DHCP server.

- **session** — The session is the VPN session ID in hexadecimal.
- **num** — The attempt number

**Recommended Action** Validate the DHCP configuration and connectivity to the DHCP server.

**737019**

**Error Message** %FTD-4-737019: IPAA: Session= session, Unable to get address from group-policy or tunnel-group local pools

**Explanation** The Firepower Threat Defense device failed to acquire an address from the local pools configured on the group policy or tunnel group. The local pools may be exhausted.

- **session** — The session is the VPN session ID in hexadecimal.

**Recommended Action** Validate the local pool configuration and status. Validate the group policy and tunnel group configuration of local pools.

**737023**

**Error Message** %FTD-5-737023: IPAA: Session= session, Unable to allocate memory to store local pool address ip-address

**Explanation** The Firepower Threat Defense device is low on memory.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IP address that was acquired

**Recommended Action** The Firepower Threat Defense device may be overloaded and need more memory, or there may be a memory leak caused by a software defect. Contact the Cisco TAC and report the issue.

**737024**

**Error Message** %FTD-5-737024: IPAA: Session= session, Client requested address ip-address, already in use, retrying

**Explanation** The client requested an IP address that is already in use. The request will be tried using a new IP address.

- **session** — The session is the VPN session ID in hexadecimal.
- **ip-address** — The IP address that the client requested

**Recommended Action** None required.
737025

Error Message %FTD-5-737025: IPAA:Session= session, Duplicate local pool address found, ip-address in quarantine

Explanation The IP address that was to be given to the client is already in use. The IP address has been removed from the pool and will not be reused.

- session — The session is the VPN session ID in hexadecimal.
- ip-address — The IP address that was acquired

Recommended Action Validate the local pool configuration; there may be an overlap caused by a software defect. Contact the Cisco TAC and report the issue.

737026

Error Message %FTD-6-737026: IPAA:Session= session, Client assigned ip-address from local pool pool-name

Explanation The client has assigned the given address from a local pool.

- session — The session is the VPN session ID in hexadecimal.
- ip-address — The IP address that was assigned to the client
- pool-name — The pool from which the address was allocated

Recommended Action None required.

737027

Error Message %FTD-3-737027: IPAA:Session= session, No data for address request

Explanation A software defect has been found.

- session — The session is the VPN session ID in hexadecimal.

Recommended Action Contact the Cisco TAC and report the issue.

737028

Error Message %FTD-4-737028: IPAA:Session= session, Unable to send ip-address to standby: communication failure

Explanation The active Firepower Threat Defense device was unable to communicate with the standby Firepower Threat Defense device. The failover pair may be out-of-sync.

- session — The session is the VPN session ID in hexadecimal.
- ip-address — The IP address that was assigned to the client

Recommended Action Validate the failover configuration and status.
737029

**Error Message** %FTD-6-737029: IPAA:Session= session, Added ip-address to standby  

**Explanation** The standby Firepower Threat Defense device accepted the IP address assignment.  
- *session* — The session is the VPN session ID in hexadecimal.  
- *ip-address* — The IP address that was assigned to the client  

**Recommended Action** None required.

737030

**Error Message** %FTD-4-737030: IPAA:Session= session, Unable to send ip-address to standby: address in use  

**Explanation** The standby Firepower Threat Defense device has the given address already in use when the active Firepower Threat Defense device attempted to acquire it. The failover pair may be out-of-sync.  
- *session* — The session is the VPN session ID in hexadecimal.  
- *ip-address* — The IP address that was assigned to the client  

**Recommended Action** Validate the failover configuration and status.

737031

**Error Message** %FTD-6-737031: IPAA:Session= session, Removed ip-address from standby  

**Explanation** The standby Firepower Threat Defense device cleared the IP address assignment.  
- *session* — The session is the VPN session ID in hexadecimal.  
- *ip-address* — The IP address that was assigned to the client  

**Recommended Action** None required.

737032

**Error Message** %FTD-4-737032: IPAA:Session= session, Unable to remove ip-address from standby: address not found  

**Explanation** The standby Firepower Threat Defense device did not have an IP address in use when the active Firepower Threat Defense device attempted to release it. The failover pair may be out-of-sync.  
- *session* — The session is the VPN session ID in hexadecimal.  
- *ip-address* — The IP address that was assigned to the client  

**Recommended Action** Validate the failover configuration and status.
Error Message %FTD-4-737033: IPAA: Session= session, Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator

Explanation The address assigned by the AAA/DHCP/local pool is already in use.

- session — The session is the VPN session ID in hexadecimal.
- addr_allocator — The DHCP/AAA/local pool
- ip_addr — The IP address allocated by the DHCP/AAA/local pool
- previous_addr_allocator — The address allocator that already assigned the IP address (local pool, AAA, or DHCP)

Recommended Action Validate the AAA/DHCP/local pool address configurations. Overlap may occur.

Error Message %FTD-5-737034: IPAA: Session= session, <IP version> address: <explanation>

Explanation The IP address assignment process is unable to provide an address. The <explanation> text will describe the reason.

- session — The session is the VPN session ID in hexadecimal.

Recommended Action Action will be based on explanation.

Error Message %FTD-7-737035: IPAA: Session= session, '<message type>' message queued

Explanation A message is queued to the IP address assignment. This corresponds with syslog 737001. This message is not rate limited.

- session — The session is the VPN session ID in hexadecimal.

Recommended Action No action required.

Error Message %FTD-6-737035: IPAA: Session= session, Client assigned <address> from DHCP

Explanation IP address assignment process has provided a DHCP provisioned address back to the VPN client. This message is not rate limited.

- session — The session is the VPN session ID in hexadecimal.

Recommended Action No action required.
737038

**Error Message** %FTD-7-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.

**Explanation** This log occurs when the AAA server (internal or external) has specified an address to assign to the user; but this address already in-use. The request is being re-queued without a specified address to fall back to DHCP or local pools.

- **session** —The VPN session ID of the requesting session.
- **ip-address** —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

737200

**Error Message** %FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool

**Explanation** This log occurs an address is allocated from a local pool.

- **pool** —The local pool name.
- **ip-address** —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

737201

**Error Message** %FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)

**Explanation** This log occurs when an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision, the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- **pool** —The local pool name.
- **ip-address** —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

737202

**Error Message** %FTD-3-737202: VPNFIP: Pool=pool, ERROR: message

**Explanation** This log is generated when an error event is detected related to the VPN FIP database.

- **pool** —The local pool name.
- **message** —The details for the event.

**Recommended Action** If error is persistent, contact Cisco TAC.
737203

**Error Message** %FTD-4-737203: VPNFIP: Pool=pool, WARN: message

**Explanation** This log is generated to warn of an event related to the VPN FIP database.
- `pool` — The local pool name.
- `message` — The details for the event.

**Recommended Action** If warning is persistent, contact Cisco TAC.

737204

**Error Message** %FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message

**Explanation** This log is generated to notify of an event related to the VPN FIP database.
- `pool` — The local pool name.
- `message` — The details for the event.

**Recommended Action** None required

737205

**Error Message** %FTD-6-737205: VPNFIP: Pool=pool, INFO: message

**Explanation** This log is generated to inform of an event related to the VPN FIP database.
- `pool` — The local pool name.
- `message` — The details for the event.

**Recommended Action** None required

737206

**Error Message** %FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message

**Explanation** This log is generated to debug an event related to the VPN FIP database.
- `pool` — The local pool name.
- `message` — The details for the event.

**Recommended Action** None required

737400

**Error Message** %FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool

**Explanation** This log occurs an address is allocated from a local pool.
- `pool` — The local pool name
**737401**

**Error Message** `%FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle).`

**Explanation** This log occurs an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision—the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- **pool** —The local pool name
- **ip-address** —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

---

**737402**

**Error Message** `%FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message`

**Explanation** This log occurs unable to return an address to an address pool.

- **pool** —The local pool name
- **ip-address** —The IPv4 or IPv6 address specified by AAA
- **message** —The details of the failure. (For example, address not in pool range)

**Recommended Action** None required

---

**737403**

**Error Message** `%FTD-3-737403: POOLIP: Pool=pool, ERROR: message`

**Explanation** This log is generated when an error event is detected related to an IP local pool database.

- **pool** —The local pool name
- **message** —The details for the event.

**Recommended Action** If error is persistent, contact Cisco TAC.

---

**737404**

**Error Message** `%FTD-4-737404: POOLIP: Pool=pool, WARN: message`

**Explanation** This log is generated to warn of an event related to an IP local pool database.

- **pool** —The local pool name
- **message** —The details for the event.
**Recommended Action** If warning is persistent, contact Cisco TAC.

---

**737405**

**Error Message** %FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message

**Explanation** This log is generated to notify of an event related to an IP local pool database.

- *pool* — The local pool name
- *message* — The details for the event.

**Recommended Action** None required

---

**737406**

**Error Message** %FTD-6-737406: POOLIP: Pool=pool, INFO: message

**Explanation** This log is generated to inform of an event related to an IP local pool database.

- *pool* — The local pool name
- *message* — The details for the event.

**Recommended Action** None required

---

**737407**

**Error Message** %FTD-7-737407: POOLIP: Pool=pool, DEBUG: message

**Explanation** This log is generated to debug an event related to an IP local pool database.

- *pool* — The local pool name
- *message* — The details for the event.

**Recommended Action** None required

---

**741000**

**Error Message** %FTD-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB

**Explanation** A core dump file system was successfully created. The file system is used to manage core dumps by capping the amount of disk space that core dumps may use.

- *variable 1* — The file system on which the core dumps are placed (for example, disk0:, disk1:, and flash:)
- *variable 2* — The size of the created core dump file system in MB

**Recommended Action** Make sure that you save your configuration after creating the core dump file system.
ErrorMessage %FTD-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB

Explanation The core dump file system has been successfully resized.

- variable 1 —The file system on which the core dumps are placed
- variable 2 —The size of the previous core dump file system in MB
- variable 3 —The size of the current, newly resized core dump file system in MB

Recommended Action Make sure that you save your configuration after resizing the core dump file system. Resizing the core dump file system deletes the contents of the existing core dump file system. As a result, make sure that you archive any information before you resize the core dump file system.

ErrorMessage %FTD-6-741002: Coredump log and filesystem contents cleared on variable 1

Explanation All core dumps have been deleted from the core dump file system, and the core dump log has been cleared. The core dump file system and coredump log are always synchronized with each other.

- variable 1 —The file system on which the core dumps are placed (for example, disk0:, disk1:, and flash:)

Recommended Action None required. You can clear the core dump file system to reset it to a known state using the clear coredump command.

ErrorMessage %FTD-6-741003: Coredump filesystem and its contents removed on variable 1

Explanation The core dump file system and its contents have been removed, and the core dump feature has been disabled.

- variable 1 —The file system on which the core dumps are placed (for example, disk0:, disk1:, and flash:)

Recommended Action Make sure that you save your configuration after the core dump feature has been disabled.

ErrorMessage %FTD-6-741004: Coredump configuration reset to default values

Explanation The core dump configuration has been reset to its default value, which is disabled.

Recommended Action Make sure that you save your configuration after the core dump feature has been disabled.

ErrorMessage %FTD-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3

Explanation An error occurred during the performance of a core dump-related operation.
• variable 1 — This variable may have the following values:
  - CREATE_FSYS—An error occurred when creating the core dump file system.
  - CLEAR_LOG—An error occurred when clearing the core dump log.
  - DELETE_FSYS—An error occurred when deleting the core dump file system.
  - CLEAR_FSYS—An error occurred when removing the contents of the core dump file system.
  - MOUNT_FSYS—An error occurred when mounting the core dump file system.
    • variable 2 — The decimal number that provides additional information about the cause of the error specified in variable 1.
    • variable 3 — The descriptive ASCII string associated with variable 2. The ASCII string can have the following values:
      - coredump files already exist
      - unable to create coredump filesystem
      - unable to create loopback device
      - filesystem type not supported
      - unable to delete the coredump filesystem
      - unable to delete loopback device
      - unable to unmount coredump filesystem
      - unable to mount coredump filesystem
      - unable to mount loopback device
      - unable to clear coredump filesystem
      - coredump filesystem not found
      - requested coredump filesystem too big
      - coredump operation aborted by administrator
      - coredump command execution failed
      - coredump IFS error encountered
      - coredump, unidentified error encountered

Recommended Action Make sure that the core dump feature is disabled in the configuration, and send the message to the Cisco TAC for further analysis.

Error Message FTD-4-741006: Unable to write Coredump Helper configuration, reason variable 1

Explanation An error occurred when writing to the coredump helper configuration file. This error occurs only if disk0: is full. The configuration file is located in disk0:.coredumpinfo/coredump.cfg.

• variable 1 — This variable includes a basic file system-related string that indicates why the writing of the core dump helper configuration file failed.
**Recommended Action** Disable the core dump feature, remove unneeded items from disk0:, and then reenable core dumps, if desired.

**742001**

**Error Message** %FTD-3-742001: failed to read master key for password encryption from persistent store

**Explanation** An attempt to read the master password encryption key from the nonvolatile memory after bootup failed. Encrypted passwords in the configuration are not decrypted unless the master key is set to the correct value using the `key config-key password encryption` command.

**Recommended Action** If there are encrypted passwords in the configuration that must be used, set the master key to the previous value used to encrypt the password using the `key config-key password encryption` command. If there are no encrypted passwords or they can be discarded, set a new master key. If password encryption is not used, no action is required.

**742002**

**Error Message** %FTD-3-742002: failed to set master key for password encryption

**Explanation** An attempt to read the `key config-key password encryption` command failed. The error may be caused by the following reasons:

- Configuration from a nonsecure terminal (for example, over a Telnet connection) was made.
- Failover is enabled, but it does not use an encrypted link.
- Another user is setting the key at the same time.
- When trying to change the key, the old key is incorrect.
- The key is too small to be secure.

Other reasons for the error may be valid. In these cases, the actual error is printed in response to the command.

**Recommended Action** Correct the problem indicated in the command response.

**742003**

**Error Message** %FTD-3-742003: failed to save master key for password encryption, reason `reason_text`

**Explanation** An attempt to save the master key to nonvolatile memory failed. The actual reason is specified by the `reason_text` parameter. The reason can be an out-of-memory condition, or the nonvolatile store can be inconsistent.

**Recommended Action** If the problem persists, reformat the nonvolatile store that is used to save the key by using the `write erase` command. Before performing this step, make sure that you back up the out-of-the-box configuration. Then reenter the `write erase` command.

**742004**

**Error Message** %FTD-3-742004: failed to sync master key for password encryption, reason `reason_text`
Explanation An attempt to synchronize the master key to the peer failed. The actual reason is specified by the `reason_text` parameter.

**Recommended Action** Try to correct the problem specified in the `reason_text` parameter.

---

**Error Message** `%FTD-3-742005`: cipher text `enc_pass` is not compatible with the configured master key or the cipher text has been tampered with

**Explanation** An attempt to decrypt a password failed. The password may have been encrypted using a master key that is different from the current master key, or the encrypted password has been changed from its original form.

**Recommended Action** If the correct master key is not being used, correct the problem. If the encrypted password has been modified, reapply the configuration in question with a new password.

---

**Error Message** `%FTD-3-742006`: password decryption failed due to unavailable memory

**Explanation** An attempt to decrypt a password failed because no memory was available. Features using this password will not work as desired.

**Recommended Action** Correct the memory problem.

---

**Error Message** `%FTD-3-742007`: password encryption failed due to unavailable memory

**Explanation** An attempt to encrypt a password failed because no memory was available. Passwords may be left in clear text form in the configuration.

**Recommended Action** Correct the memory problem, and reapply the configuration that failed password encryption.

---

**Error Message** `%FTD-3-742008`: password `enc_pass` decryption failed due to decoding error

**Explanation** Password decryption failed because of decoding errors, which may occur if the encrypted password has been modified after being encrypted.

**Recommended Action** Reapply the configuration in question with a clear text password.

---

**Error Message** `%FTD-3-742009`: password encryption failed due to decoding error

**Explanation** Password encryption failed because of decoding errors, which may be an internal software error.

**Recommended Action** Reapply the configuration in question with a clear text password. If the problem persists, contact the Cisco TAC.
742010

**Error Message** %FTD-3-742010: encrypted password enc_pass is not well formed

**Explanation** The encrypted password provided in the command is not well formed. The password may not be a valid, encrypted password, or it may have been modified since it was encrypted.

- **reason_text** — A string that represents the actual cause of the failure
- **enc_pass** — The encrypted password that is related to the issue

**Recommended Action** Reapply the configuration in question with a clear text password.

743000

**Error Message** %FTD-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val.

**Explanation** A PCI device in the system is not configured correctly, which may result in the system not performing at its optimum level.

**Recommended Action** Collect the output of the `show controller pci detail` command, and contact the Cisco TAC.

743001

**Error Message** %FTD-1-743001: Backplane health monitoring detected link failure

**Explanation** A hardware failure has probably occurred and has been detected on one of the links between the Firepower Threat Defense Services Module and the switch chassis.

**Recommended Action** Contact the Cisco TAC.

743002

**Error Message** %FTD-1-743002: Backplane health monitoring detected link OK

**Explanation** A link has been restored between the Firepower Threat Defense Services Module and the switch chassis. However, the failure and subsequent recovery probably indicates a hardware failure.

**Recommended Action** Contact the Cisco TAC.

743004

**Error Message** %FTD-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name ), device ID device_id (device_name ) not found

**Explanation** A PCI device in the system that is needed for it to be fully operational was not found.

- **vendor_id** — Hexadecimal value that identifies the device vendor
- **vendor_name** — Text string that identifies the vendor name
- **device_id** — Hexadecimal value that identifies the vendor device
- **device_name** — Text string that identifies the device name
**Recommended Action** Collect the output of the `show controller pci detail` command and contact the Cisco TAC.

743010

**Error Message** `%FTD-3-743010: EOBC RPC server failed to start for client module client name`.
**Explanation** The service failed to start for a particular client of the EOBC RPC service on the server.
**Recommended Action** Call the Cisco TAC.

743011

**Error Message** `%FTD-3-743011: EOBC RPC call failed, return code code string`.
**Explanation** The EOBC RPC client failed to make an RPC to the intended server.
**Recommended Action** Call the Cisco TAC.

746014

**Error Message** `%FTD-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete`.
**Explanation** A fully qualified domain name has become obsolete.
**Recommended Action** None required.

746015

**Error Message** `%FTD-5-746015: user-identity: FQDN] fqdn resolved IP address`.
**Explanation** A fully qualified domain name lookup has succeeded.
**Recommended Action** None required.

746016

**Error Message** `%FTD-3-746016: user-identity: DNS lookup failed, reason: reason`.
**Explanation** A DNS lookup has failed. Failure reasons include timeout, unresolvable, and no memory.
**Recommended Action** Verify that the FQDN is valid, and that the DNS server is reachable from the ASA. If the problem persists, contact the Cisco TAC.

747001

**Explanation** The cluster FSM event queue is full, and a new event has been dropped.
**Recommended Action** None.
747002


Explanation The cluster FSM received an event that is incompatible with the current state.

Recommended Action None.

747003

Error Message %FTD-5-747003: Clustering: Recovered from state machine failure to process event (event-id, ptr-in-hex, ptr-in-hex) at state state-name.

Explanation The cluster FSM failed to process an event for all reasons given.

Recommended Action None.

747004

Error Message %FTD-6-747004: Clustering: state machine changed from state state-name to state-name.

Explanation The cluster FSM has progressed to a new state.

Recommended Action None.

747005

Error Message %FTD-7-747005: Clustering: State machine notify event event-name (event-id, ptr-in-hex, ptr-in-hex)

Explanation The cluster FSM has notified clients about an event.

Recommended Action None.

747006

Error Message %FTD-7-747006: Clustering: State machine is at state state-name

Explanation The cluster FSM moved to a stable state; that is, Disabled, Slave, or Master.

Recommended Action None.

747007


Explanation Astray configuration sync thread has been detected.

Recommended Action None.
747008

**Error Message** %FTD-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B.

**Explanation** The same unit name has been configured on multiple units.

**Recommended Action** None.

---

747009

**Error Message** %FTD-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name.

**Explanation** The Firepower Threat Defense device failed to create an RPC server.

**Recommended Action** Disable clustering on this unit and try to re-enable it. Contact the Cisco TAC if the problem persists.

---

747010

**Error Message** %FTD-3-747010: Clustering: RPC call failed, message message-name, return code code-value.

**Explanation** An RPC call failure has occurred. The system tries to recover from the failure.

**Recommended Action** None.

---

747011

**Error Message** %FTD-2-747011: Clustering: Memory allocation error.

**Explanation** A memory allocation failure occurred in clustering.

**Recommended Action** Disable clustering on this unit and try to re-enable it. If the problem persists, check the memory usage on the Firepower Threat Defense device.

---

747012

**Error Message** %FTD-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continuing operation.

**Explanation** A global object ID replication failure has occurred.

**Recommended Action** None.

---

747013

**Error Message** %FTD-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continuing operation.

**Explanation** A global object ID removal failure has occurred.
Recommended Action None.

747014

Error Message %FTD-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name, continuing operation.
Explanation A global object ID installation failure has occurred.
Recommended Action None.

747015

Error Message %FTD-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
Explanation A stray cluster member has been found.
Recommended Action None.

747016

Error Message %FTD-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A, unit-name-B will leave, then join as a slave.
Explanation A split cluster has been found.
Recommended Action None.

747017

Error Message %FTD-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
Explanation The Firepower Threat Defense device failed to enroll a new unit because the maximum member limit has been reached.
Recommended Action None.

747018

Error Message %FTD-3-747018: Clustering: State progression failed due to timeout in module module-name.
Explanation The cluster FSM progression has timed out.
Recommended Action None.

747019

Error Message %FTD-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address /ip-mask on new unit, ip-address /ip-mask on local unit).
Explanation The master unit found that a new joining unit has an incompatible cluster interface IP address.
Recommended Action None.

**747020**

Error Message %FTD-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
Explanation The master unit found that a new joining unit has an incompatible encryption license.
Recommended Action None.

**747021**

Error Message %FTD-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on interface-name.
Explanation The master unit has disabled clustering because of an interface health check failure.
Recommended Action None.

**747022**

Error Message %FTD-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name.
Explanation This syslog message occurs when the maximum number of rejoin attempts has not been exceeded. A slave unit has disabled clustering because of an interface health check failure for the specified amount of time. This unit will re-enable itself automatically after the specified amount of time (ms).
Recommended Action None.

**747025**

Error Message %FTD-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
Explanation A master unit found a joining unit that has an incompatible firewall mode.
Recommended Action None.

**747026**

Error Message %FTD-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).
Explanation A master unit found a joining unit that has an incompatible cluster control link interface name.
Recommended Action None.
**747027**

**Error Message** %FTD-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.

**Explanation** A master unit could not enroll a joining unit because of the size limit of the minimal cluster pool configured.

**Recommended Action** None.

**747028**

**Error Message** %FTD-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).

**Explanation** A master unit found a joining unit that has an incompatible interface-mode, either spanned or individual.

**Recommended Action** None.

**747029**

**Error Message** %FTD-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.

**Explanation** A unit disabled clustering because of a cluster interface failure.

**Recommended Action** None.

**747030**

**Error Message** %FTD-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name), Clustering must be manually enabled on the unit to re-join.

**Explanation** An interface health check has failed and the maximum number of rejoin attempts has been exceeded. A slave unit has disabled clustering because of an interface health check failure.

**Recommended Action** None.

**747031**

**Error Message** %FTD-3-747031: Clustering: Platform mismatch between cluster master (platform-type) and joining unit unit-name (platform-type), unit-name aborting cluster join.

**Explanation** The joining unit's platform type does not match with that of the cluster master.

- unit-name — Name of the unit in the cluster bootstrap
- platform-type — Type of Firepower Threat Defense platform

**Recommended Action** Make sure that the joining unit has the same platform type as that of the cluster master.
### 747032

**Error Message**  %FTD-3-747032: Clustering: Service module mismatch between cluster master {module-name} and joining unit unit-name {module-name} in slot slot-number. unit-name aborting cluster join.

**Explanation** The joining unit's external modules are not consistent (module type and order in which they are installed) with those on the cluster master.

- **module-name** — Name of the external module
- **unit-name** — Name of the unit in the cluster bootstrap
- **slot-number** — The number of the slot in which the mismatch occurred

**Recommended Action** Make sure that the modules installed on the joining unit are of the same type and are in the same order as they are in the cluster master.

### 747033

**Error Message**  %FTD-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name. unit-name aborting cluster join.

**Explanation** The joining unit's interfaces are not the same as those on the cluster master.

- **unit-name** — Name of the unit in the cluster bootstrap

**Recommended Action** Make sure that the interfaces available on the joining unit are the same as those on the cluster master.

### 747034

**Error Message**  %FTD-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin). Rejoin will be attempted after %d minutes.

**Explanation** Cluster Control Link down and the unit is kicked out with rejoin.

**Recommended Action** Wait for the unit to rejoin.

### 747035

**Error Message**  %FTD-4-747035: Unit %s is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.

**Explanation** Cluster Control Link down and the unit is kicked out without rejoin.

**Recommended Action** Rejoin the unit manually.

### 747036

**Error Message**  %FTD-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]). %s[Joining member name] aborting cluster join.

**Explanation** The applications on master and the joining slave are not the same. Slave will be kicked out.
**Recommended Action**  Make sure that the slave run the same applications/services, and manually rejoin the unit.

**747042**

**Error Message**  %FTD-3-747042: Clustering: Master received the config hash string request message from an unknown member with id cluster-member-id

**Explanation**  Master unit received the config hash string request event.

**Recommended Action**  Verify requestor member is still in OnCall state.

**747043**

**Error Message**  %FTD-3-747043: Clustering: Get config hash string from master error: ret_code, string_len

**Explanation**  Failed to get config hash string from master unit.

- **ret_code** — The error return code; 0 indicates OK, and 1 indicates Failed
- **string_len** — The hash_str length

**Recommended Action**  Contact technical support to troubleshoot the issue on master unit. Ensure to turn on ‘debug cluster ccp’ to identify the root cause.

**747044**

**Error Message**  %FTD-6-747044: Configuration Hash string verification result

**Explanation**  The result of configuration hash string comparison.

- **result** — This result can be PASSED or FAILED

**Recommended Action**  None required.

**748001**

**Error Message**  %FTD-5-748001: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change

**Explanation**  A cluster control link has changed in the MIO, a cluster group has been removed in the MIO, or a blade module has been removed in the MIO configuration.

- **slot_number** — The blade slot ID within the chassis
- **chassis_number** — The chassis ID, which is unique for each chassis

**Recommended Action**  None required.

**748002**

**Error Message**  %FTD-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled
Explanation Configurations are missing or incomplete in the MIO (for example, a cluster group is not configured, or a cluster control link is not configured).

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Go to the MIO console and configure the cluster service type, add the module to the service type, and define the cluster control link accordingly.

748003 Error Message %FTD-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure

Explanation The blade cannot talk to the MIO, so it relies on the MIO to detect this communication problem and de-bundle the data ports. If data ports are de-bundled, the Firepower Threat Defense device will be kicked out by an interface health check.

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO card is up or if the communication between the MIO and the blade is still up.

748004 Error Message %FTD-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery

Explanation The MIO blade health check has recovered, and the Firepower Threat Defense device tries to rejoin the cluster.

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO card is up or if the communication between the MIO and the blade is still up.

748005 Error Message %FTD-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number; clustering is disabled

Explanation The MIO failed to bundle the ports for itself.

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

748006 Error Message %FTD-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure
Explanation The MIO failed to bundle ports for a blade, so the blade has been kicked out.

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

---

Error Message %FTD-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number; traffic may be black holed

Explanation The MIO failed to de-bundle the ports.

- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

---

Error Message %FTD-6-748008: [CPU load percentage | memory load percentage] of module slot_number in chassis chassis_number (member-name) exceeds overflow protection threshold [CPU percentage | memory percentage]. System may be oversubscribed on member failure.

Explanation The CPU load has exceeded \((N-1)/N\), where \(N\) is the total number of active cluster members, or the memory load has exceeded \((100 - x) \times (N - 1)/N + x\), where \(N\) is the number of cluster members, and \(x\) is the baseline memory usage of the last joining member.

- percentage — The CPU load or memory load percentile data
- slot_number — The blade slot ID within the chassis
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

---

Error Message %FTD-6-748009: [CPU load percentage | memory load percentage] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage]. System may be oversubscribed on chassis failure.

Explanation The chassis traffic load exceeded a certain threshold.

- percentage — The CPU load or memory load percentile data
- chassis_number — The chassis ID, which is unique for each chassis

Recommended Action Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

---

Error Message %FTD-4-748011: Mismatched resource profile size with Master. Master: cores number CPU cores / RAM size MB RAM, Mine: cores number CPU cores / RAM size MB RAM
**Explanation** When the unit that is joining into cluster has different resource profile size compared to Master, this syslog appears on the joining unit.

**Example**

```
%FTD-4-748011: Mismatched resource profile size with Master. Master: 6 CPU cores / 14426 MB RAM, Mine: 8 CPU cores 19261 MB RAM.
```

**Recommended Action** None required.

---

**Error Message** `%FTD-4-748012: Mismatched module type with Master. Master: PID, MINE: PID`

**Explanation** When the unit that is joining into cluster has different module type compared to the Master, this syslog appears on the joining unit.

**Example**

```
```

**Recommended Action** None required.

---

**Error Message** `%FTD-3-748100: <application_name> application status is changed from <status> to <status>.
```

**Explanation** Detect the application status change from one state to another. Application status change will trigger application health check mechanism.

- **application name**—snort or disk_full
- **status**—init, up, down

**Recommended Action** Verify the status of the application.

---

**Error Message** `%FTD-3-748101: Peer unit <unit_id> reported its <application_name> application status is <status>.
```

**Explanation** Peer unit reported application status change that will trigger application health check mechanism.

- **unit id**—the unit id
- **application name**—snort or disk_full
- **status**—init, up, down

**Recommended Action** Verify the status of the application.
748102

**Error Message** %FTD-3-748102: Master unit &lt;unit_id&gt; is quitting due to &lt;application_name&gt;
Application health check failure, and master's application state is &lt;status&gt;.

**Explanation** Application health check detects that the Master unit is not healthy. The Master unit will leave the cluster group.

- **unit id**—the unit id
- **application name**—snort or disk_full
- **status**—init, up, down

**Recommended Action** Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

748103

**Error Message** %FTD-3-748103: Asking slave unit &lt;unit_id&gt; to quit due to &lt;application_name&gt;
Application health check failure, and slave's application state is &lt;status&gt;.

**Explanation** Application health check detects that the Slave unit is not healthy. Master unit will evict the slave node.

- **unit id**—the unit id
- **application name**—snort or disk_full
- **status**—init, up, down

**Recommended Action** Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

748201

**Error Message** %FTD-4-748201: &lt;Application name&gt; application on module &lt;module id&gt; in chassis &lt;chassis id&gt; is &lt;status&gt;.

**Explanation** Status of the application in the service chain gets changed.

- **status**—up, down

**Recommended Action** Verify the status of the application in the service chain.

748202

**Error Message** %FTD-3-748202: Module &lt;module_id&gt; in chassis &lt;chassis id&gt; is leaving the cluster due to &lt;application name&gt; application failure.

**Explanation** Unit will be kicked out of cluster if the application such as vDP, fails.

**Recommended Action** Verify the status of the application in the service chain.
**748203**

**Error Message** %FTD-5-748203: Module <module_id> in chassis <chassis id> is re-joining the cluster due to a service chain application recovery.

**Explanation** Unit automatically rejoins the cluster if the service chain application such as vDP, recovers.

**Recommended Action** Verify the status of the application in the service chain.

---

**750001**

**Error Message** %FTD-5-750001: Local: local IP : local port Remote: remote IP : remote port
Username: username
Received request to request an IPsec tunnel;
local traffic selector = local selectors: range, protocol, port range;
remote traffic selector = remote selectors: range, protocol, port range

**Explanation** A request is being made for an operation on the IPsec tunnel such as a rekey, a request to establish a connection, and so on.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
- **remote IP:remote port** — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- **username** — Username of the requester for remote access, if known, or the tunnel group
- **local selectors** — Locally configured traffic selectors or proxies that are being used for this IPsec tunnel
- **remote selectors** — Remote peers requested traffic selectors or proxies for this IPsec tunnel

**Recommended Action** None required.

---

**750002**

**Error Message** %FTD-5-750002: Local: local IP : local port Remote: remote IP : remote port
Username: username
Received a IKE_INIT_SA request

**Explanation** An incoming tunnel or SA initiation request (IKE_INIT_SA request) has been received.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
- **remote IP:remote port** — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- **username** — Username of the requester for remote access, if known, or the tunnel group

**Recommended Action** None required.

---

**750003**

**Error Message** %FTD-4-750003: Local: local IP:local port Remote: remote IP:remote port
Username: username
Negotiation aborted due to ERROR: error

**Explanation** The negotiation of an SA was aborted because of the provided error reason.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
- **remote IP:remote port** — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- **username** — Username of the requester for remote access, if known yet
- **error** — Error reason for aborting the negotiation. Errors include the following:
  - Failed to send data on the network
  - Asynchronous request queued
  - Failed to enqueue packet
  - A supplied parameter is incorrect
  - Failed to allocate memory
  - Failed the cookie negotiation
  - Failed to find a matching policy
  - Failed to locate an item in the database
  - Failed to initialize the policy database
  - Failed to insert a policy into the database
  - The peer's proposal is invalid
  - Failed to compute the DH value
  - Failed to construct a NONCE
  - An expected payload is missing from the packet
  - Failed to compute the SKEYSEED
  - Failed to create child SA keys
  - The peer's KE payload contained the wrong DH group
  - Received invalid KE notify, yet we've tried all configured DH groups
  - Failed to compute a hash value
  - Failed to authenticate the IKE SA
  - Failed to compute or verify a signature
  - Failed to validate the certificate
  - The certificate has been revoked and is consequently invalid
  - Failed to build or process a certificate request
  - We requested a certificate, but the peer supplied none
  - While sending the certificate chain, peer did not send its certificate as the first in the chain
  - Detected an unsupported ID type
  - Failed to construct an encrypted payload
  - Failed to decrypt an encrypted payload
  - Detected an invalid value in the packet
  - The initiator bit is asserted in packet from original responder
- The initiator bit isn't asserted in packet from original initiator
- The message response bit is asserted in a packet from the exchange initiator
- The message response bit isn't asserted in a packet from the exchange responder
- Detected an invalid IKE SPI
- Packet is a retransmission
- Detected an invalid protocol ID
- Detected unsupported critical payload
- Detected an invalid traffic selector type
- Failed to create new SA
- Failed to delete SA
- Failed to add new SA into session DB
- Failed to add session to PSH
- Failed to delete session from osal
- Failed to delete a session from the database
- Failed to add request to SA
- Throttling request queue exceeds reasonable limit, increase the window size on peer
- Received an IKE msg id outside supported window
- Detected unsupported version number
- Received no proposal chosen notify
- Detected an error notify payload
- Detected NAT-d hash doesn't match
- Initialize sadb failed
- Initialize session db failed
- Failed to get PSH
- Negotiation context locked currently in use
- Negotiation context was not freed!
- Invalid data state found
- Failed to open PKI session
- Failed to insert public keys
- No certificate found
- Unsupported cert encoding found or Peer requested HTTP URL but never sent HTTP_LOOKUP_SUPPORTED Notification
- Sending BUNDLE URL is not supported at least for now. However, processing a BUNDLE URL is supported
- Local certificate has expired
- Failed to construct State Machine
- Error encountered while navigating State Machine
- SM Validation failed
- Could not find neg context
- Failed to add work request to SM Q
- Nonce payload is missing
- Traffic selector payload is missing
- Unsupported DH group
- Expected keypair is unavailable
- Packet isn't encrypted
- Packet is missing KE payload
- Packet is missing SA payload
- Invalid SA
- Invalid negotiation context
- Remote or local ID isn't defined
- Invalid connection id
- Unsupported auth method
- Ipsec policy not found
- Failed to initialize the event priority queue
- Failed to enqueue an item to a list
- Failed to remove an item from list
- Data in the event priority queue is NULL or corrupt
- No local IKE policy found
- Can't delete IKE SA due to in-progress task
- Expected Cookie Notify not received
- Failed to generate auth data: My auth info missing
- Failed to generate auth data: Failed to sign data
- Failed to generate auth data: Signature operation successful but unable to locate generated auth material
- Failed to receive the AUTH msg before the timer expired
- Maximum number of retransmissions reached
- Initial exchange failed
- Auth exchange failed
- Create child exchange failed
- Platform errors
- Failed to log a message
- Unwanted debug level turned on
- There are additional TS possible
- A single pairs of addresses is required
- Invalid session
- There was no IPSEC policy found for received TS
- Cannot remove request from window
- There was no proposal found in configured policy
- Nat-t test failure
- No pskey found
- Invalid compression algorithm
- Failed to get profile name from platform service handle
- Failed to find profile
- Initiator failed to match profile sent by IPSEC with profile found by peer id or certificate
- Failed to get peer id from platform service handle
- The transform attribute is invalid
- Extensible Authentication Protocol failed
- Authenticator sent NULL EAP message
- The config attribute is invalid
- Failed to calculate packet hash
- The AAA context is deleted
- Cannot alloc AAA ID
- Cannot alloc AAA request
- Cannot init AAA request
- The Authen list is not configured
- Fail to send AAA request
- Fail to alloc IP addr
- Invalid message context
- Key Auth memory failure
- EAP method does not generate MSK
- Failed to register new SA with platform
- Failed to async process session register, error: %d
- Failed to insert SA due to ipsec rekey collision
- Failed while handling a ipsec rekey collision
- Failed to accept rekey on SA that caused a rekey collision
- Failed to start timer to ensure IPsec collision SA SPI %s/%s will be deleted by the peer
- Error/Debug codes and strings are not matched
- Failed to initialize SA lifetime
- Failed to find rekey SA
- Failed to generate DH shared secret
- Failed to retrieve issuer public key hash list
- Failed to build certificate payload
- Unable to initialize the timer
- Failed to generate DH shared secret
- Failed to initialized authorization request
- Incorrect author record received from AAA
- Failed to fetch the keys from AAA
- Failed to add attribute to AAA request
- Failed to send tunnel password request to AAA
- Failed to allocate AAA context
- Insertion to policy AVL tree failed
- Deletion from policy AVL tree failed
- No Matching node found in policy AVL tree
- No Matching policy found
- No Matching proposal found
- Proposal is incomplete to be attached to the policy
- Proposal is in use
- Peer authentication method configured is mismatching with the method proposed by peer
- Failed to find the session in osal
- Failed to allocate event
- Failed to create accounting record
- Accounting not required
- Accounting not started for this session
- NAT-T disabled via cli
- Negotiating limit reached, deny SA request
- SA is already in negotiation, hence not negotiating again
- AAA group authorization failed
- AAA user authorization failed
- %% Dropping received fragment, as fragmentation is not negotiated for this SA!
- Maximum number of received fragments reached for the SA
- Number of fragments exceeds maximum allowed
- Assembled packet length %d is greater than maximum ikev2 packet size %d
- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet
- Received fragment is not valid, hence being dropped
- AAA group authorization failed
- AAA user authorization failed
- AAA author not configured in IKEv2 profile
- Failed to extract the skeid
- Failed to send a failover msg to the standby unit
- Detected unsupported failover version
- Request was received but failover is not enabled
- Received an active unit request but the negotiated role is %s
- Received a standby unit request but the negotiated role is %s
- Invalid IP Version
- GDOI is not yet supported in IKEv2
- Failed to allocate PSH from platform
- Redirect the session to another gateway
- Redirect check failed
- Accept the session on this gateway after Redirect check
- Detected unsupported Redirect gateway ID type
- Redirect accepted, initiate new request
- Redirect accepted, clean-up IKEv2 SA, platform will initiate new request
- SA got redirected, it should not do any CREATE_CHILD_SA exchange
- DH public key computation failed
- DH secret computation failed
- IN-NEG IKEv2 Rekey SA got deleted
- Number of cert req exceeds the reasonable limit (%d)
- The negotiation context has been freed
- Assembled packet length %d is greater than maximum ikev2 packet size %d
- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet
- AAA author not configured in IKEv2 profile
- Assembled packet is not valid, hence being dropped
- Invalid VCID context

**Recommended Action** Review the syslog and follow the flow of the logs to determine if this syslog is the final in the exchange and if it is the cause of a potential failure or a transient error that was renegotiated through. For example, a peer may suggest a DH group via the KE payload that is not configured that causes an initial request to fail, but the correct DH group is communicated so that the peer can come back with the correct group in a new request.

### 750004

**Error Message** %FTD-5-750004: Local: local IP: local port Remote: remote IP: remote port
Username: username Sending COOKIE challenge to throttle possible DoS

**Explanation** An incoming connection request was challenged with a cookie based on the cookie challenge thresholds that are configured to prevent a possible DoS attack.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
- **remote IP:remote port** — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- **username** — Username of the requester for remote access, if known yet

**Recommended Action** None required.

### 750005

**Error Message** %FTD-5-750005: Local: local IP: local port Remote: remote IP: remote port
Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI

**Explanation** A rekey collision was detected (both peers trying to initiate a rekey at the same time), and it was resolved by keeping the one initiated by this Firepower Threat Defense device because it had the lowest nonce. This action caused the indicated SA referenced by the SPI to be deleted.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
- **remote IP:remote port** — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- **username** — Username of the requester for remote access, if known yet
- **SPI** — SPI handle of the SA being deleted by resolving the rekey collision that was detected

**Recommended Action** None required.

### 750006

**Error Message** %FTD-5-750006: Local: local IP: local port Remote: remote IP: remote port
Username: username SA UP. Reason: reason

**Explanation** An SA came up for the given reason, such as for a newly established connection or a rekey.

- **local IP:local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
• remote IP:remote port — Remote IP address for this request. Peer IP address and port number that the connection is coming from
• username — Username of the requester for remote access, if known yet
• reason — Reason that the SA came into the UP state

**Recommended Action** None required.

### 750007

**Error Message** %FTD-5-750007: Local: local IP: local port Remote: remote IP: remote port
Username: username SA DOWN. Reason: reason

**Explanation** An SA was torn down or deleted for the given reason, such as a request by the peer, operator request (via an administrator action), rekey, and so on.

• local IP:local port — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
• remote IP:remote port — Remote IP address for this request. Peer IP address and port number that the connection is coming from
• username — Username of the requester for remote access, if known yet
• reason — Reason that the SA came into the DOWN state

**Recommended Action** None required.

### 750008

**Error Message** %FTD-5-750008: Local: local IP: local port Remote: remote IP: remote port
Username: username SA rejected due to system resource low

**Explanation** An SA request was rejected to alleviate a low system resource condition.

• local IP:local port — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
• remote IP:remote port — Remote IP address for this request. Peer IP address and port number that the connection is coming from
• username — Username of the requester for remote access, if known yet

**Recommended Action** Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

### 750009

**Error Message** %FTD-5-750009: Local: local IP: local port Remote: remote IP: remote port
Username: username SA rejected due to CAC limit reached: Rejection reason: reason

**Explanation** A Connection Admission Control (CAC) limiting threshold was reached, which caused the SA request to be rejected.

• local IP:local port — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
• remote IP:remote port — Remote IP address for this request. Peer IP address and port number that the connection is coming from
• username — Username of the requester for remote access, if known yet
• **reason** — Reason that the SA was rejected

**Recommended Action** Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

---

**Syslog Messages 722001 to 776254**

### 750010

**Error Message** %FTD-5-750010: Local: local-ip Remote: remote-ip Username: username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance

- **local-ip** — Local peer IP address
- **remote-ip** — Remote peer IP address
- **username** — Username of the requester for remote access or tunnel group name for L2L, if known yet
- **threshold** — Queue depth threshold of the local throttle-request queue reached
- **peer** — Remote peer IP address

**Explanation** The Firepower Threat Defense device overflowed its throttle request queue to the specified peer, indicating that the peer is slow. The throttle request queue holds requests destined for the peer, which cannot be sent immediately because the maximum number of requests allowed to be in-flight based on the IKEv2 window size were already in-flight. As in-flight requests are completed, requests are pulled off of the throttle request queue and sent to the peer. If the peer is not processing these requests quickly, the throttle queue backs up.

**Recommended Action** If possible, increase the IKEv2 window size on the remote peer to allow more concurrent requests to be in-flight, which may improve performance.

---

**Note** The Firepower Threat Defense device does not currently support an increased IKEv2 window size setting.

### 750011

**Error Message** %FTD-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).

**Explanation** The tunnel was rejected because the selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

**Recommended Action** Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.

### 750012

**Error Message** %FTD-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).

**Explanation** The selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

**Recommended Action** Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.
Error Message %FTD-5-750013: IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>. Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>

Explanation The new mobike feature allows peer IP to be changed without tearing down the tunnel. For example, a mobile device (smartphone) acquires new IP after connecting to a different network. The following list describes the message values:

- **ip** — Specifies the previous, the new local, and remote IP addresses
- **port** — Specifies the previous, the new local, and remote port information
- **SPI** — Indicates the Initiator and Responder SPI
- **iSPI** — Specifies the Initiator SPI
- **rSPI** — Specifies the Responder SPI

Recommended Action Contact the Development engineers.

---

Error Message %FTD-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group
Failed to complete Diffie-Hellman operation. Error: error

Explanation A failure to complete a Diffie-Hellman operation occurred, as indicated by the error.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **error** — The error string that indicates the specific error

Recommended Action A low memory issue or other internal error that should be resolved has occurred. If it persists, use the memory tracking tool to isolate the issue.

---

Error Message %FTD-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group
No preshared key or trustpoint configured for self in tunnel group group

Explanation The Firepower Threat Defense device was unable to find any type of authentication information in the tunnel group that it could use to authenticate itself to the peer.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **group** — The name of the tunnel group

Recommended Action Check the tunnel group configuration, and configure a preshared key or certificate for self-authentication in the indicated tunnel group.
751003

**Error Message** %FTD-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group

*Need to send a DPD message to peer*

**Explanation** Dead peer detection needs to be performed for the specified peer to determine if it is still alive. The Firepower Threat Defense device may have terminated a connection to the peer.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt

**Recommended Action** None required.

751004

**Error Message** %FTD-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group

*No remote authentication method configured for peer in tunnel group group*

**Explanation** A method to authenticate the remote peer was not found in the configuration to allow the connection.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt
- *group* — The name of the tunnel group

**Recommended Action** Check the configuration to make sure that a valid remote peer authentication setting is present.

751005

**Error Message** %FTD-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group

*AnyConnect client reconnect authentication failed. Session ID: sessionID, Error: error*

**Explanation** A failure occurred during an AnyConnect client reconnection attempt using the session token.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt
- *sessionID* — The session ID used to try to reconnect
- *error* — The error string to indicate the specific error that occurred during the reconnection attempt

**Recommended Action** Take action according to the error specified, if necessary. The error may indicate that a session was removed instead of remaining in resume state because a client disconnect was detected or sessions were cleared on the Firepower Threat Defense device. If necessary, also compare this message to the event logs on the Anyconnect client.

751006

**Error Message** %FTD-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group

*Certificate authentication failed. Error: error*
Explanation  A failure related to certificate authentication occurred.

- **localIP:port** —The local IP address and port number
- **remoteIP:port** —The remote IP address and port number
- **username/group** —The username or group associated with this connection attempt
- **error** —The error string to indicate the specific certificate authentication failure

**Recommended Action**  Take action according to the error specified, if necessary. Check the certificate trustpoint configuration and make sure that the necessary CA certificate exists to be able to correctly verify client certificate chains. Use the **debug crypto ca** commands to isolate the failure.

---

**751007**

**Error Message**  %FTD-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group
Configured attribute not supported for IKEv2. Attribute: attribute

**Explanation**  A configured attribute could not be applied to the IKE version 2 connection because it is not supported for IKE version 2 connections.

- **localIP:port** —The local IP address and port number
- **remoteIP:port** —The remote IP address and port number
- **username/group** —The username or group associated with this connection attempt
- **attribute** —The attribute that is configured to be applied

**Recommended Action**  None required, To eliminate this message from being generated, you can remove the IKE version 2 configuration setting.

---

**751008**

**Error Message**  %FTD-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group
Group=group, Tunnel rejected: IKEv2 not enabled in group policy

**Explanation**  IKE version 2 is not allowed based on the enabled protocols for the indicated group to which a connection attempt was mapped, and the connection was rejected.

- **localIP:port** —The local IP address and port number
- **remoteIP:port** —The remote IP address and port number
- **username/group** —The username or group associated with this connection attempt
- **group** —The tunnel group used for connection

**Recommended Action**  Check the group policy VPN tunnel protocol setting and enable IKE version 2, if desired.

---

**751009**

**Error Message**  %FTD-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group
Unable to find tunnel group for peer.

**Explanation**  A tunnel group could not be found for the peer.

- **localIP:port** —The local IP address and port number
- **remoteIP:port** —The remote IP address and port number
- **username/group** —The username or group associated with this connection attempt
**Recommended Action** Check the configuration and tunnel group mapping rules, then configure them to allow the peer to land on a configured group.

---

**751010**

**Error Message** %FTD-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group

Unable to determine self-authentication method. No crypto map setting or tunnel group found.

**Explanation** A method for authenticating the Firepower Threat Defense device to the peer could not be found in either the tunnel group or crypto map.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt

**Recommended Action** Check the configuration, and configure a self-authentication method in the crypto map for the initiator L2L or in the applicable tunnel group.

---

**751011**

**Error Message** %FTD-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group

Failed user authentication. Error: error

**Explanation** A failure occurred during user authentication within EAP for an IKE version 2 remote access connection.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt
- *error* — The error string that indicates the specific error

**Recommended Action** Make sure that the correct authentication credentials were provided and debug further to determine the exact cause of failure, if necessary.

---

**751012**

**Error Message** %FTD-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group

Failure occurred during Configuration Mode processing. Error: error

**Explanation** A failure occurred during configuration mode processing while settings were being applied to the connection.

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt
- *error* — The error string that indicates the specific error

**Recommended Action** Take action based on the indicated error. Use the `debug crypto ikev2` commands to determine the cause of the failure, or debug the indicated subsystem that is specified by the error, if necessary.
751013

**Error Message** %FTD-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group

Failed to process Configuration Payload request for attribute attribute ID . Error: error

**Explanation** The Configuration Payload request failed to process and generate a Configuration Payload response for an attribute that was requested by the peer.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **attribute ID** — The attribute ID on which the failure occurred
- **error** — The error string that indicates the specific error

**Recommended Action** A memory error, configuration error, or another type of error has occurred. Use the `debug crypto ikev2` commands to help isolate the cause of the failure.

751014

**Error Message** %FTD-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group

Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error

**Explanation** A warning occurred while processing a CP request to generate a CP response for a requested attribute.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **attribute ID** — The attribute ID on which the failure occurred
- **error** — The error string that indicates the specific error

**Recommended Action** Take action based on the attribute indicated in the warning and the indicated warning message. For example, a newer client is being used with an older Firepower Threat Defense image, which does not understand a new attribute that has been added to the client. An upgrade of the Firepower Threat Defense image may be necessary to allow the attribute to be processed.

751015

**Error Message** %FTD-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group

SA request rejected by CAC. Reason: reason

**Explanation** The connection was rejected by the call admission control to protect the Firepower Threat Defense device based on configured thresholds or conditions indicated by the reason listed.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **reason** — The reason that the SA request was rejected

**Recommended Action** Check the reason and resolve the condition if a new connection should have been accepted or change the configured thresholds.
**751016**

**Error Message** %FTD-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!

**Explanation** The peer may be configured for originate-only connections based on the received outer and inner IP addresses for the tunnel.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt

**Recommended Action** Check the L2L peer configuration.

---

**751017**

**Error Message** %FTD-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group Configuration Error error description

**Explanation** An error in the configuration that prevented the connection has been detected.

- **localIP:port** — The local IP address and port number
- **remoteIP:port** — The remote IP address and port number
- **username/group** — The username or group associated with this connection attempt
- **error description** — A brief description of the configuration error

**Recommended Action** Correct the configuration based on the indicated error.

---

**751018**

**Error Message** %FTD-3-751018: Terminating the VPN connection attempt from attempted group . Reason: This connection is group locked to locked group .

**Explanation** The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- **attempted group** — The tunnel group over which the connection came in
- **locked group** — The tunnel group that the connection is locked or restricted to

**Recommended Action** Check the group-lock value in the group policy or the user attributes.

---

**751019**

**Error Message** %FTD-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.

**Explanation** A session creation failed because the maximum license limit was exceeded, which caused a failure to either initiate or respond to a tunnel request.

- **LocalAddr** — Local address for this connection attempt
- **RemoteAddr** — Remote peer address for this connection attempt
- **username** — Username for the peer attempting the connection
- **licenseType** — License type that was exceeded (other VPN or AnyConnect Premium/Essentials)
• limit — Number of licenses allowed and was exceeded

**Recommended Action** Make sure that enough licenses are available for all allowed users and/or obtain more licenses to allow the rejected connections. For multiple context mode, allow more licenses for the context that reported the failure, if necessary.

---

**751020**

**Error Message** %FTD-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.

**Explanation** An IKEv2 remote access tunnel could not be created because the AnyConnect Premium license was applied but explicitly disabled with the `anyconnect-essentials` command in the webvpn configuration mode.

**Recommended Action** Make sure that an AnyConnect Premium license is installed on the Firepower Threat Defense device is configured in the remote access IKEv2 policies or IPsec proposals.

---

**751021**

**Error Message** %FTD-4-751021: Local:variable 1:variable 2 Remote:variable 3:variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest AnyConnect Client.

**Explanation** An out-of-date AnyConnect client tried to connect to an Firepower Threat Defense device that has IKEv2 with AES-GCM encryption policy configured.

• variable 1 — Local IP address
• variable 2 — Local port
• variable 3 — Remote client IP address
• variable 4 — Remote client port
• variable 5 — Username of the AnyConnect client (may be unknown because this occurs before the user enters a username)
• variable 6 — Connection protocol type (IKEv1, IKEv2)
• variable 7 — Combined mode encryption type (AES-GCM, AES-GCM 256)

**Recommended Action** Upgrade the AnyConnect client to the latest version to use IKEv2 with AES-GCM encryption.

---

**751022**


**Explanation** The Firepower Threat Defense device was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Firepower Threat Defense device. This is most likely a misconfiguration.

• local-ip — Local peer IP address
• remote-ip — Remote peer IP address
• **username** — Username of the requester for remote access, if known yet
• **rem-ts-start** — Remote traffic selector start address
• **rem-ts-end** — Remote traffic selector end address
• **rem-ts.startport** — Remote traffic selector start port
• **rem-ts.endport** — Remote traffic selector end port
• **rem-ts.protocol** — Remote traffic selector protocol
• **local-ts-start** — Local traffic selector start address
• **local-ts-end** — Local traffic selector end address
• **local-ts.startport** — Local traffic selector start port
• **local-ts.endport** — Local traffic selector end port
• **local-ts.protocol** — Local traffic selector protocol

**Recommended Action** Check the protected network configuration in the crypto ACLs on both sides and make sure that the local network on the initiator is the remote network on the responder and vice-versa. Pay special attention to wildcard masks and host addresses as compared to network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or “red” networks.

---

**751023**

**Error Message** %FTD-6-751023: Local a:p Remote: a:p Username:n Unknown client connection

**Explanation** An unknown non-Cisco IKEv2 client has connected to the Firepower Threat Defense device.

• **n** — The group or username (depending on context)
• **a** — An IP address
• **p** — The port number
• **ua** — The user-agent presented by the client to the Firepower Threat Defense device

**Recommended Action** Upgrade to a Cisco-supported IKEv2 client.

---

**751024**

**Error Message** %FTD-3-751024: Local:ip-addr Remote:ip-addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection

**Explanation** The IPv6 VPN filter has been deprecated and if it is configured instead of a unified filter for IPv6 traffic access control, the connection will be terminated.

**Recommended Action** Configure a unified filter with IPv6 entries to control IPv6 traffic for the user.

---

**751025**


**Explanation** This message displays the assigned IP address information for the AnyConnect IKEv2 connection of the specified user.

• **local IP :local port** — Local IP address for this request. The Firepower Threat Defense IP address and port number used for this connection
• remote IP:remote port — Remote IP address for this request. Peer IP address and port number that the connection is coming from
• username — Username of the requester for remote access, if known yet
• group-policy — The group policy that allowed the user to gain access
• assigned_IPv4_addr — The IPv4 address that is assigned to the client
• assigned_IPv6_addr — The IPv6 address that is assigned to the client

Recommended Action None required.

751026


Explanation The indicated user is attempting to connect with the shown operating system and client version.
• localIP:port — The local IP address and port number
• remoteIP:port — The remote IP address and port number
• username/group — The username or group associated with this connection attempt
• client-os — The operating system reported by the client
• client-name — The client name reported by the client (usually AnyConnect)
• client-version — The client version reported by the client

Recommended Action None required.

751027

Error Message %FTD-4-751027: Local:local IP :local port Remote:peer IP :peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn’t match the negotiated policy in the SA. Packet destination pkt_daddr, port pkt_dest_port, source pkt_saddr, port pkt_src_port, protocol pkt_prot.

Explanation A peer received a packet on an IPsec security association (SA) that did not match the negotiated traffic descriptors for that SA. The peer sent an INVALID_SELECTORS notification containing the SPI and packet data for the offending packet.

• local IP — The Firepower Threat Defense local IP address
• local port — The Firepower Threat Defense local port
• peer IP — Peer IP address
• peer port — Peer port
• username — Username
• spi — SPI of the IPsec SA for the packet
• pkt_daddr — Packet destination IP address
• pkt_dest_port — Packet destination port
• pkt_saddr — Packet source IP address
• pkt_src_port — Packet source port
• pkt_prot — Packet protocol

Recommended Action Copy the error message, the configuration, and any details about the events leading up to this error, then submit them to Cisco TAC.
752001

**Error Message** %FTD-2-752001: Tunnel Manager received invalid parameter to remove record

**Explanation** A failure to remove a record from the tunnel manager that might prevent future tunnels to the same peer from initiating has occurred.

**Recommended Action** Reloading the device will remove the record, but if the error persists or recurs, perform additional debugging of the specific tunnel attempt.

---

752002

**Error Message** %FTD-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag . Map Sequence Number = mapSeq.

**Explanation** An entry to initiate a tunnel was successfully removed.

- *mapTag* — Name of the crypto map for which the initiation entry was removed
- *mapSeq* — Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

---

752003

**Error Message** %FTD-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag . Map Sequence Number = mapSeq.

**Explanation** An attempt is being made to initiate an IKEv2 tunnel that was based on the crypto map indicated.

- *mapTag* — Name of the crypto map for which the initiation entry was removed
- *mapSeq* — Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

---

752004

**Error Message** %FTD-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag . Map Sequence Number = mapSeq.

**Explanation** An attempt is being made to initiate an IKEv1 tunnel that was based on the crypto map indicated.

- *mapTag* — Name of the crypto map for which the initiation entry was removed
- *mapSeq* — Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

---

752005

**Error Message** %FTD-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag . Map Sequence Number = mapSeq.

**Explanation** An attempt to dispatch a tunnel initiation attempt failed because of an internal error, such as a memory allocation failure.

- *mapTag* — Name of the crypto map for which the initiation entry was removed
• mapSeq — Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Use the memory tracking tools and additional debugging to isolate the issue.

### 752006

**Error Message** `%FTD-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag . Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port .

**Explanation** An attempt to dispatch a tunnel initiation attempt failed because of a configuration error of the indicated crypto map or associated tunnel group.

- *Tag* — Name of the crypto map for which the initiation entry was removed
- *num* — Sequence number of the crypto map for which the initiation entry was removed
- *address* — The source IP address or destination IP address
- *port* — The source port number or destination port number

**Recommended Action** Check the configuration of the tunnel group and crypto map indicated to make sure that it is complete.

### 752007

**Error Message** `%FTD-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag . Map Sequence Number = mapSeq

**Explanation** An attempt was made to re-add an existing entry into the tunnel manager.

- *mapTag* — Name of the crypto map for which the initiation entry was removed
- *mapSeq* — Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** If the issue persists, make sure that the configuration of the peer will allow the tunnel, and debug further to make sure that the tunnel manager entries are being added and removed correctly during tunnel initiation and successful or failed initiation attempts. Debug IKE version 2 or IKE version 1 connections further, because they may still be in the process of creating the tunnel.

### 752008

**Error Message** `%FTD-7-752008: Duplicate entry already in Tunnel Manager

**Explanation** A duplicate request to initiate a tunnel was made, and the tunnel manager is already attempting to initiate the tunnel.

**Recommended Action** None required. If the issue persists, either IKE version 1 or IKE version 2 may have attempted a tunnel initiation and not have timed out yet. Debug further using the applicable commands to make sure that the tunnel manager entry is removed after successful or failed initiation attempts.

### 752009

 `%FTD-4-752009: IKEv2 Doesn’t support Multiple Peers

**Explanation** An attempt to initiate a tunnel with IKE version 2 failed because the crypto map is configured with multiple peers, which is not supported for IKE version 2. Only IKE version 1 supports multiple peers.
**Recommended Action** Check the configuration to make sure that multiple peers are not expected for IKE version 2 site-to-site initiation.

**752010**

**Error Message** %FTD-4-752010: IKEv2 Doesn't have a proposal specified

**Explanation** No IPsec proposal was found to be able to initiate an IKE version 2 tunnel.

**Recommended Action** Check the configuration, then configure an IKE version 2 proposal that can be used to initiate the tunnel, if necessary.

**752011**

**Error Message** %FTD-4-752011: IKEv1 Doesn't have a transform set specified

**Explanation** No IKE version 1 transform set was found to be able to initiate an IKE version 2 tunnel.

**Recommended Action** Check the configuration, then configure an IKE version 2 transform set that can be used to initiate the tunnel, if necessary.

**752012**

**Error Message** %FTD-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .

**Explanation** The indicated protocol failed to initiate a tunnel using the configured crypto map.

- *protocol*— IKE version number 1 or 2 for IKEv1 or IKEv2
- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, then debug further within the indicated protocol to determine the cause of the failed tunnel attempt.

**752013**

**Error Message** %FTD-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .

**Explanation** The tunnel manager is attempting to initiate the tunnel again after it failed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

**752014**

**Error Message** %FTD-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .
Explanation The tunnel manager is falling back and attempting to initiate the tunnel using IKE version 1 after the tunnel failed.

- mapTag — Name of the crypto map for which the initiation entry was removed
- mapSeq — Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

Error Message %FTD-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq.

Explanation An attempt to bring up an L2L tunnel to a peer failed after trying with all configured protocols.

- mapTag — Name of the crypto map for which the initiation entry was removed
- mapSeq — Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, and make sure that the crypto maps are correctly configured. Debug the individual protocols to isolate the cause of the failure.

Error Message %FTD-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq.

Explanation The indicated protocol (IKE version 1 or IKE version 2) successfully created an L2L tunnel.

- protocol — IKE version number 1 or 2 for IKEv1 or IKEv2
- mapTag — Name of the crypto map for which the initiation entry was removed
- mapSeq — Sequence number of the crypto map for which the initiation entry was removed

Recommended Action None required.

Error Message %FTD-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name , sequence number number . Unsupported configuration.

Explanation The Firepower Threat Defense device uses IKEv1 to initiate the connection because IKEv2 does not support the backup L2L feature.

Recommended Action None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

Error Message %FTD-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>
Explanation This syslog is generated when an IKEv2 packet is received when the cluster is operating in Distributed VPN clustering mode and fails early consistency and/or error checks performed on it in the datapath.

- `<IP>`—source IP address from where the packet was received
- `<port>`—source port from where the packet was received
- `<reason>`—Reason why the packet is considered invalid. This value could be *Corrupted SPI detected* or *Expired SPI received*.

**Recommended Action** None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

### 767001

**Error Message** `%FTD-6-767001: Inspect-name : Dropping an unsupported IPv6/IP46/IP64 packet from interface :IP Addr to interface :IP Addr (fail-close)`

**Explanation** A fail-close option was set for a service policy, and a particular inspect received an IPv6, IP64, or IP46 packet. Based on the fail-close option setting, this syslog message is generated and the packet is dropped.

**Recommended Action** None required.

### 768001

**Error Message** `%FTD-3-768001: QUOTA: resource utilization is high: requested req , current curr , warning level level`

**Explanation** A system resource allocation level has reached its warning threshold. In the case of a management session, the resource is simultaneous administrative sessions.

- `resource`— The name of the system resource; in this case, it is a management session.
- `req` —The number requested; for a management session, it is always 1.
- `curr` —The current number allocated; equals `level` for a management session
- `level` —The warning threshold, which is 90 percent of the configured limit

**Recommended Action** None required.

### 768002

**Error Message** `%FTD-3-768002: QUOTA: resource quota exceeded: requested req , current curr , limit limit`

**Explanation** A request for a system resource would have exceeded its configured limit and was denied. In the case of a management session, the maximum number of simultaneous administrative sessions on the system has been reached.

- `resource`— The name of the system resource; in this case, it is a management session.
- `req` —The number requested; for a management session, it is always 1.
- `curr` —The current number allocated; equals `level` for a management session
- `limit` —The configured resource limit
Recommended Action None required.

768003

Error Message %FTD-3-768003: QUOTA: management session quota exceeded for user user name: current 3, user limit 3
Explanation The current management session exceeded the configured limits for the user.
- **current** — The current number allocated for management session for the user
- **limit** — The configured management session limit. The default value being 15.
Recommended Action None required.

768004

Error Message %FTD-3-768004: QUOTA: management session quota exceeded for ssh/telnet/http protocol: current 2, protocol limit 2
Explanation The maximum number of management sessions for the protocol - ssh, telnet, or http exceeded the configured limit.
- **current** — The current number allocated for a management session
- **limit** — The configured resource limit per protocol. The default values being 5.
Recommended Action None required.

769001

Error Message %FTD-5-769001: UPDATE: ASA image src was added to system boot list
Explanation The system image has been updated. The name of a file previously downloaded onto the system has been added to the system boot list.
- **src** — The name or URL of the source image file
Recommended Action None required.

769002

Error Message %FTD-5-769002: UPDATE: ASA image src was copied to dest
Explanation The system image has been updated. An image file has been copied onto the system.
- **src** — The name or URL of the source image file
- **dest** — The name of the destination image file
Recommended Action None required.

769003

Error Message %FTD-5-769003: UPDATE: ASA image src was renamed to dest
Explanation The system image has been updated. An existing image file has been renamed to an image file name in the system boot list.

- **src**— The name or URL of the source image file
- **dest**— The name of the destination image file

**Recommended Action** None required.

### 769004

**Error Message** %FTD-2-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason

**Explanation** The image failed verification from either the copy command or verify command.

- **src_file** — The file name or URL of the source image file
- **failure_reason** — The file name of the destination image file

**Recommended Action** Possible failure reasons are: insufficient system memory, no image found in file, checksum failed, signature not found in file, signature invalid, signature algorithm not supported, signature processing issue

### 769005

**Error Message** %FTD-5-769005: UPDATE: ASA image image_name passed image verification.

**Explanation** This is a notification message indicating that the image passed verification.

- **image_name** — The file name of the Firepower Threat Defense image file

**Recommended Action** None Required.

### 769006

**Error Message** %FTD-3-769006: UPDATE: ASA boot system image image_name was not found on disk.

**Explanation** This is an error message indicating that the file configured in the boot system list could not be located on disk.

- **image_name** — The file name of the Firepower Threat Defense image file

**Recommended Action** If the device fails to boot, change the boot system command to point to a valid file or install the missing file to the disk before rebooting the device.

### 769007

**Error Message** %FTD-6-769007: UPDATE: Image version is version_number

**Explanation** This message appears when the device is upgraded.

- **version_number** — The version number of the Firepower Threat Defense image file

**Recommended Action** None required.
769009

**Error Message** %FTD-4-769009: UPDATE: Image booted image_name is different from boot images.

**Explanation** This is an error message appears after upgrading the device indicating that the file configured is different from the existing list of boot images.

- **image_name** — The file name of the Firepower Threat Defense image file

**Recommended Action** None required.

770001

**Error Message** %FTD-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.

**Explanation** The CPU or memory resource allocation for the Firepower Threat Defense virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Firepower Threat Defense virtual machine has been changed from that specified in the software downloaded from Cisco.com.

**Recommended Action** To continue Firepower Threat Defense operation, change the CPU or memory resource allocation of the virtual machine to what was specified with the software downloaded from Cisco.com.

770002

**Error Message** %FTD-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.

**Explanation** The CPU or memory resource allocation for the Firepower Threat Defense virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Firepower Threat Defense virtual machine has been changed from that specified in the software downloaded from Cisco.com. The Firepower Threat Defense device will continue to reboot if the resource allocation is not changed.

**Recommended Action** Change the CPU or memory resource allocation to the virtual machine to what was specified with the software downloaded from Cisco.com.

770003

**Error Message** %FTD-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.

**Explanation** The CPU or memory resource allocation to the Firepower Threat Defense virtual machine is less than the minimum requirement for this platform. If this condition persists, performance will be lower than normal.

**Recommended Action** To continue Firepower Threat Defense operation, change the CPU or memory resource allocation of the virtual machine to what was specified with the software downloaded from Cisco.
**772002**

**Error Message** %FTD-3-772002: PASSWORD: console login warning, user username, cause: password expired

**Explanation** A user logged into the system console with an expired password, which is permitted to avoid system lockout.

- **username**— The name of the user

**Recommended Action** The user should change the login password.

---

**772003**

**Error Message** %FTD-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired

**Explanation** A user logged tried to log into the system with an expired password and was denied access.

- **session**— The session type, which can be SSH or Telnet
- **username**— The name of the user
- **ip**— The IP address of the user

**Recommended Action** If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example, traffic from that IP address can be blocked.

---

**772004**

**Error Message** %FTD-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired

**Explanation** A user logged tried to log into the system with an expired password and was denied access.

- **session**— The session type, which is ASDM
- **username**— The name of the user
- **ip**— The IP address of the user

**Recommended Action** If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example, traffic from that IP address can be blocked.

---

**772005**

**Error Message** %FTD-6-772005: REAUTH: user username passed authentication

**Explanation** The user authenticated successfully after changing the password.

- **username**— The name of the user

**Recommended Action** None required.
772006

**Error Message** %FTD-2-772006: REAUTH: user username failed authentication

**Explanation** The user entered the wrong password while trying to change it. As a result, the password was not changed.

- **username** — The name of the user

**Recommended Action** The user should retry changing the password using the `change-password` command.

---

774001

**Error Message** %FTD-2-774001: POST: unspecified error

**Explanation** The crypto service provider failed the power on self-test.

**Recommended Action** Contact the Cisco TAC.

---

774002

**Error Message** %FTD-2-774002: POST: error err, func func, engine eng, algorithm alg, mode mode, dir dir, key len len

**Explanation** The crypto service provider failed the power on self-test.

- **err** — The failure cause
- **func** — The function
- **eng** — The engine, which can be NPX, Nlite, or software
- **alg** — The algorithm, which can be any of the following: RSA, DSA, DES, 3DES, AES, RC4, MD5, SHA1, SHA256, SHA386, SHA512, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC
- **mode** — The mode, which can be any of the following: none, CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4
- **dir** — Either encryption or decryption
- **len** — The key length in bits

**Recommended Action** Contact the Cisco TAC.

---

776251

**Error Message** %FTD-6-776251: CTS SGT-MAP: Binding binding IP - SGname (SGT) from source name added to binding manager.

**Explanation** Binding from the specified source was added to the binding manager.

- **binding IP** — IPv4 or IPv6 binding address.
- **SGname (SGT)** — Binding SGT information. Has the following format if SGname is available: `SGname (SGT)` and the following format if SGname is unavailable: `SGT`.
- **source name** — Name of the contributing source.

**Recommended Action** None required.
776252

**Error Message** %FTD-5-776252: CTS SGT-MAP: Binding binding IP - SGname (SGT) from source name deleted from binding manager.

**Explanation** Binding from the specified source was deleted from the binding manager.

Binding from the specified source was added to the binding manager.

- **binding IP** — IPv4 or IPv6 binding address.
- **SGname (SGT)** — Binding SGT information. Has the following format if SGname is available: SGname (SGT) and the following format if SGname is unavailable: SGT.
- **source name** — Name of the contributing source.

**Recommended Action** None required.

776253

**Error Message** %FTD-6-776253: CTS SGT-MAP: Binding binding IP - new SGname (SGT) from new source name changed from old sgt: old SGname (SGT) from old source old source name.

**Explanation** A particular IP to SGT binding has changed in the binding manager.

- **binding IP** — IPv4 or IPv6 binding address.
- **new SGname (SGT)** — New binding SGT information. Has the following format if SGname is available: SGname (SGT) and the following format if SGname is unavailable: SGT.
- **new source name** — Name of the new contributing source.
- **old SGname (SGT)** — Old binding SGT information. Has the following format if SGname is available: SGname (SGT) and the following format if SGname is unavailable: SGT.
- **old source name** — Name of the old contributing source.

**Recommended Action** None required.

776254

**Error Message** %FTD-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT) from source name.

**Explanation** The binding manager cannot insert, delete, or update the binding

- **action** — Binding manager operation. Either insert, delete or update.
- **binding IP** — IPv4 or IPv6 binding address.
- **SGname (SGT)** — Binding SGT information. Has the following format if SGname is available: SGname (SGT) and the following format if SGname is unavailable: SGT.
- **source name** — Name of the contributing source.

**Recommended Action** Contact the Cisco TAC for assistance.
This chapter contains the following sections:

- Messages 778001 to 785001, on page 473
- Messages 803001 to 8300006, on page 477

## Messages 778001 to 785001

This section includes messages from 778001 to 785001.

### 778001

**Error Message**  %FTD-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port).

**Explanation** The Firepower Threat Defense device tries to create an inner connection for a VXLAN packet, but the VXLAN packet has an invalid segment ID.

**Recommended Action** None required.

### 778002

**Error Message**  %FTD-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.

**Explanation** A decapsulated ingress VXLAN packet is discarded, because the segment ID in the VXLAN header does not match the segment ID of any VNI interface configured on the Firepower Threat Defense device.

**Recommended Action** None required.

### 778003

**Error Message**  %FTD-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.

**Explanation** The Firepower Threat Defense Fast Path sees a VXLAN packet with an invalid segment ID.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration.
778004

**Error Message** %FTD-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name : (IP-address/port) to ifc-name : (IP-address/port) in FP.

**Explanation** The Firepower Threat Defense VTEP sees a VXLAN packet with an invalid VXLAN header.

**Recommended Action** None required.

778005

**Error Message** %FTD-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.

**Explanation** A VXLAN packet is denied by a Fast Path L2 check.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration. Check to see if the STS table has an entry that matches the dropped packet’s segment ID.

778006

**Error Message** %FTD-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name : (IP-address/port) to ifc-name : (IP-address/port) in FP.

**Explanation** The Firepower Threat Defense VTEP received a VXLAN packet with an invalid UDP checksum value.

**Recommended Action** None required.

778007

**Error Message** %FTD-6-778007: VXLAN: Packet from ifc-name :IP-address/port to IP-address/port was discarded due to invalid NVE peer.

**Explanation** The Firepower Threat Defense VTEP received a VXLAN packet from an IP address that is different from the configured NVE peer.

**Recommended Action** None required.

779001

**Error Message** %FTD-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name :IP-address /port to IP-address /port .

**Explanation** The Firepower Threat Defense device tries to create a connection for a VXLAN packet, but failed to use the STS lookup table to locate the out-tag for the in-tag (segment ID) in the VXLAN packet.

**Recommended Action** None required.
Error Message %FTD-6-779002: STS: STS and NAT locate different egress interface for segment-id, protocol from ifc-name:IP-address/port to IP-address/port

Explanation The Firepower Threat Defense device tries to create a connection for a VXLAN packet, but the STS lookup table and NAT policy locate a different egress interface.

Recommended Action None required.

Error Message %FTD-3-779003: STS: Failed to read tag-switching table - reason

Explanation The Firepower Threat Defense device tried to read the tag-switching table, but failed.

Recommended Action None required.

Error Message %FTD-3-779004: STS: Failed to write tag-switching table - reason

Explanation The Firepower Threat Defense device tried to write to the tag-switching table, but failed.

Recommended Action None required.

Error Message %FTD-3-779005: STS: Failed to parse tag-switching request from http - reason

Explanation The Firepower Threat Defense device tried to parse the HTTP request to see what to do on the tag-switching table, but failed.

Recommended Action None required.

Error Message %FTD-3-779006: STS: Failed to save tag-switching table to flash - reason

Explanation The Firepower Threat Defense device tried to save the tag-switching table to flash memory, but failed.

Recommended Action None required.

Error Message %FTD-3-779007: STS: Failed to replicate tag-switching table to peer - reason

Explanation The Firepower Threat Defense device attempts to replicate the tag-switching table to the failover standby unit or clustering slave units, but failed to do so.

Recommended Action None required.
780001

**Error Message** %FTD-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction.

**Explanation** The rule engine has started compilation for an access group transaction. The description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

780002

**Error Message** %FTD-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction.

**Explanation** The rule engine has finished compilation for a transaction. Taking access group as an example, the description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

780003

**Error Message** %FTD-6-780003: RULE ENGINE: Started compilation for nat transaction - description of the transaction.

**Explanation** The rule engine has started compilation for a NAT transaction. The description of the transaction is the command line input of the `nat` command itself.

**Recommended Action** None required.

780004

**Error Message** %FTD-6-780004: RULE ENGINE: Finished compilation for nat transaction - description of the transaction.

**Explanation** The rule engine has finished compilation for a NAT transaction. The description of the transaction is the command line input of the `nat` command itself.

**Recommended Action** None required.

785001

**Error Message** %FTD-7-785001: Clustering: Ownership for existing flow from `<in_interface>:<src_ip_addr>/<src_port>` to `<out_interface>:<dest_ip_addr>/<dest_port>` moved from unit `<old-owner-unit-id>` at site `<old-site-id>` to `<new-owner-unit-id>` at site `<old-site-id>` due to `<reason>`.

**Explanation** This syslog is generated when clustering moved the flow from one unit in one site to another unit in another site in inter-DC environment. Reason must be whatever triggered the move, such as LISP notification.

**Recommended Action** Verify the flow status in the new unit at new site.
Messages 803001 to 8300006

This section includes messages from 803001 to 852002 and 8300001 to 8300006.

803001

Error Message %FTD-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

Explanation Informational message to the user that the hardware bypass will be continued after bootup.

Recommended Action None required.

Error Message %FTD-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

Explanation Informational message to the user that the hardware bypass will be continued after bootup.

Recommended Action None required.

803002

Error Message %FTD-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

Explanation Informational message to the user that hardware bypass is manually enabled.

Recommended Action None required.

Error Message %FTD-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

Explanation Informational message to the user that hardware bypass is manually enabled.

Recommended Action None required.

803003

Error Message %FTD-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2.

Explanation Informational message to the user that hardware bypass is manually disabled.

Recommended Action None required.

Error Message %FTD-6-803003: User disabled bypass manually on GigabitEthernet 1/3-1/4.

Explanation Informational message to the user that hardware bypass is manually disabled.

Recommended Action None required.

804001

Error Message %FTD-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted

Explanation Informational message to the user about the online insertion of the supported SFP module.
Recommended Action None required.

804002

Error Message %FTD-6-804002: Interface GigabitEthernet1/3 SFP has been removed
Explanation Informational message to the user about removal of the supported SFP module.
Recommended Action None required.

805001

Error Message %FTD-6-805001: Flow offloaded: connection conn_id
outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port)
inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
Explanation Indicates flow is offloaded to the super-fast path.
Recommended Action None required.

805002

Error Message %FTD-6-805002: Flow is no longer offloaded: connection conn_id
outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port)
inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
Explanation Indicates flow offloading is disabled on a flow which was offloaded to the super-fast path.
Recommended Action None required.

805003

Error Message %FTD-6-805003: Flow is no longer offloaded: connection conn_id
outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port)
inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
Explanation Indicates flow couldn’t be offloaded. For example, due to flow entry collision on the offload flow table.
Recommended Action None required.

806001

Error Message %FTD-6-806001: Primary alarm CPU temperature is High temperature
Explanation The CPU has reached temperature over primary alarm temperature setting for high temperature and such alarm is enabled.
  • temperature – Current CPU temperature (in Celsius).
Recommended Action Contact Administrator who configured this alarm on following actions.
806002

**Error Message** %FTD-6-806002: Primary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under primary alarm temperature setting for high temperature.

**Recommended Action** None required.

806003

**Error Message** %FTD-6-806003: Primary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under primary alarm temperature setting for low temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

806004

**Error Message** %FTD-6-806004: Primary alarm for CPU Low temperature is cleared

**Explanation** The CPU temperature goes up to over primary alarm temperature setting for low temperature.

**Recommended Action** None required.

806005

**Error Message** %FTD-6-806005: Secondary alarm CPU temperature is High temperature

**Explanation** The CPU has reached temperature over secondary alarm temperature setting for high temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

806006

**Error Message** %FTD-6-806006: Secondary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under secondary alarm temperature setting for high temperature.

**Recommended Action** None required.

806007

**Error Message** %FTD-6-806007: Secondary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under secondary alarm temperature setting for low temperature and such alarm is enabled.
• temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

#### 806008

**Error Message** %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared  
**Explanation** The CPU temperature goes up to over secondary alarm temperature setting for low temperature.  
**Recommended Action** None required.

#### 806009

**Error Message** %FTD-6-806009: Alarm asserted for ALARM_IN_1 description  
**Explanation** Alarm input port 1 is triggered.  
• description – Alarm description configured by user for this alarm input port.  

**Recommended Action** Contact Administrator who configured this alarm on following actions.

#### 806010

**Error Message** %FTD-6-806010: Alarm cleared for ALARM_IN_1 alarm_1_description  
**Explanation** Alarm input port 1 is cleared.  
• description – Alarm description configured by user for this alarm input port.  

**Recommended Action** None required.

#### 806011

**Error Message** %FTD-6-806011: Alarm asserted for ALARM_IN_2 description  
**Explanation** Alarm input port 2 is triggered.  
• description – Alarm description configured by user for this alarm input port.  

**Recommended Action** Contact Administrator who configured this alarm on following actions.

#### 806012

**Error Message** %FTD-6-806012: Alarm cleared for ALARM_IN_2 alarm_2_description  
**Explanation** Alarm input port 2 is cleared.  
• description – Alarm description configured by user for this alarm input port.  

**Recommended Action** None required.
840001

Error Message %FTD-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>

Explanation In the high-availability setup of distributed site-to-site VPN, an attempt to create a backup session is made when an IKEv2 session is established or when the cluster membership changes. However, the attempt may fail for reasons such as capacity limit. Hence this message is generated on the unit of a session owner whenever it is notified of failing to create a backup.

Recommended Action None.

850001

Error Message %FTD-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>)
Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>

Explanation The Automatic-Application-Bypass (AAB) event is triggered due to packet delay exceeding the AAB threshold.

Recommended Action Collect troubleshoot archive, snort core files and contact Cisco TAC.

850002

Error Message %FTD-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>)
Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms (threshold <AAB-threshold>ms)

Explanation The Automatic-Application-Bypass (AAB) event is triggered due to SNORT not responding to traffics for a period exceeding the AAB threshold.

Recommended Action Collect troubleshoot archive, snort core files and contact Cisco TAC.

852001

Error Message %FTD-6-852001: Received Lightweight to Full Proxy event from application Snort for TCP flow ip-address/port to ip-address/port

Explanation This message appears when Snort decides to inspect payload of TCP based upon the matching policy of connection, for example, SSL policy.

  • ip-address: The IPv4 or IPv6 address of flow
  • port: The TCP port number

Recommended Action None required.

852002

Error Message %FTD-6-852002: Received Full Proxy to Lightweight event from application Snort for TCP flow ip-address/port to ip-address/port
Explanation This message appears when Snort is no longer interested to inspect payload of TCP based upon the matching policy of connection, for example, SSL policy DND.

- ip-address: The IPv4 or IPv6 address of flow
- port: The TCP port number

Recommended Action None required.

Error Message %FTD-6-8300001: VPN session redistribution <variable 1>

Explanation These events notify the administrator that the operation related to ‘cluster redistribute vpn-sessiondb’ has started or completed. Where,

- <variable 1>—Action: started or completed

Recommended Action None.

Error Message %FTD-6-8300002: Moved <variable 1> sessions to <variable 2>

Explanation Provides details on how many active sessions were moved to another member of the cluster.

- <variable 1>—number of active sessions moved (this can be less than the number requested)
- <variable 2>—name of the cluster member the sessions where moved to

Recommended Action None.

Error Message %FTD-3-8300003: Failed to send session redistribution message to <variable 1>

Explanation There was an error sending a request to another cluster member. This could be due to an internal error or the cluster member the message was destined for is not available.

- <variable 1>—name of the cluster member the message was destined for

Recommended Action If this message is persistent contact customer support.

Error Message %FTD-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

Explanation This event is displayed when a cluster member receives a request from the master to move a specific number of active sessions to another member in the cluster.

- <variable 1>—Action: Received, Sent
- <variable 2>—number of active sessions to move
Recommended Action None.

8300005

Error Message %FTD-3-8300005: Failed to receive session move response from <variable 1>

Explanation The cluster master has requested a cluster member to move active sessions to another member. If the master has not received a response to this request within a defined period, it will display this event and terminate the redistribution process.

• <variable 1>—name of cluster member which failed to send a move response within timeout period

Recommended Action Re-issue the “cluster redistribute vpn-sessiondb” and if the problem persists, contact support.

8300006

Error Message %FTD-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

Explanation The VPN session redistribution move calculations are based on the active cluster members at the time the process is started. If a cluster member joins or leaves during this process, the master will terminate the session redistribution.

Recommended Action Retry the operation when all of the members have joined or left the cluster.
APPENDIX A

System Health and Network Diagnostic Messages Listed by Severity Level

This appendix contains the following sections:

- Alert Messages, Severity 1, on page 485
- Critical Messages, Severity 2, on page 488
- Error Messages, Severity 3, on page 490
- Warning Messages, Severity 4, on page 504
- Notification Messages, Severity 5, on page 515
- Informational Messages, Severity 6, on page 522
- Debugging Messages, Severity 7, on page 534
- Variables Used in Syslog Messages, on page 540

Alert Messages, Severity 1

The following messages appear at severity 1, alerts:

- %FTD-1-101001: (Primary) Failover cable OK.
- %FTD-1-101002: (Primary) Bad failover cable.
- %FTD-1-101003: (Primary) Failover cable not connected (this unit).
- %FTD-1-101004: (Primary) Failover cable not connected (other unit).
- %FTD-1-101005: (Primary) Error reading failover cable status.
- %FTD-1-103001: (Primary) No response from other firewall (reason code = code).
- %FTD-1-103002: (Primary) Other firewall network interface interface_number OK.
- %FTD-1-103003: (Primary) Other firewall network interface interface_number failed.
- %FTD-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string
- %FTD-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure
- %FTD-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num
- %FTD-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num
- %FTD-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %FTD-1-104008: Mate hwid index is not compatible.
- %FTD-1-104002: (Primary) Switching to STANDBY (cause: string).
- %FTD-1-104003: (Primary) Switching to FAILED.
- %FTD-1-104004: (Primary) Switching to OK.
- %FTD-1-105001: (Primary) Disabling failover.
- %FTD-1-105002: (Primary) Enabling failover.
- %FTD-1-105003: (Primary) Monitoring on interface interface_name waiting
- %FTD-1-105004: (Primary) Monitoring on interface interface_name normal
- %FTD-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %FTD-1-105006: (Primary) Link status Up on interface interface_name.
- %FTD-1-105007: (Primary) Link status Down on interface interface_name.
- %FTD-1-105008: (Primary) Testing interface interface_name.
- %FTD-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %FTD-1-105011: (Primary) Failover cable communication failure
- %FTD-1-105020: (Primary) Incomplete/slow config replication
- %FTD-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name
- %FTD-1-105031: Failover LAN interface is up
- %FTD-1-105032: (Primary) LAN Failover interface is down
- %FTD-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %FTD-1-105035: Receive a LAN failover interface down msg from peer.
- %FTD-1-105036: dropped a LAN Failover command message.
- %FTD-1-105037: The primary and standby units are switching back and forth as the active unit.
- %FTD-1-105038: (Primary) Interface count mismatch
- %FTD-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %FTD-1-105040: (Primary) Mate failover version is not compatible.
- %FTD-1-105041: cmd failed during sync.
- %FTD-1-105042: (Primary) Failover interface OK
- %FTD-1-105043: (Primary) Failover interface failed
- %FTD-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %FTD-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %FTD-1-105046 (Primary|Secondary) Mate has a different chassis
- %FTD-1-105047: Mate has a io_card_name1 card in slot_number which is different from my io_card_name2
- %FTD-1-105048: (unit) Mate’s service module (application) is different from mine (application)
- %FTD-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name
- %FTD-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name
- %FTD-1-106101 The number of ACL log deny-flows has reached limit (number).
- %FTD-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name
- %FTD-1-107002: RIP pkt failed from IP_address: version=number on interface interface_name
- %FTD-1-111111 error_message
- %FTD-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).
- %FTD-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).
- %FTD-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string).
- %FTD-1-1199012: Stack smash during new_stack_call in process/fiber process/fiber, call target f, stack size s, process/fiber name of the process/fiber that caused the stack smash
- %FTD-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0x132e03b, corrective action at 0xa1961a0%FTD-1-199013: syslog
- %FTD-1-199021: System memory utilization has reached the configured watchdog trigger level of Y%. System will now reload
- %FTD-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.
- %FTD-n-216001: internal error in: function: message
- %FTD-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.
- %FTD-1-332004: Web Cache IP_address/service_ID lost
- %FTD-1-505011: Module ips data channel communication is UP.
- %FTD-1-505014: Module module_id, application down name, version version reason
- %FTD-1-505015: Module module_id, application up application, version version
- %FTD-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %FTD-1-709004: (Primary) End Configuration Replication (ACT)
- %FTD-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %FTD-1-709006: (Primary) End Configuration Replication (STB)
- %FTD-1-713900: Descriptive_event_string.
- %FTD-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.
- %FTD-1-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating
- %FTD-1-716509: internal error in: function: Fiber scheduler is scheduling alien fiber. Cannot continue terminating
- %FTD-1-716510: internal error in: function: Fiber scheduler is scheduling finished fiber. Cannot continue terminating
- %FTD-1-716516: internal error in: function: OCCAM has corrupted ROL array. Cannot continue terminating
- %FTD-1-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating
- %FTD-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition
- %FTD-1-717049: Local CA Server certificate is due to expire in number days and a replacement certificate is available for export.
- %FTD-1-717054: The type certificate in the trustpoint tp name is due to expire in number days. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number
- %FTD-1-717055: The type certificate in the trustpoint tp name has expired. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number
- %FTD-1-735001 Cooling Fan var1: OK
- %FTD-1-735002 Cooling Fan var1: Failure Detected
- %FTD-1-735003 Power Supply var1: OK
- %FTD-1-735004 Power Supply var1: Failure Detected
- %FTD-1-735005 Power Supply Unit Redundancy OK
- %FTD-1-735006 Power Supply Unit Redundancy Lost
- %FTD-1-735007 CPU var1: Temp: var2 var3, Critical
- %FTD-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical
- %FTD-1-735011: Power Supply var1: Fan OK
- %FTD-1-735012: Power Supply var1: Fan Failure Detected
- %FTD-1-735013: Voltage Channel var1: Voltage OK
- %FTD-1-735014: Voltage Channel var1: Voltage Critical
- %FTD-1-735017: Power Supply var1: Temp: var2 var3, OK
Critical Messages, Severity 2

The following messages appear at severity 2, critical:

• %FTD-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
• %FTD-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
• %FTD-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
• %FTD-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.
• %FTD-2-106013: Dropping echo request from IP_address to PAT address IP_address
• %FTD-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
• %FTD-2-106017: Deny IP due to Land Attack from IP_address to IP_address
• %FTD-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
• %FTD-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
• %FTD-2-106024: Access rules memory exhausted
• %FTD-2-108003: Terminating ESMTPT/SMTP connection; malicious pattern detected in the mail address from source_interface/source_address/source_port to dest_interface:dest_address/dset_port. Data:string
• %FTD-2-109011: Authen Session Start: user 'user', sid number
• %FTD-2-112001: (string:dec) Clear complete.
• %FTD-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
• %FTD-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
• %FTD-2-113027: Username could not be found in certificate
• %FTD-2-115000: Critical assertion in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
• %FTD-2-199011: Close on bad channel in process/fiber process/fiber, channel ID p, channel state s process/fiber name of the process/fiber that caused the bad channel close operation.
• %FTD-2-199014: syslog
• %FTD-2-199020: System memory utilization has reached X%. System will reload if memory usage reaches the configured trigger level of Y%.
• %FTD-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
• %FTD-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
• %FTD-2-215001: Bad route_compress() call, sdb= number
• %FTD-2-217001: No memory for string in string
• %FTD-2-218001: Failed Identification Test in slot# [fail#/res].
• %FTD-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
• %FTD-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.
• %FTD-2-218004: Failed Identification Test in slot# [fail#/res]
• %FTD-2-218005: Inconsistency detected in the system information programmed in non-volatile memory
• %FTD-2-321005: System CPU utilization reached utilization %
• %FTD-2-321006: System memory usage reached utilization %
• %FTD-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src_ifc:sip/sport to dest_ifc:dip/dport
• %FTD-2-709007: Configuration replication failed for command command
• %FTD-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
• %FTD-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
• %FTD-2-713901: Descriptive_text_string.
• %FTD-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
• %FTD-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
• %FTD-2-716502: internal error in: function: Fiber library cannot allocate default arena
• %FTD-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
• %FTD-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
• %FTD-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
• %FTD-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER
• %FTD-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
• %FTD-2-716513: internal error in: function: Fiber in callback blocked on other channel
• %FTD-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
• %FTD-2-716517: internal error in: function: OCCAM cached block has no associated arena
• %ASWA-2-716518: internal error in: function: OCCAM pool has no associated arena
• %FTD-2-716520: internal error in: function: OCCAM pool has no block list
• %FTD-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
Error Messages, Severity 3

The following messages appear at severity 3, errors:

- %FTD-3-105010: (Primary) Failover message block alloc failed
- %FTD-3-106010: Deny inbound protocol src [interface_name: source_address/source_port] [[idfw_user | FQDN_string], sg_info] dst [interface_name: dest_address/dest_port] [[idfw_user | FQDN_string], sg_info]
- %FTD-3-106011: Deny inbound (No xlate) string
- %FTD-3-106014: Deny inbound icmp src interface_name: IP_address [[idfw_user | FQDN_string], sg_info] dst interface_name: IP_address [[idfw_user | FQDN_string], sg_info] (type dec, code dec)
- %FTD-3-109013: User must authenticate before using this service
- %FTD-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %FTD-3-109018: Downloaded ACL acl_ID is empty
- %FTD-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %FTD-3-109020: Downloaded ACL has config error; ACE
- %FTD-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %FTD-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.
- %FTD-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username
- %FTD-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name
- %FTD-3-109103: CoA action-type from coa-source-ip failed for user username, with session ID: audit-session-id.
- %FTD-3-109104: CoA action-type from coa-source-ip failed for user username, session ID: audit-session-id. Action not supported.
- %FTD-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %FTD-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action
- %FTD-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds
- %FTD-3-113021: Attempted console login failed. User username did NOT have appropriate Admin Rights.
- %FTD-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).
- %FTD-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).
- %FTD-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %FTD-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string).
- %FTD-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string).
- %FTD-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).
- %FTD-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).
- %FTD-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).
- %FTD-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).
- %FTD-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).
- %FTD-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).
- %FTD-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).
- %FTD-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).
- %FTD-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).
- %FTD-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %FTD-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.
- %FTD-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string
- %FTD-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string.
- %FTD-3-115001: Error in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition.
- %FTD-3-199015: syslog
- %FTD-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %FTD-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit
- %FTD-3-201005: FTP data connection failed for IP_address IP_address
- %FTD-3-201006: RCMD backconnection failed for IP_address/port.
- %FTD-3-201008: Disallowing new connections.
- %FTD-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded
- %FTD-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
- %FTD-3-201013: Per-client connection limit exceeded curr num/limit for [input|output] packet from ip/port to ip/port on interface_interface_name
- %FTD-3-202010: [NAT | PAT] pool exhausted for pool-name, port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface:src-ip/src-port to out-interface:dst-ip/dst-port
- %FTD-3-208005: (function;line_num) clear command return code
- %FTD-3-210001: LU sw_module_name error = number
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-3-210002: LU allocate block (bytes) failed.
- %FTD-3-210003: Unknown LU Object number
- %FTD-3-210005: LU allocate secondary(optional) connection failed for protocol[TCP|UDP] connection from ingress interface name:Real IP Address/Real Port to egress interface name:Real IP Address/Real Port
- %FTD-3-210006: LU look NAT for IP_address failed
- %FTD-3-210007: LU allocate xlate failed for type[static | dynamic]-[NAT | PAT] secondary(optional) protocol translation from ingress interface name:Real IP Address/real port (Mapped IP Address/Mapped Port) to egress interface name:Real IP Address/Real Port (Mapped IP Address/Mapped Port)
- %FTD-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %FTD-3-210010: LU make UDP connection for outside_address/inside_port inside_address:inside_port failed
- %FTD-3-210020: LU PAT port port reserve failed
- %FTD-3-210021: LU create static xlate global_address ifc interface_name failed
- %FTD-3-211001: Memory allocation Error
- %FTD-3-211003: Error in computed percentage CPU usage value
- %FTD-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %FTD-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %FTD-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %FTD-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %FTD-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %FTD-3-212006: Dropping SNMP request from src_addr/src_port to ifc:dst_addr/dst_port because: reason_username.
- %FTD-3-212010: Configuration request for SNMP user %s failed. Host %s reason.
- %FTD-3-212011: SNMP engineBoots is set to maximum value. Reason: %s User intervention necessary.
- %FTD-3-212012: Unable to write SNMP engine data to persistent storage.
- %FTD-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num
- %FTD-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num
- %FTD-3-219002: I2C_API_name error, slot = slot_number, device = device_number, address = address, byte count = count. Reason: reason_string
- %FTD-3-302019: H.323 library_name ASN Library failed to initialize, error code number
- %FTD-3-302302: ACL = deny; no sa created
- %FTD-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dest_port [(idfw_user)]
- %FTD-3-305016: Unable to create protocol connection from real_interface:real_host_ip/real_source_port to real_dest_interface:real_dest_ip/real_dest_port due to reason.
- %FTD-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from <source device IP> to <destination device IP>/Active Port Block >
- %FTD-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
- %FTD-3-313008: Denied ICMPv6 type=number, code=code from IP_address on interface interface_name
• %FTD-3-316001: Denied new tunnel to IP_address. VPN peer limit (platform_vpn_peer_limit) exceeded
• %FTD-3-316002: VPN Handle error: protocol=protocol, src in_if_num=src_addr, dst out_if_num=dst_addr
• %FTD-3-317001: No memory available for limit_slow
• %FTD-3-317002: Bad path index of number for IP_address, number max
• %FTD-3-317003: IP routing table creation failure - reason
• %FTD-3-317004: IP routing table limit warning
• %FTD-3-317005: IP routing table limit exceeded - reason, IP_address_netmask
• %FTD-3-317006: Pdb index error pdb, pdb_index, pdb_type
• %FTD-3-317012: Interface IP route counter negative - name=if-string-value
• %FTD-3-318001: Internal error: reason
• %FTD-3-318002: Flagged as being an ABR without a backbone area
• %FTD-3-318003: Reached unknown state in neighbor state machine
• %FTD-3-318004: area string lsid IP_address mask netmask adv IP_address type number
• %FTD-3-318005: lsid ip_address adv IP_address type number gateway gateway_address metric number
• %FTD-3-318006: if interface_name if_state number
• %FTD-3-318007: OSPF is enabled on interface_name during idb initialization
• %FTD-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
• %FTD-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line_num
• %FTD-3-318101: Internal error: %REASON
• %FTD-3-318102: Flagged as being an ABR without a backbone area T
• %FTD-3-318103: Reached unknown state in neighbor state machine
• %FTD-3-318104: DB already exist : area %AREA_ID_STR lsid %i adv %i type 0x%x
• %FTD-3-318105: lsid %i adv %i type 0x%x gateway %i metric %d network %i mask %i protocol %#x attr %#x net-metric %d
• %FTD-3-318106: if %IF_NAME if_state %d
• %FTD-3-318107: OSPF is enabled on %IF_NAME during idb initialization
• %FTD-3-318108: OSPF process %d is changing router-id. Reconfigure virtual link neighbors with our new router-id
• %FTD-3-318109: OSPFv3 has received an unexpected message: %0x/%0x
• %FTD-3-318110: Invalid encrypted key %s.
• %FTD-3-318111: SPI %u is already in use with ospf process %d
• %FTD-3-318112: SPI %u is already in use by a process other than ospf process %d.
• %FTD-3-318113: %s %s is already configured with SPI %u.
• %FTD-3-318114: The key length used with SPI %u is not valid
• %FTD-3-318115: %s error occured when attempting to create an IPsec policy for SPI %u
• %FTD-3-318116: SPI %u is not being used by ospf process %d.
• %FTD-3-318117: The policy for SPI %u could not be removed because it is in use.
• %FTD-3-318118: %s error occurred when attempting to remove the IPsec policy with SPI %u
• %FTD-3-318119: Unable to close secure socket with SPI %u on interface %s
• %FTD-3-318120: OSPFv3 was unable to register with IPsec
• %FTD-3-318121: IPsec reported a GENERAL ERROR: message %s, count %d
• %FTD-3-318122: IPsec sent a %s message %s to OSPFv3 for interface %s. Recovery attempt %d.
• %FTD-3-318123: IPsec sent a %s message %s to OSPFv3 for interface %IF_NAME. Recovery aborted
• %FTD-3-318125: Init failed for interface %IF_NAME
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-3-318126: Interface %IF_NAME is attached to more than one area
- %FTD-3-318127: Could not allocate or find the neighbor
- %FTD-3-320001: The subject name of the peer cert is not allowed for connection
- %FTD-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)
- %FTD-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %FTD-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is {statically|dynamically} bound to MAC Address MAC_address_2.
- %FTD-3-322003: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is not bound to any MAC Address.
- %FTD-3-323001: Module module_id experienced a control channel communications failure.
- %FTD-3-323002: Module module_id is not able to shut down, shut down request not answered.
- %FTD-3-323003: Module module_id is not able to reload, reload request not answered.
- %FTD-3-323004: Module module_id failed to write software version (currently vver), reason. Hw-module reset is required before further use.
- %FTD-3-323005: Module module_id can not be started completely
- %FTD-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.
- %FTD-3-325001: Router ipv6 address on interface has conflicting ND (Neighbor Discovery) settings
- %FTD-3-326001: Unexpected error in the timer library: error_message
- %FTD-3-326002: Error in error_message: error_message
- %FTD-3-326004: An internal error occurred while processing a packet queue
- %FTD-3-326005: Mrib notification failed for (IP_address, IP_address)
- %FTD-3-326006: Entry-creation failed for (IP_address, IP_address)
- %FTD-3-326007: Entry-update failed for (IP_address, IP_address)
- %FTD-3-326008: MRIB registration failed
- %FTD-3-326009: MRIB connection-open failed
- %FTD-3-326010: MRIB unbind failed
- %FTD-3-326011: MRIB table deletion failed
- %FTD-3-326012: Initialization of string functionality failed
- %FTD-3-326013: Internal error: string in string line %d (%s)
- %FTD-3-326014: Initialization failed: error_message error_message
- %FTD-3-326015: Communication error: error_message error_message
- %FTD-3-326016: Failed to set un-numbered interface for interface_name (string)
- %FTD-3-326017: Interface Manager error - string in string: string
- %FTD-3-326019: string in string: string
- %FTD-3-326020: List error in string: string
- %FTD-3-326021: Error in string: string
- %FTD-3-326022: Error in string: string
- %FTD-3-326023: string - IP_address: string
- %FTD-3-326024: An internal error occurred while processing a packet queue.
- %FTD-3-326025: string
- %FTD-3-326026: Server unexpected error: error_message
- %FTD-3-326027: Corrupted update: error_message
- %FTD-3-326028: Asynchronous error: error_message
• %FTD-3-327001: IP SLA Monitor: Cannot create a new process
• %FTD-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
• %FTD-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
• %FTD-3-328001: Attempt made to overwrite a set stub function in string.
• %FTD-3-329001: The string0 subblock named string1 was not removed
• FTD-3-331001: Dynamic DNS Update for 'fqdn_name' = ip_address failed
• %FTD-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.
• %FTD-3-332002: Unable to allocate message buffer, WCCP V2 closing down.
• %FTD-3-336001 Route destination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up
• %FTD-3-336002: Handle handle_id is not allocated in pool.
• %FTD-3-336003: No buffers available for bytes byte packet
• %FTD-3-336004: Negative refcount in pakdesc pakdesc.
• %FTD-3-336005: Flow control error, error, on interface_name.
• %FTD-3-336006: num peers exist on IIDB interface_name.
• %FTD-3-336007: Anchor count negative
• %FTD-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str
• %FTD-3-336009 ddb_name as_id: Internal Error
• %FTD-3-336012: Interface interface_names going down and neighbor_links links exist
• %FTD-3-336013: Route iproute, iproute_successors successors, db_successors rdfs
• %FTD-3-336014: "EIGRP_PDM_Process_name, event_log"
• %FTD-3-336015: Unable to open socket for AS as_number"
• %FTD-3-336016: Unknown timer type timer_type expiration
• %FTD-3-336018: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached
• %FTD-3-336019: process_name as_number: prefix_source prefix limit reached (prefix_threshold).
• %FTD-3-339006: Umbrella resolver current resolver ipv46 is reachable, resuming Umbrella redirect.
• FTD-3-339007: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-open. Starting probe to resolver.
• FTD-3-339008: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-close.
• %FTD-3-340001: Loopback-proxy info: error_string context id context_id, context type = version/request_type/address_type client socket (internal)= client_address_internal/client_port_internal server socket (internal)= server_address_internal/server_port_internal server socket (external)= server_address_external/server_port_external remote socket (external)= remote_address_external/remote_port_external
• %FTD-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr
• %FTD-3-341004: Storage device not available: Attempt to shutdown module %s failed.
• %FTD-3-341005: Storage device not available. Shutdown issued for module %s.
• %FTD-3-341006: Storage device not available. Failed to stop recovery of module %s .
• %FTD-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.
• %FTD-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.
• %FTD-3-341011: Storage device with serial number ser_no in bay bay_no faulty.
• %FTD-3-402140: CRYPTO: RSA key generation error: modulus len len
• %FTD-3-402141: CRYPTO: Key zeroization error: key set type, reason reason
• %FTD-3-402142: CRYPTO: Bulk data op error: algorithm alg, mode mode
• %FTD-3-402143: CRYPTO: alg type key op
• %FTD-3-402144: CRYPTO: Digital signature error: signature algorithm sig, hash algorithm hash
• %FTD-3-402145: CRYPTO: Hash generation error: algorithm hash
• %FTD-3-402146: CRYPTO: Keyed hash generation error: algorithm hash, key len len
• %FTD-3-402147: CRYPTO: HMAC generation error: algorithm alg
• %FTD-3-402148: CRYPTO: Random Number Generator error
• %FTD-3-402149: CRYPTO: weak encryption type (length). Operation disallowed. Not FIPS 140-2 compliant
• %FTD-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg). Operation disallowed. Not FIPS 140-2 compliant
• %FTD-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface_name AC:ac_name
• %FTD-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface_name AC:ac_name
• %FTD-3-403503: PPPoE:PPP link down:reason
• %FTD-3-403504: PPPoE:No vpdn group group_name for PPPoE is created
• %FTD-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name
• %FTD-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
• %FTD-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
• %FTD-3-414003: TCP Syslog Server intf:IP_Address/port not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.
• %FTD-3-414005: TCP Syslog Server intf:IP_Address/port connected, New connections are permitted based on logging permit-hostdown policy
• %FTD-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.
• %FTD-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.
• %FTD-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.
• %FTD-3-425006 Redundant interface redundant_interface_name switch active member to interface_name failed.
• %FTD-3-505016: Module module_id application changed from: name version version state state to: name version state state.
• %FTD-3-500005: connection terminated from in_ifc_name:src_address/src_port to out_ifc_name:dest_address/dest_port due to invalid combination of inspections on same flow. Inspect inspect_name is not compatible with inspect inspect_name_2
• %FTD-3-507003: The flow of type protocol from the originating interface: src_ip/src_port to dest_if:dest_ip/dest_port terminated by inspection engine, reason -
• %FTD-3-520001: error_string
• %FTD-3-520002: bad new ID table size
• %FTD-3-520003: bad id in error_string (id: 0xid_num)
• %FTD-3-520004: error_string
• %FTD-3-520005: error_string
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-3-520010: Bad queue elem – qelem_ptr: flink flink_ptr, blink blink_ptr, flink->blink
  flink_blink_ptr, blink->flink_blink_flink_ptr
- %FTD-3-520011: Null queue elem
- %FTD-3-520013: Regular expression access check with bad list acl_ID
- %FTD-3-520020: No memory available
- %FTD-3-520021: Error deleting trie entry, error_message
- %FTD-3-520022: "Error adding mask entry, error_message
- %FTD-3-520023: Invalid pointer to head of tree, 0x<radix_node_ptr>
- %FTD-3-520024: Orphaned mask #radix_mask_ptr, refcount= radix_mask_ptr `s ref count at #
  radix_node_address, next=# radix_node_next
- %FTD-3-520025: No memory for radix initialization: error_msg%FTD-3-602305: IPSEC: SA creation
  error, source source address, destination destination address, reason error string
- %FTD-3-611313: VPN Client: Backup Server List Error: reason
- %FTD-3-613004: Internal error: memory allocation failure
- %FTD-3-613005: Flagged as being an ABR without a backbone area
- %FTD-3-613006: Reached unknown state in neighbor state machine
- %FTD-3-613007: area string lsid IP_address mask netmask type number
- %FTD-3-613008: if inside if_state number
- %FTD-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with
  our new router-id
- %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
- %FTD-3-613029: Router-ID IP_address is in use by ospf process number%FTD-3-613016: Area string
  router-LSA of length number bytes plus update overhead bytes is too large to flood.
- %FTD-3-613032: Init failed for interface inside, area is being deleted. Try again.%FTD-3-613033:
  Interface inside is attached to more than one area
- %FTD-3-613034: Neighbor IP_address not configured
- %FTD-3-613035: Could not allocate or find neighbor IP_address%FTD-4-613015: Process 1 flushes
  LSA ID IP_address type-number adv-rtr IP_address in area mask.
- %FTD-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to
  interface_name:dest_IP/service
- %FTD-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface
  interface num, for Peer IP_address ignored
- %FTD-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %FTD-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %FTD-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %FTD-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %FTD-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %FTD-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %FTD-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %FTD-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %FTD-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %FTD-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %FTD-3-713033: Received invalid remote Proxy Range IP_address - IP_address
- %FTD-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst:
  dest_address
- %FTD-3-713043: Cookie/peer address IP_address session already in progress
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-3-713048: Error processing payload: Payload ID: id
- %FTD-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!
- %FTD-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.
- %FTD-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!
- %FTD-3-713062: IKE Peer address same as our interface address IP_address
- %FTD-3-713063: IKE Peer address not configured for destination IP_address
- %FTD-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %FTD-3-713072: Password for user (user) too long, truncating to number characters
- %FTD-3-713081: Unsupported certificate encoding type encoding_type
- %FTD-3-713082: Failed to retrieve identity certificate
- %FTD-3-713083: IKE lost contact with remote peer, deleting connection (keepalive_type)
- %FTD-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %FTD-3-713107: IP_Address request attempt failed!
- %FTD-3-713109: Unable to process the received peer certificate
- %FTD-3-713112: IKE lost contact with remote peer, deleting connection (keepalive_type)
- %FTD-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)
- %FTD-3-713123: IKE lost contact with remote peer, deleting connection (keepalive_type = keepalive_type)
- %FTD-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %FTD-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %FTD-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %FTD-3-713130: Cannot obtain an IP_address for remote peer
- %FTD-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number
- %FTD-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %FTD-3-713137: Group group_name not found and BASE GROUP default preshared key not configured
- %FTD-3-713140: Split Tunneling Policy requires network list but none configured
- %FTD-3-713141: IPv6 address in IPSec SA not in the configured network list
- %FTD-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value. Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value

System Health and Network Diagnostic Messages Listed by Severity Level
%FTD-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
%FTD-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
%FTD-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
%FTD-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
%FTD-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
%FTD-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
%FTD-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
%FTD-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
%FTD-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
%FTD-3-713167: Remote peer has failed user authentication - check configured username and password
%FTD-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
%FTD-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
%FTD-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
%FTD-3-713185: Error: Username too long - connection aborted
%FTD-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value) is illegal
%FTD-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.
%FTD-3-713191: Maximum concurrent IKE negotiations exceeded!
%FTD-3-713193: Received packet with missing payload, Expected payload: payload_id
%FTD-3-713194: Sending IKE|IPSec Delete With Reason message: termination_reason
%FTD-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
%FTD-3-713203: IKE Receiver: Error reading from socket.
%FTD-3-713205: Could not add static route for client address: IP_address
%FTD-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
%FTD-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id
%FTD-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
%FTD-3-713210: Cannot create dynamic map for Backup L2L entry rule_id
%FTD-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
%FTD-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
%FTD-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version
%FTD-3-713218: Tunnel Rejected: Client Type or Version not allowed.
%FTD-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group
%FTD-3-713227: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address/Local_netmask, remote Proxy Remote_address/Remote_netmask
%FTD-3-713230: Internal Error, ike_lock trying to lock bit that is already locked for type type
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-3-713231: Internal Error, ike_lock trying to unlock bit that is not locked for type type
- %FTD-3-713232: SA lock refCnt = value, bitmask = hexvalue, p1_decrypt_cb = value, qm_decrypt_cb = value, qm_hash_cb = value, qm_spi_ok_cb = value, qm_db = value, qm_secret_key_cb = value, qm_encrypt_cb = value
- %FTD-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %FTD-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPSec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPSec/NAT-T
- %FTD-3-713260: Output interface %d to peer was not found
- %FTD-3-713261: IPV6 address on output interface %d was not found
- %FTD-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address/Local_prefix_len, remote Proxy Remote_address/Remote_prefix_len
- %FTD-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len
- %FTD-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %FTD-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: /prefix_len
- %FTD-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: /prefix_len
- %FTD-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed
- %FTD-3-713902: Descriptive_event_string.
- %FTD-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason
- %FTD-3-716057: Group group User user IP ip Session terminated, no type license available.
- %FTD-3-716061: Group DfltGrpPolicy User user ID IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection
- %FTD-3-716600: Rejected size-recv KB Hostscan data from IP src-ip. Hostscan results exceed default | configured limit of size-conf KB.
- %FTD-3-716601: Rejected size-recv KB Hostscan data from IP src-ip. System-wide limit on the amount of Hostscan data stored on ASA exceeds the limit of data-max KB.
- %FTD-3-716602: Memory allocation error. Rejected size-recv KB Hostscan data from IP src-ip.
- %FTD-3-717001: Querying keypair failed.
- %FTD-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.
- %FTD-3-717010: CRL polling failed for trustpoint trustpoint_name.
- %FTD-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure
- %FTD-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %FTD-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %FTD-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)
- %FTD-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.
- %FTD-3-717020: Failed to install device certificate for trustpoint label. Reason: reason_string.
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

• %FTD-3-717021: Certificate data could not be verified. Locate Reason: reason_string serial number: serial number, subject name: subject name, key length key length bits.
• %FTD-3-717023: SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason_string.
• %FTD-3-717027: Certificate chain failed validation. reason_string.
• %FTD-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address, User username, TunnelGroup tunnel group name, GroupPolicy group policy name to CA ca ip address. Reason: msg
• %FTD-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca
• %FTD-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.
• %FTD-3-719008: Email Proxy service is shutting down.
• %FTD-3-722007: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
• %FTD-3-722008: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
• %FTD-3-722009: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
• %FTD-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection
• %FTD-3-722035: Group group User user-name IP IP_address Received large packet length threshold num).
• %FTD-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).
• %FTD-3-722045: Connection terminated: no SSL tunnel initialization data.
• %FTD-3-722046: Group group User user-name IP IP_address Session terminated: unable to establish tunnel.
• %FTD-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.
• %FTD-3-734004: DAP: Processing error: internal error code
• %FTD-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.
• %FTD-3-737002: IPAA: Received unknown message 'num'
• %FTD-3-737027: IPAA: No data for address request
• % FTD-3-737202: VPNFIP: Pool=pool, ERROR: message
• % FTD-3-737403: POOILIP: Pool=pool, ERROR: message
• %FTD-3-742001: failed to read master key for password encryption from persistent store
• %FTD-3-742002: failed to set master key for password encryption
• %FTD-3-742003: failed to save master key for password encryption, reason reason_text
• %FTD-3-742004: failed to sync master key for password encryption, reason reason_text
• %FTD-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with
• %FTD-3-742006: password decryption failed due to unavailable memory
• %FTD-3-742007: password encryption failed due to unavailable memory
• %FTD-3-742008: password enc_pass decryption failed due to decoding error
• %FTD-3-742009: password encryption failed due to decoding error
• %FTD-3-742010: encrypted password enc_pass is not well formed
• %FTD-3-743010: EOBC RPC server failed to start for client module client name.
• %FTD-3-743011: EOBC RPC call failed, return code code string.
• %FTD-3-746016: user-identity: DNS lookup failed, reason: reason.
• %FTD-3-747010: Clustering: RPC call failed, message message-name, return code code-value.
• %FTD-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continuing operation.
• %FTD-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continuing operation.
• %FTD-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name, continuing operation.
• %FTD-3-747018: Clustering: State progression failed due to timeout in module module-name.
• %FTD-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on failed-interface.
• %FTD-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name.
• %FTD-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name), Clustering must be manually enabled on the unit to re-join.
• %FTD-3-747031: Clustering: Platform mismatch between cluster master (platform-type) and joining unit unit-name (platform-type), unit-name aborting cluster join.
• %FTD-3-747032: Clustering: Service module mismatch between cluster master (module-name) and joining unit unit-name (module-name) in slot slot-number. unit-name aborting cluster join.
• %FTD-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name. unit-name aborting cluster join.
• %FTD-3-747042: Master receives config hash string request message from unknown member id <cluster-member-id>
• %FTD-3-747043: Get config hash string from master error: ret_code <ret_code>, string_len: <string_len>
• %FTD-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number; clustering is disabled
• %FTD-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure
• %FTD-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
• %FTD-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation. Error: error
• %FTD-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group
• %FTD-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group
• %FTD-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group Group=group, Tunnel rejected: IKEv2 not enabled in group policy
• %FTD-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.
• %FTD-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method. No crypto map setting or tunnel group found.
• %FTD-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication. Error: error
• %FTD-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing. Error: error
• %FTD-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID. Error: error
• %FTD-3-751017: Local: localIP:port Remote:remoteIP:port Username: username/group Configuration Error error description
• %FTD-3-751018: Terminating the VPN connection attempt from landing group. Reason: This connection is group locked to locked group.
• %FTD-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.
• %FTD-3-751024: Local:ip addr Remote:ip addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection
• %FTD-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag. Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port.
• %FTD-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag. Map Sequence Number = mapSeq.
• %FTD-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
• %FTD-3-768001: QUOTA: resource utilization is high: requested req, current curr, warning level level
• %FTD-3-768002: QUOTA: resource quota exceeded: requested req, current curr, limit limit
• %FTD-3-768003: QUOTA: management session quota exceeded for user user name: current 3, user limit 3
• %FTD-3-768004: QUOTA: management session quota exceeded for ssh/telnet/http protocol: current 2, protocol limit 2
• %FTD-3-769006: UPDATE: ASA boot system image image_name was not found on disk
• %FTD-3-772002: PASSWORD: console login warning, user username, cause: password expired
• %FTD-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired
• %FTD-3-776202: CTS PAC for Server IP_address, A-ID PAC issuer name has expired
• %FTD-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT ) from source name .
• %FTD-3-779003: STS: Failed to read tag-switching table - reason
• %FTD-3-779004: STS: Failed to write tag-switching table - reason
• %FTD-3-779005: STS: Failed to parse tag-switching request from http - reason
• %FTD-3-779006: STS: Failed to save tag-switching table to flash - reason
• %FTD-3-779007: STS: Failed to replicate tag-switching table to peer - reason
• %FTD-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>
Warning Messages, Severity 4

The following messages appear at severity 4, warning:

- %FTD-4-106023: Deny protocol src [interface_name:source_address/source_port] [(idfw_user|FQDN_string), sg_info)] dst interface_name:dest_address/dest_port [(idfw_user|FQDN_string), sg_info)] [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0x8852875]
- %FTD-4-106027: Deny src [source_address] dst [destination address] by access-group “access-list name”.
- %FTD-4-106103: access-list acl_ID denied protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number first hit hash codes
- %FTD-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %FTD-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.
- %FTD-4-109033: Authentication failed for admin user from src_IP. Interactive challenge processing is not supported for protocol connections
- %FTD-4-109034: Authentication failed for network user from src_IP/port to dst_IP/port. Interactive challenge processing is not supported for protocol connections
- %FTD-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id
- %FTD-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %FTD-4-113026: Error error while executing Lua script for group tunnel group
- %FTD-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached
- %FTD-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn’t exist on the device, terminating connection.
- %FTD-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.
- %FTD-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.
- %FTD-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.
- %FTD-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
- %FTD-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.
- %FTD-4-113038: Group group User user IP ipaddr Unable to create AnyConnect p0arent session.
- %FTD-4-113040: Terminating the VPN connection attempt from attempted group. Reason: This connection is group locked to locked group.
Cisco Firepower Threat Defense Syslog Messages

%FTD-4-113041: Redirect ACL configured for assigned IP does not exist on the device.
%FTD-4-113042: CoA: Non-HTTP connection from src_if:src_ip/src_port to dest_if:dest_ip/dest_port
for user username at client_IP denied by redirect filter; only HTTP connections are supported for
redirection.
%FTD-4-115002: Warning in process: process name fiber: fiber name, component: component name,
subcomponent: subcomponent name, file: filename, line: line number, cond: condition
%FTD-4-199016: syslog
%FTD-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address,
proto = protocol, id = number
%FTD-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address,
dest = dest_address, proto = protocol, id = number
%FTD-4-209005: Discard IP fragment set with more than number elements: src = Too many elements
are in a fragment set.
%FTD-4-216004: prevented: error in function at file(line) - stack trace
%FTD-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign
address/foreign-port to laddr interface:local-address/local-port
%FTD-4-302311: Failed to create a new [protocol] connection from [ingress interface]:[source IP]/[source
port] to [egress interface]:[destination IP]/[destination port] due to application cache memory allocation
failure. The app-cache memory threshold level is [threshold%] and threshold check is [enabled/disabled].
%FTD-4-308002: static global_address inside_address netmask netmask overlapped with global_address
inside_address
%FTD-4-313004: Denied ICMP type=icmp_type, from source_address on interface interface_name to
dest_address:no matching session
%FTD-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface_name
interface. Original IP payload: embedded_frame_info icmp_msg_info = icmp src
src_interface_name:src_address [([idfw_user | FQDN_string], sg_info)] dst
dest_interface_name:dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code
icmp_code) embedded_frame_info = prot src source_address/source_port [([idfw_user | FQDN_string],
sg_info)] dst dest_address/destination_port [([idfw_user | FQDN_string], sg_info)]
%FTD-4-313009: Denied invalid ICMP code icmp-code, for src-ifc:src-address/src-port
(mapped-src-address/mapped-src-port) to dest-ifc:dest-address/dest-port
(mapped-mapped-address/mapped-duration-port) [user], ICMP id icmp-id, ICMP type icmp-type
%FTD-4-325002: Duplicate address ipv6_address/MAC_address on interface
%FTD-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port
for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
%FTD-4-338101: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port
(mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source
malicious address resolved from local or dynamic list: domain name
%FTD-4-338102: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port
(mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination
malicious address resolved from local or dynamic list: domain name
%FTD-4-338103: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port
(mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), source
malicious address resolved
%FTD-4-338104: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port
(mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination
malicious address resolved from local or dynamic list: ip address/netmask
from local or dynamic list: ip address/netmask
%FTD-4-338301: Intercepted DNS reply for domain name from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, matched list
%FTD-4-401001: Shuns cleared
%FTD-4-401002: Shun added: IP_address IP_address port port
%FTD-4-401003: Shun deleted: IP_address
%FTD-4-401004: Shunned packet: IP_address = IP_address on interface interface_name
%FTD-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port
%FTD-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.
%FTD-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.
%FTD-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP. The decapsulated inner packet doesn’t match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot. The SA specifies its local proxy as id_daddr/id_dmask/id_dprot/id_dport and its remote proxy as id_saddr/id_smask/id_sprot/id_sport.
%FTD-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
%FTD-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.
%FTD-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.
%FTD-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed authentication.
%FTD-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from peer_addr (username) to lcl_addr that was dropped by IPSec (drop_reason).
%FTD-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPsec that was dropped by IPsec (drop_reason).
%FTD-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command.
%FTD-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).
%FTD-4-402125: The ASA hardware accelerator ring timed out (parameters).
%FTD-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.
%FTD-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, max_number, allowed have been written to archive_directory. Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.
%FTD-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.
%FTD-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
%FTD-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name
%FTD-4-405001: Received ARP {request | response} collision from IP_address/MAC_address on interface interface_name to IP_address/MAC_address on interface interface_name
%FTD-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
%FTD-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name, MAC_address.

%FTD-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]

%FTD-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]

%FTD-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex

%FTD-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP

%FTD-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest

%FTD-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name

%FTD-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name

%FTD-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded

%FTD-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside_address/outside_port to global_address(inside_address)/inside_port on interface interface_name

%FTD-4-407003: Established limit for RPC services exceeded number

%FTD-4-408001: IP route counter negative - reason, IP_address Attempt: number

%FTD-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2

%FTD-4-408003: can't track this type of object hex

%FTD-4-408101: KEYMAN : Type <encryption_type> encryption unknown. Interpreting keystring as literal.

%FTD-4-408102: KEYMAN : Bad encrypted keystring for key id <key_id>

%FTD-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstall

%FTD-4-409002: db_free: external LSA IP_address netmask

%FTD-4-409003: Received invalid packet: reason from IP_address, interface_name

%FTD-4-409004: Received reason from unknown neighbor IP_address

%FTD-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name

%FTD-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name

%FTD-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask

%FTD-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string

%FTD-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

%FTD-4-409010: Virtual link information found in non-backbone area: string

%FTD-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name

%FTD-4-409012: Detected router with duplicate router ID IP_address in area string

%FTD-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
• %FTD-4-409014: No valid authentication send key is available on interface nameif.
• %FTD-4-409015: Key ID key-id received on interface nameif.
• %FTD-4-409016: Key chain name key-chain-name on nameif is invalid.
• %FTD-4-409017: Key ID key-id in key chain key-chain-name is invalid.
• %FTD-4-409023: Attempting AAA Fallback method method_name for request_type request for user user:Auth-server group server_tag unreachable
• %FTD-4-409101: Received invalid packet: %s from %P, %s
• %FTD-4-409102: Received packet with incorrect area from %P, %s, area %AREA_ID_STR, packet area %AREA_ID_STR
• %FTD-4-409103: Received %s from unknown neighbor %i
• %FTD-4-409104: Invalid length %d in OSPF packet type %d from %P (ID %i), %s
• %FTD-4-409105: Invalid lsa: %s: Type 0x%x, Length 0x%x, LSID %u from %i
• %FTD-4-409106: Found generating default LSA with non-zero mask LSA type: 0x%x Mask: %i metric: %lu area: %AREA_ID_STR
• %FTD-4-409107: OSPFv3 process %d could not pick a router-id, please configure manually
• %FTD-4-409108: Virtual link information found in non-backbone area: %AREA_ID_STR
• %FTD-4-409109: OSPF detected duplicate router-id %i from %P on interface %IF_NAME
• %FTD-4-409110: Detected router with duplicate router ID %i in area %AREA_ID_STR
• %FTD-4-409111: Multiple interfaces (%IF_NAME/%IF_NAME) on a single link detected.
• %FTD-4-409112: Packet not written to the output queue
• %FTD-4-409113: Doubly linked list linkage is NULL
• %FTD-4-409114: Doubly linked list prev linkage is NULL %x
• %FTD-4-409115: Unrecognized timer %d in OSPF %s
• %FTD-4-409116: Error for timer %d in OSPF process %s
• %FTD-4-409117: Can't find LSA database type %x, area %AREA_ID_STR, interface %x
• %FTD-4-409118: Could not allocate DBD packet
• %FTD-4-409119: Invalid build flag %x for LSA %i, type 0x%X
• %FTD-4-409120: Router-ID %i is in use by ospf process %d
• %FTD-4-409121: Router is currently an ASBR while having only one area which is a stub area
• %FTD-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.
• %FTD-4-409123: Neighbor command allowed only on NBMA networks
• %FTD-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
• %FTD-4-409128: OSPFv3-%d Area %AREA_ID_STR: Router %i originating invalid type 0x%x LSA, ID %u, Metric %d on Link ID %d Link Type %d
• %FTD-4-410001: UDP DNS request from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.
• %FTD-4-411001: Line protocol on interface interface_name changed state to up
• %FTD-4-411002: Line protocol on interface interface_name changed state to down
• %FTD-4-411003: Configuration status on interface interface_name changed state to downup
• %FTD-4-411004: Configuration status on interface interface_name changed state to up
• %FTD-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
• %FTD-4-412001: MAC MAC_address moved from interface_1 to interface_2
• %FTD-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
• %FTD-4-413001: Module module_id is not able to shut down. Module Error: errnum message
• %FTD-4-413002: Module module_id is not able to reload. Module Error: errnum message
• %FTD-4-413003: Module module_id is not a recognized type
• %FTD-4-413004: Module module_id failed to write software vnew ver (currently vver), reason. Trying again.
• %FTD-4-413005: Module module_id, application is not supported app_name version app_vers type
• %FTD-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.
• %FTD-4-415016: policy-map map_name: Maximum number of unanswered HTTP requests exceeded
• %FTD-4-417001: Unexpected event received: number
• %FTD-4-417004: Filter violation error: conn number (string:string) in string
• %FTD-4-417006: No memory for string) in string. Handling: string
• %FTD-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) [[idfw_user|FQDN_string], sg_info]] to interface_name IP_address (port) [[idfw_user|FQDN_string], sg_info]]
• %FTD-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: MSS exceeded, MSS size, data size
• %FTD-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.
• %FTD-4-419003: Cleared TCP urgent flag from out_ifc:src_ip/src_port to in_ifc:dest_ip/dest_port.
• %FTD-4-422004: IP SLA Monitor number: Duplicate event received. Event number number1
• %FTD-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
• %FTD-4-422006: IP SLA Monitor Probe number: string
• %FTD-4-424001: Packet denied protocol_string intf_in:src_ip/src_port [[idfw_user | FQDN_string], sg_info]] intf_out:dst_ip/dst_port[[idfw_user | FQDN_string], sg_info]]. [Ingress|Egress] interface is in a backup state.
• %FTD-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port
• %FTD-4-426004: PORT-CHANNEL: Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed of ifc_name1 is X Mbps, Y is 1000 Mbps).
• %FTD-4-429008: Unable to respond to VPN query from CX for session 0x%x. Reason %
• %FTD-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address/source port to egress interface: destination IP address/destination port
• %FTD-4-434007: SFR redirect will override Scansafe redirect for flow from ingress interface:source IP address/source port to egress interface: destination IP address/destination port (user)
• %FTD-4-446003: Denied TLS Proxy session from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, UC-IME license is disabled.
• %FTD-4-447001: ASP DP to CP queue_name was full. Queue length length, limit limit
• %FTD-4-448001: Denied SRTP crypto session setup on flow from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, licensed K8 SRTP crypto session of limit exceeded
• %FTD-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
• %FTD-4-507002: Data copy in proxy-mode exceeded the buffer limit
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-4-603110: Failed to establish L2TP session, tunnel_id = tunnel_id, remote_peer_ip = peer_ip, user = username. Multiple sessions per tunnel are not supported
- %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.
- %FTD-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too small
- %FTD-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too large
- %FTD-4-612002: Auto Update failed: filename, version: number, reason: reason
- %FTD-4-612003: Auto Update failed to contact: url, reason: reason
- %FTD-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address
- %FTD-4-613018: Maximum number of non self-generated LSA has been exceeded "OSPF number" - number LSAs
- %FTD-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs
- %FTD-4-613021: Packet not written to the output queue
- %FTD-4-613022: Doubly linked list linkage is NULL
- %FTD-4-613023: Doubly linked list prev linkage is NULL number
- %FTD-4-613024: Unrecognized timer number in OSPF string
- %FTD-4-613025: Invalid build flag number for LSA IP_address, type number
- %FTD-4-613026: Can not allocate memory for area structure
- %FTD-4-613030: Router is currently an ASBR while having only one area which is a stub area
- %FTD-4-613031: No IP address for interface inside
- %FTD-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network
- %FTD-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %FTD-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network
- %FTD-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks
- %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
- %FTD-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared
- %FTD-4-620002: Unsupported CTIQBE version: hex from interface_name:IP_address/port to interface_name:IP_address/port
- %FTD-4-769009: UPDATE: Image booted image_name is different from boot images.
- %FTD-4-709008: (Primary | Secondary) Configuration sync in progress. Command: 'command' executed from (terminal/http) will not be replicated to or executed by the standby unit.
- %FTD-4-711002: Task ran for elapsed_time msecs, process = process_name, PC = PC Traceback = traceback
- %FTD-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call stack
- %FTD-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %FTD-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %FTD-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
• %FTD-4-713240: Received DH key with bad length: received length=rlength expected length=elength
• %FTD-4-713241: IE Browser Proxy Method setting_number is Invalid
• %FTD-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
• %FTD-4-713243: META-DATA Unable to find the requested certificate
• %FTD-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
• %FTD-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
• %FTD-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
• %FTD-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
• %FTD-4-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
• %FTD-4-713249: META-DATA Received unsupported authentication results: result
• %FTD-4-713251: META-DATA Received authentication failure message
• %FTD-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name
• %FTD-4-713903: Group = group policy, Username = user name, IP = remote IP, ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP.
• %FTD-4-716007: Group group User user WebVPN Unable to create session.
• %FTD-4-716022: Unable to connect to proxy server reason.
• %FTD-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.
• %FTD-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.
• %FTD-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.
• %FTD-4-716046: Group group-name-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.
• %FTD-4-716047: Group group-name User user-name IP IP_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
• %FTD-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.
• %FTD-4-716052: Group group-name User user-name IP IP_address Pending session terminated.
• %FTD-4-717026: Name lookup failed for hostname hostname during PKI operation.
• %FTD-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string
• %FTD-4-717035: OCSP status is being checked for certificate certificate_identifier.
• %FTD-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.
• %FTD-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
• %FTD-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
• %FTD-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
• %FTD-4-720008: (VPN-unit) Failed to register to High Availability Framework.
• %FTD-4-720009: (VPN-unit) Failed to create version control block.
• %FTD-4-720011: (VPN-unit) Failed to allocate memory
• %FTD-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name
• %FTD-4-720022: (VPN-unit) Cannot find trust point trustpoint
• %FTD-4-720033: (VPN-unit) Failed to queue add to message queue.
• %FTD-4-720038: (VPN-unit) Corrupted message from active unit.
• %FTD-4-720043: (VPN-unit) Failed to send type message id to standby unit
• %FTD-4-720044: (VPN-unit) Failed to receive message from active unit
• %FTD-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.
• %FTD-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
• %FTD-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
• %FTD-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port
• %FTD-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.
• %FTD-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
• %FTD-4-720058: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.
• %FTD-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
• %FTD-4-720066: (VPN-unit) Failed to activate IKE database.
• %FTD-4-720067: (VPN-unit) Failed to deactivate IKE database.
• %FTD-4-720068: (VPN-unit) Failed to parse peer message.
• %FTD-4-720069: (VPN-unit) Failed to activate cTCP database.
• %FTD-4-720070: (VPN-unit) Failed to deactivate cTCP database.
• %FTD-4-720073: VPN Session failed to replicate - ACL acl_name not found
• %FTD-4-721007: (device) Fail to update access list list_name on standby unit.
• %FTD-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.
• %FTD-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.
• %FTD-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.
• %FTD-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.
• %FTD-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.
• %FTD-4-722001: IP IP_address Error parsing SVC connect request.
• %FTD-4-722002: IP IP_address Error consolidating SVC connect request.
• %FTD-4-722003: IP IP_address Error authenticating SVC connect request.
• %FTD-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
• %FTD-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num
• %FTD-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length
• %FTD-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
• %FTD-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version
• %FTD-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length
• %FTD-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection
• %FTD-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
• %FTD-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
• %FTD-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
• %FTD-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
• %FTD-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
• %FTD-4-72054: Group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP
• %FTD-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.
• %FTD-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
• %FTD-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
• %FTD-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.
• %FTD-4-733102: Threat-detection adds host %I to shun list
• %FTD-4-733103: Threat-detection removes host %I from shun list
• %FTD-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED
• %FTD-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED
• %FTD-4-735015: CPU var1: Temp: var2 var3, Warm
• %FTD-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm
• %FTD-4-735018: Power Supply var1: Temp: var2 var3, Critical
• %FTD-4-735019: Power Supply var1: Temp: var2 var3, Warm
• %FTD-4-735026: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.
• %FTD-4-737012: IPAA: Address assignment failed
• %FTD-4-737013: IPAA: Error freeing address ip-address, not found
• %FTD-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
• %FTD-4-737028: IPAA: Adding ip-address to standby: failed
• %FTD-4-737030: IPAA: Adding %m to standby: address already in use
• %FTD-4-737032: IPAA: Removing ip-address from standby: not found
• %FTD-4-737033: IPAA: Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator
• %FTD-4-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.
• %FTD-4-737203: VPNFIP: Pool=pool, WARN: message
• %FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message
• %FTD-4-737404: POOLIP: Pool=pool, WARN: message
• %FTD-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3
• %FTD-4-741006: Unable to write Coredump Helper configuration, reason variable 1
• %FTD-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B.
• %FTD-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
• %FTD-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A, unit-name-B will leave, then join as a slave.
• %FTD-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
Cisco Firepower Threat Defense Syslog Messages

- %FTD-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address/ip-mask on new unit, ip-address/ip-mask on local unit).
- %FTD-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
- %FTD-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
- %FTD-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).
- %FTD-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.
- %FTD-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).
- %FTD-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.
- %FTD-4-747030: Clustering: Configuration on the chassis is missing or incomplete; clustering is disabled.
- %FTD-4-747031: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure.
- %FTD-4-747032: Mismatched resource profile size with Master. Master: <cores number> CPU cores / <RAM size> MB RAM, Mine: <cores number> CPU cores / <RAM size> MB RAM
- %FTD-4-747033: Mismatched module type with Master. Master: <PID>, MINE: <PID>
- %FTD-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error
- %FTD-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %FTD-4-751014: Local:localIP:port Remote:remotelP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error
- %FTD-4-751015: Local:localIP:port Remote:remotelP:port Username: username/group SA request rejected by CAC. Reason: reason
- %FTD-4-751016: Local:localIP:port Remote:remotelP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!
- %FTD-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.
- %FTD-4-751021: Local:variable 1:variable 2 Remote:variable 3:variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.
- %FTD-4-751027: Local:local IP:local port Remote:peer IP:peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn’t match the negotiated policy in the SA. Packet destination pkt_daddr, port pkt_dest_port, source pkt_saddr, port pkt_src_port, protocol pkt_proto.
- %FTD-4-752009: IKEv2 Doesn't support Multiple Peers
- %FTD-4-752010: IKEv2 Doesn't have a proposal specified
- %FTD-4-752011: IKEv1 Doesn't have a transform set specified
- %FTD-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
• %FTD-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
• %FTD-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number. Unsupported configuration.
• %FTD-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>
• %FTD-4-768003: SSH: connection timed out: username username, IP ip
• %FTD-4-769009: UPDATE: Image booted image_name is different from boot images.
• %FTD-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.
• %FTD-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.
• %FTD-4-775002: Reason - protocol connection conn_id from interface_name:real_address/real_port [(idfw_user)] to interface_name:real_address/real_port is action locally
• %FTD-4-802006: IP ip_address MDM request details has been rejected: details.

Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

• %FTD-5-109012: AuthenSessionEnd: user ‘user’, sid number, elapsed number seconds
• %FTD-5-109029: Parsing downloaded ACL: string
• %FTD-5-109039: AAA Authentication: Dropping an unsupported IPv6/IP46/IP64 packet from lifc:laddr to fifc:faddr
• %FTD-5-111001: Begin configuration: IP_address writing to device
• %FTD-5-111002: Begin configuration: IP_address reading from device
• %FTD-5-111003: IP_address Erase configuration
• %FTD-5-111004: IP_address end configuration: {FAILED|OK}
• %FTD-5-111005: IP_address end configuration: OK
• %FTD-5-111007: Begin configuration: IP_address reading from device.
• %FTD-5-111008: User user executed the command string
• %FTD-5-111010: User username, running application-name from IP ip addr, executed cmd
• %FTD-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate
• %FTD-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip
• %FTD-5-119001: Reload command executed from Telnet (remote IP_address).
• %FTD-5-119017: syslog
• %FTD-5-212009: Configuration request for SNMP group groupname failed. User username, reason.
• %FTD-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_port
• %FTD-5-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc:sip/sport to dest_ifc:dp/dport
• %FTD-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dst_port [(idfw_user)] denied due to NAT reverse path failure.
• %FTD-5-321001: Resource var1 limit of var2 reached.

Cisco Firepower Threat Defense Syslog Messages
- %FTD-5-321002: Resource var1 rate limit of var2 reached.
- FTD-5-331002: Dynamic DNS type RR for ('fqdn_name' - ip_address | ip_address - 'fqdn_name') successfully updated in DNS server dns_server_ip
- %FTD-5-332003: Web Cache IP_address/service_ID acquired
- %FTD-5-333002: Timeout waiting for EAP response - context:EAP-context
- %FTD-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %FTD-5-334002: EAPoUDP association successfully established - host-address
- %FTD-5-334003: EAPoUDP association failed to establish - host-address
- %FTD-5-334005: Host put into NAC Hold state - host-address
- %FTD-5-334006: EAPoUDP failed to get a response from host - host-address
- %FTD-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg
- %FTD-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %FTD-5-425005 Interface interface_name become active in redundant interface redundant_interface_name
- %FTD-5-4302310: SCTP packet received from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port contains unsupported Hostname Parameter.
- %FTD-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally
- %FTD-5-500001: ActiveX content in java script is modified: src src_ip dest dest_ip on interface interface_name
- %FTD-5-500002: Java content in java script is modified: src src_ip dest dest_ip on interface interface_name
- %FTD-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address/source_port to dest_address/dest_port, flags: tcp_flags, on interface interface_name
- %FTD-5-501101: User transitioning priv level
- %FTD-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %FTD-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %FTD-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %FTD-5-502111: New group policy added: name: policy_name Type: policy_type
- %FTD-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %FTD-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason
- %FTD-5-503002: The last key has expired for interface nameif, packets sent using last valid key.
- %FTD-5-503003: Packet sent | received on interface nameif with expired Key ID key-id.
- %FTD-5-503004: Key ID key-id in key chain key-chain-name does not have a key.
- FTD-5-503005: Key ID key-id in key chain key-chain-name does not have a cryptographic algorithm.
- %FTD-5-504001: Security context context_name was added to the system
- %FTD-5-504002: Security context context_name was removed from the system
- %FTD-5-505001: Module module_id is shutting down. Please wait...
- %FTD-5-505002: Module ips is reloading. Please wait...
- %FTD-5-505003: Module module_id is resetting. Please wait...
- %FTD-5-505004: Module module_id shutdown is complete.
- %FTD-5-505005: Module module_name is initializing control communication. Please wait...
- %FTD-5-505006: Module module_id is Up.
- %FTD-5-505007: Module module_id is recovering. Please wait...
- %FTD-5-505008: Module module_id software is being updated to vnewver (currently vver)
- %FTD-5-505009: Module module_id software was updated to vnewver (previously vver)
• %FTD-5-505010: Module in slot slot removed.
• %FTD-5-505012: Module module_id, application stopped application, version version
• %FTD-5-505013: Module module_id application changed from: application version version to:
  new application version new version.
• %FTD-5-506001: event_source_string event_string
• %FTD-5-507001: Terminating TCP-Proxy connection from interface inside:source_address/source_port
to interface outside:dest_address/dest_port - reassembly limit of limit bytes exceeded
• %FTD-5-509001: Connection attempt from src_intf:src_ip/src_port [[idfw_user | FQDN_string], sg_info]
to dst_intf:dst_ip/dst_port [[idfw_user | FQDN_string], sg_info] was prevented by "no forward" command.
• %FTD-5-503101: Process %id, Nbr %i on %s from %s to %s, %s
• %FTD-5-611004: Serial console idle timeout exceeded
• %FTD-5-612001: Auto Update succeeded: filename, version: number
• %FTD-5-711005: Traceback: call_stack
• %FTD-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
• %FTD-5-713010: IKE area: failed to find centry for message Id message_number
• %FTD-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number, IKE Peer IP_address
  local Proxy Address IP_address, remote Proxy Address IP_address, Crypto map (crypto map tag)
• %FTD-5-713049: Security negotiation complete for tunnel_type type (group_name) Initiator/Responder,
  Inbound SPI = SPI, Outbound SPI = SPI
• %FTD-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy
  IP_address, Local Proxy IP_address
• %FTD-5-713068: Received non-routine Notify message: notify_type (notify_value)
• %FTD-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger_value to
  smaller_value seconds
• %FTD-5-713074: Responder forcing change of IPSec rekeying duration from larger_value to smaller_value
  Kbs
• %FTD-5-713075: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value
  seconds
• %FTD-5-713076: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value Kbs
• %FTD-5-713092: Failure during phase 1 rekeying attempt due to collision
• %FTD-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
• %FTD-5-713119: Group group IP ip PHASE 1 COMPLETED
• %FTD-5-713120: PHASE 2 COMPLETED (msgid=msgid)
• %FTD-5-713130: Received unsupported transaction mode attribute: attribute id
• %FTD-5-713131: Received unknown transaction mode attribute: attribute_id
• %FTD-5-713135: message received, redirecting tunnel to IP_address.
• %FTD-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
• %FTD-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
• %FTD-5-713139: group_name not found, using BASE GROUP default preshared key
• %FTD-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type
  attribute_value correction
• %FTD-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete
  static route for address: IP_address, mask: netmask
• %FTD-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a
  previous failure. Resetting any Backup Server init.
• %FTD-5-713156: Initializing Backup Server [server_name or IP_address]
• %FTD-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
• %FTD-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
• %FTD-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload
• %FTD-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Origininate Only - Possible misconfiguration!
• %FTD-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.
• %FTD-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
• %FTD-5-713201: Duplicate Phase Phase packet detected. Action
• %FTD-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed
• %FTD-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
• %FTD-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.
• %FTD-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
• %FTD-5-713250: META-DATA Received unknown Internal Address attribute: attribute
• %FTD-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
• %FTD-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.
• %FTD-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4
• %FTD-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason
• %FTD-5-713904: Descriptive_event_string.
• %FTD-5-716053: SSO Server added: name: name Type: type
• %FTD-5-716054: SSO Server deleted: name: name Type: type
• %FTD-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
• %FTD-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
• %FTD-5-717050: SCEP Proxy: Processed request type type from IP client ip address, User username, TunnelGroup tunnel_group name, GroupPolicy group-policy name to CA IP ca ip address
• %FTD-5-717053: Group group name User user name IP Address Periodic certificate authentication succeeded. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
• %FTD-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name. Request Type type Mode mode
• %FTD-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial
• %FTD-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal
• %FTD-5-718002: Create peer IP_address failure, already at maximum of number_of_peers
• %FTD-5-718005: Fail to send to IP_address, port port
• %FTD-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]
• %FTD-5-718007: Socket open failure failure_code
• %FTD-5-718008: Socket bind failure failure_code
• %FTD-5-718009: Send HELLO response failure to IP_address
• %FTD-5-718010: Sent HELLO response to IP_address
• %FTD-5-718011: Send HELLO request failure to IP_address
• %FTD-5-718012: Sent HELLO request to IP_address
• %FTD-5-718014: Master peer IP_address is not answering HELLO
• %FTD-5-718015: Received HELLO request from IP_address
• %FTD-5-718016: Received HELLO response from IP_address
• %FTD-5-718024: Send CFG UPDATE failure to IP_address
• %FTD-5-718028: Send OOS indicator failure to IP_address
• %FTD-5-718031: Received OOS obituary for IP_address
• %FTD-5-718032: Received OOS indicator from IP_address
• %FTD-5-718033: Send TOPOLOGY indicator failure to IP_address
• %FTD-5-718042: Unable to ARP for IP_address
• %FTD-5-718043: Updating/removing duplicate peer entry IP_address
• %FTD-5-718044: Deleted peer IP_address
• %FTD-5-718045: Created peer IP_address
• %FTD-5-718048: Create of secure tunnel failure for peer IP_address
• %FTD-5-718050: Delete of secure tunnel failure for peer IP_address
• %FTD-5-718052: Received GRAT-ARP from duplicate master MAC_address
• %FTD-5-718053: Detected duplicate master, mastership stolen MAC_address
• %FTD-5-718054: Detected duplicate master MAC_address and going to SLAVE
• %FTD-5-718055: Detected duplicate master MAC_address and staying MASTER
• %FTD-5-718057: Queue send failure from ISR, msg type failure_code
• %FTD-5-718060: Inbound socket select fail: context=context_ID.
• %FTD-5-718061: Inbound socket read fail: context=context_ID.
• %FTD-5-718062: Inbound thread is awake (context=context_ID).
• %FTD-5-718063: Interface interface_name is down.
• %FTD-5-718064: Admin. interface interface_name is down.
• %FTD-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB_state, master=IP_address, session=Enable/Disable).
• %FTD-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.
• %FTD-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.
• %FTD-5-718068: Start VPN Load Balancing in context context_ID.
• %FTD-5-718069: Stop VPN Load Balancing in context context_ID.
• %FTD-5-718070: Reset VPN Load Balancing in context context_ID.
• %FTD-5-718071: Terminate VPN Load Balancing in context context_ID.
• %FTD-5-718072: Becoming master of Load Balancing in context context_ID.
• %FTD-5-718073: Becoming slave of Load Balancing in context context_ID.
• %FTD-5-718074: Fail to create access list for peer context_ID.
• %FTD-5-718075: Peer IP_address access list not set.
• %FTD-5-718076: Fail to create tunnel group for peer IP_address.
• %FTD-5-718077: Fail to delete tunnel group for peer IP_address.
• %FTD-5-718078: Fail to create crypto map for peer IP_address.
• %FTD-5-718079: Fail to delete crypto map for peer IP_address.
• %FTD-5-718080: Fail to create crypto policy for peer IP_address.
• %FTD-5-718081: Fail to delete crypto policy for peer IP_address.
• %FTD-5-718082: Fail to create crypto ipsec for peer IP_address.
• %FTD-5-718083: Fail to delete crypto ipsec for peer IP_address.
Cisco Firepower Threat Defense Syslog Messages

520

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address
- %FTD-5-718085: Interface interface_name has no IP address defined.
- %FTD-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.
- %FTD-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.
- %FTD-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.
- %FTD-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %FTD-5-720017: (VPN-unit) Failed to update LB runtime data.
- %FTD-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %FTD-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %FTD-5-720020: (VPN-unit) Failed to send type timer message.
- %FTD-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number. HA error code.
- %FTD-5-720035: (VPN-unit) Fail to look up CTCP flow handle.
- %FTD-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %FTD-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %FTD-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %FTD-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %FTD-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %FTD-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.
- %FTD-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.
- %FTD-5-722010: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %FTD-5-722011: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %FTD-5-722012: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %FTD-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.
- %FTD-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.
- %FTD-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.
- %FTD-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.
- %FTD-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %FTD-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %FTD-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.
- %FTD-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.
- %FTD-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names
- %FTD-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'
- %FTD-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'
- %FTD-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'
- %FTD-5-737008: IPAA: 'tunnel-group' not found
- %FTD-5-737011: IPAA: AAA assigned address ip-address, not permitted, retrying
System Health and Network Diagnostic Messages Listed by Severity Level

Cisco Firepower Threat Defense Syslog Messages

- %FTD-5-737018: IPAA: DHCP request attempt num failed
- %FTD-5-737021: IPAA: Address from local pool (ip-address) duplicates address from DHCP
- %FTD-5-737022: IPAA: Address from local pool (ip-address) duplicates address from AAA
- %FTD-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address
- %FTD-5-737024: IPAA: Local pool assignment failed for suggested IP ip-address, retrying
- %FTD-5-737025: IPAA: Not releasing local pool ip-address, due to local pool duplicate issue
- %FTD-5-737034: IPAA: Session=<session>, <IP version> address: <explanation>
- % FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message
- % FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message
- %FTD-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete.
- %FTD-5-746015: user-identity: [FQDN] fqdn resolved IP address.
- %FTD-5-747003: Clustering: Recovered from state machine failure to process event (event-id, ptr-in-hex, ptr-in-hex) at state state-name.
- %FTD-5-748001: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change
- %FTD-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery
- %FTD-5-750001: Local:local IP:local port Remote:remote IP: remote port Username: username Received request to request an IPsec tunnel; local traffic selector = local selectors: range, protocol, port range; remote traffic selector = remote selectors: range, protocol, port range
- %FTD-5-750002: Local:local port Remote:remote IP: remote port Username: username Received a IKE_INIT_SA request
- %FTD-5-750004: Local:local IP:local port Remote:remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS
- %FTD-5-750005: Local:local IP:local port Remote:remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI
- %FTD-5-750008: Local:local IP:local port Remote:remote IP: remote port Username: username SA rejected due to system resource low
- %FTD-5-750009: Local:local IP:local port Remote:remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason
- %FTD-5-750010: Local:local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance
- %FTD-5-750013-IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>. Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>
Informational Messages, Severity 6

The following messages appear at severity 6, informational:

- %FTD-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %FTD-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %FTD-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port)(idfw_user, sg_info) interface_name/dest_address(dest_port) (idfw_user, sg_info) hit-cnt number {first hit | number-second interval}
- %FTD-6-106102: access-list acl_ID {permitted | denied} protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number {first hit | number-second interval} hash codes
- %FTD-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username.
- %FTD-6-109100: Received CoA update from coa-source-ip for user username, with session ID: audit-session-id, changing authorization attributes
- %FTD-6-109101: Received CoA disconnect request from coa-source-ip for user username, with audit-session-id: audit-session-id
- %FTD-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %FTD-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %FTD-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone/parent_outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) to inside_zone/parent_inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port)
- %FTD-6-113003: AAA group policy for user user is being set to policy_name.
- %FTD-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
• %FTD-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user: user IP = user_ip
• %FTD-6-113006: User user locked out on exceeding number successive failed authentication attempts
• %FTD-6-113007: User user unlocked by administrator
• %FTD-6-113008: AAA transaction status ACCEPT: user = user
• %FTD-6-113009: AAA retrieved default group policy policy for user user
• %FTD-6-113010: AAA challenge received for user user from server server_IP_address
• %FTD-6-113011: AAA retrieved user specific group policy policy for user user
• %FTD-6-113012: AAA user authentication Successful: local database: user = user
• %FTD-6-113013: AAA unable to complete the request Error: reason = reason: user = user
• %FTD-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
• %FTD-6-113015: AAA user authentication Rejected: reason = reason: local database: user = user: user IP =xxx.xxx.xxx.xxx
• %FTD-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user: user IP = xxx.xxx.xxx.xxx
• %FTD-6-113017: AAA credentials rejected: reason = reason: local database: user = user: user IP = user_ip=xxx.xxx.xxx.xxx
• %FTD-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. ACL parse error.
• %FTD-6-113037: Reboot pending, new sessions disabled. Denied user login.
• %FTD-6-113039: Group group User user IP ipaddr AnyConnect parent session started.
• %FTD-6-114004: 4GE SSM I/O Initialization start.
• %FTD-6-114005: 4GE SSM I/O Initialization end.
• %FTD-6-199002: startup completed. Beginning operation.
• %FTD-6-199003: Reducing link MTU dec.
• %FTD-6-199005: Startup begin
• %FTD-6-199018: syslog
• %FTD-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
• %FTD-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input/output] packet from IP_address/ port to ip/port on interface interface_name
• %FTD-6-210022: LU missed number updates
• %FTD-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
• %FTD-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
• %FTD-6-302010: connections in use, connections most used
• %FTD-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
• %FTD-6-302013: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
• %FTD-6-302014: Teardown TCP connection_id for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes bytes [reason] [(user)]
• %FTD-6-302015: Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] to interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] [(user)]
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-6-302016: Teardown UDP connection number for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes [(user)]
- %FTD-6-302017: Built {inbound|outbound} GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] [(user)]
- %FTD-6-302018: Teardown GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] duration hh:mm:ss bytes [(user)]
- %FTD-6-302020: Built ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %FTD-6-302021: Teardown ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %FTD-6-302022: Built role stub TCP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %FTD-6-302023: Teardown stub TCP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %FTD-6-302024: Built role stub UDP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %FTD-6-302025: Teardown stub UDP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %FTD-6-302026: Built role stub ICMP connection for interface:real-address/real-port (mapped-address) to interface:real-address/real-port (mapped-address)
- %FTD-6-302027: Teardown stub ICMP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %FTD-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- %FTD-6-302303: Built TCP state-bypass connection conn_id from initiator_interface:real_ip/real_port(mapped_ip/mapped_port) to responder_interface:real_ip/real_port (mapped_ip/mapped_port)
- %FTD-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface:ip/port to responder_interface:ip/port duration,bytes,teardown reason.
- %FTD-6-303002: FTP connection from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port, user username action file filename
- %FTD-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user)] to interface_name:mapped_address
- %FTD-6-305010: Teardown {dynamic|static} translation from interface_name:real_address [(idfw_user)] to interface_name:mapped_address duration time
- %FTD-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name:real_address/real_port [(idfw_user)] to interface_name:mapped_address/mapped_port
- %FTD-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface_name [(acl-name)]:real_address/real_port[real_ICMP_ID] [(idfw_user)] to interface_name:mapped_address/mapped_port[mapped_ICMP_ID] duration time
- %FTD-6-308001: console enable password incorrect for number tries (from IP_address)
- %FTD-6-311001: LU loading standby start
- %FTD-6-311002: LU loading standby end
- %FTD-6-311003: LU recv thread up

System Health and Network Diagnostic Messages Listed by Severity Level
%FTD-6-311004: LU xmit thread up
%FTD-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name
%FTD-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.
%FTD-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port: reason_string.
%FTD-6-317007: Added route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
%FTD-6-317008: Deleted route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
%FTD-6-321003: Resource var1 log level of var2 reached.
%FTD-6-321004: Resource var1 rate log level of var2 reached
%FTD-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface_in:source_address/source_port to interface_out:dest_address/dest_port
%FTD-6-333001: EAP association initiated - context:EAP-context
%FTD-6-333003: EAP association terminated - context:EAP-context
%FTD-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
%FTD-6-334001: EAPoUDP association initiated - host-address
%FTD-6-334004: Authentication request for NAC Clientless host - host-address
%FTD-6-334007: EAPoUDP association terminated - host-address
%FTD-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
%FTD-6-334009: Audit request for NAC Clientless host - Assigned_IP.
%FTD-6-336011: event event
%FTD-6-337000: Created BFD session with local discriminator id on real_interface with neighbor real_host_ip.
%FTD-6-337001: Terminated BFD session with local discriminator id on real_interface with neighbor real_host_ip due to failure_reason.

%FTD-6-340002: Loopback-proxy info: error_string context id context_id, context_type = version/request_type/address_type client_socket (internal)= client_address_internal/client_port_internal server_socket (internal)= server_address_internal/server_port_internal server_socket (external)= server_address_external/server_port_external remote_socket (external)= remote_address_external/remote_port_external
%FTD-6-341001: Policy Agent started successfully for VNMC vnmc_ip_add
%FTD-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_add
%FTD-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no
%FTD-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
%FTD-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number= 0x7B) from 75.2.96.101 (user= user) to 85.2.96.10 with incorrect IPsec padding
%FTD-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name.
%FTD-6-419004: TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> is probed by DCD
%FTD-6-419005: TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> duration <hh:mm:ss> data <bytes>, is kept open by DCD as valid connection
• %FTD-6-419006: Teardown TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> duration <hh:mm:ss> data <bytes>, DCD probe was not responded from <client/server> interface <ifc_name>

• %FTD-6-421006: There are number users of application accounted during the past 24 hours.

• %FTD-6-425001 Redundant interface redundant_interface_name created.

• %FTD-6-425002 Redundant interface redundant_interface_name removed.

• %FTD-6-425003 Interface interface_name added into redundant interface redundant_interface_name.

• %FTD-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.

• %FTD-6-426001: PORT-CHANNEL: Interface ifc_name bundled into EtherChannel interface Port-channel num

• %FTD-6-426002: PORT-CHANNEL: Interface ifc_name unbundled from EtherChannel interface Port-channel num

• %FTD-6-426003: PORT-CHANNEL: Interface ifc_name1 has become standby in EtherChannel interface Port-channel num

• %FTD-6-426101: PORT-CHANNEL: Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP

• %FTD-6-426102: PORT-CHANNEL: Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP

• %FTD-6-426103: PORT-CHANNEL: Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP

• %FTD-6-426104: PORT-CHANNEL: Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP

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

• %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.

• %FTD-7-703001: H.225 message received from interface_name:IP_address/port is using an unsupported version number

• %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.

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

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

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

• %FTD-6-604102: DHCP client interface interface_name: address released

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

• %FTD-6-604104: DHCP daemon interface interface_name: address released build_name (IP_address)

• %FTD-6-605004: Login denied from source-address/source-port to interface:destination/service for user “username”

• %FTD-6-605005: Login permitted from source-address/source-port to interface:destination/service for user “username”

• %FTD-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
• %FTD-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message
• %FTD-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
• %FTD-6-611301: VPN Client: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address
• %FTD-6-611302: VPN Client: NAT exemption configured for Network Extension Mode with no split tunneling
• %FTD-6-611303: VPN Client: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask
• %FTD-6-611304: VPN Client: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask
• %FTD-6-611305: VPN Client: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
• %FTD-6-611306: VPN Client: Perfect Forward Secrecy Policy installed
• %FTD-6-611307: VPN Client: Head end: IP_address
• %FTD-6-611308: VPN Client: Split DNS Policy installed: List of domains: string string
• %FTD-6-611309: VPN Client: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address
• %FTD-6-611310: VPN Client: XAUTH Succeeded: Peer: IP_address
• %FTD-6-611311: VPN Client: XAUTH Failed: Peer: IP_address
• %FTD-6-611312: VPN Client: Backup Server List: reason
• %FTD-6-611314: VPN Client: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address
• %FTD-6-611315: VPN Client: Disconnecting from Load Balancing Cluster member IP_address
• %FTD-6-611316: VPN Client: Secure Unit Authentication Enabled
• %FTD-6-611317: VPN Client: Secure Unit Authentication Disabled
• %FTD-6-611318: VPN Client: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time
• %FTD-6-611319: VPN Client: User Authentication Disabled
• %FTD-6-611320: VPN Client: Device Pass Thru Enabled
• %FTD-6-611321: VPN Client: Device Pass Thru Disabled
• %FTD-6-611322: VPN Client: Extended XAUTH conversation initiated when SUA disabled
• %FTD-6-611323: VPN Client: Duplicate split nw entry
• %FTD-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
• %FTD-6-613002: interface interface_name has zero bandwidth
• %FTD-6-613003: IP_address netmask changed from area string to area string
• %FTD-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string %FTD-6-613027: OSPF process number removed from interface interface_name
• %FTD-6-613028: Unrecognized virtual interface interface_name. Treat it as loopback stub route
• %FTD-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge
• %FTD-6-613043:
• %FTD-6-613101: Checksum Failure in database in area %s\n Link State Id %i Old Checksum %#x New Checksum %#x\n
• %FTD-6-613102: interface %s has zero bandwidth
• %FTD-6-613103: %s\n changed from area %AREA_ID_STR to area %AREA_ID_STR
• %FTD-6-613104: Unrecognized virtual interface %IF_NAME.
• %FTD-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
• %FTD-6-614002: Split DNS: reply from server: IP_address reverse patched back to original server: IP_address
• %FTD-6-615001: vlan number not available for firewall interface
• %FTD-6-615002: vlan number available for firewall interface
• %FTD-6-621001: Interface interface_name does not support multicast, not enabled
• %FTD-6-621002: Interface interface_name does not support multicast, not enabled
• %FTD-6-621003: The event queue size has exceeded number
• %FTD-6-621006: Mrib disconnected, (IP_address, IP_address) event cancelled
• %FTD-6-621007: Bad register from interface_name:IP_address to IP_ADDRESS for (IP_address, IP_address)
• %FTD-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
• %FTD-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries
• %FTD-6-622102: Completed regex table compilation for match_command; table size = num bytes
• %FTD-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
• %FTD-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
• %FTD-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
• %FTD-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
• %FTD-6-713172: Automatic NAT Detection Status: Remote end is is not behind a NAT device This end is is not behind a NAT device
• %FTD-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
• %FTD-6-713184: Client Type: Client_type Client Application Version: Application_version_string
• %FTD-6-713202: Duplicate IP_addr packet detected.
• %FTD-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
• %FTD-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
• %FTD-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
• %FTD-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
• %FTD-6-713228: Assigned private IP address assigned_private_IP
• %FTD-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
• %FTD-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
• %FTD-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len
• %FTD-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
• %FTD-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: /prefix_len
• %FTD-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: /prefix_len
• %FTD-6-713905: Descriptive_event_string.
• %FTD-6-716001: Group group User user WebVPN session started.
• %FTD-6-716002: Group group User user WebVPN session terminated: reason.
• %FTD-6-716003: Group group User user WebVPN access GRANTED: url
• %FTD-6-716004: Group group User user WebVPN access DENIED to specified location: url
• %FTD-6-716005: Group group User user WebVPN ACL Parse Error: reason
• %FTD-6-716006: Group name User user WebVPN session terminated. Idle timeout.
• %FTD-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
• %FTD-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
• %FTD-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
• %FTD-6-716039: Authentication: rejected, group = name user = user, Session Type: %s
• %FTD-6-716040: Reboot pending, new sessions disabled. Denied user login.
• %FTD-6-716041: access-list acl_ID action url url hit_cnt count
• %FTD-6-716042: access-list acl_ID action tcp source_interface/source_address (source_port) - dest_interface/dest_address(dest_port) hit-cnt count
• %FTD-6-716043 Group group-name, User user-name, IP IP_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings
• %FTD-6-716049: Group-name User user-name IP IP_address Empty SVC ACL.
• %FTD-6-716050: Error adding to ACL: ace_command_line
• %FTD-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
• %FTD-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded
• %FTD-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.
• %FTD-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2
• %FTD-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.
• %FTD-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
• %FTD-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
• %FTD-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
• %FTD-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
• %FTD-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
• %FTD-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
• %FTD-6-717022: Certificate was successfully validated. certificate_identifiers
• %FTD-6-717028: Certificate chain was successfully validated additional info.
• %FTD-6-717033: OCSP response status - Successful.
• %FTD-6-717056: Attempting type revocation check from Src Interface:Sr Port to Ds IP/Ds Port using protocol
• %FTD-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number
• %FTD-6-718004: Got unknown internal message message_number
• %FTD-6-718013: Peer IP_address is not answering HELLO
• %FTD-6-718027: Received unexpected KEEPALIVE request from IP_address
• %FTD-6-718030: Received planned OOS from IP_address
• %FTD-6-718037: Master processed number_of_timeouts timeouts
• %FTD-6-718038: Slave processed number_of_timeouts timeouts
%FTD-6-718039: Process dead peer IP_address
%FTD-6-718040: Timed-out exchange ID exchange_ID not found
%FTD-6-718051: Deleted secure tunnel to peer IP_address
%FTD-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
%FTD-6-719003: Email Proxy session pointer resources have been freed for source_address.
%FTD-6-719004: Email Proxy session pointer has been successfully established for source_address.
%FTD-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
%FTD-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.
%FTD-6-719012: Email Proxy server listening on port port for mail protocol protocol.
%FTD-6-719013: Email Proxy server closing port port for mail protocol protocol.
%FTD-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
%FTD-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found
%FTD-6-719019: WebVPN user: vpnuser authorization failed.
%FTD-6-719020: WebVPN user vpnuser authorization completed successfully.
%FTD-6-719021: WebVPN user: vpnuser is not checked against ACL.
%FTD-6-719022: WebVPN user vpnuser has been authenticated.
%FTD-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
%FTD-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
%FTD-6-719025: Email Proxy DNS name resolution failed for hostname.
%FTD-6-719026: Email Proxy DNS name hostname resolved to IP_address.
%FTD-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
%FTD-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
%FTD-6-720004: (VPN-unit) VPN failover main thread started.
%FTD-6-720005: (VPN-unit) VPN failover timer thread started.
%FTD-6-720006: (VPN-unit) VPN failover sync thread started.
%FTD-6-720010: (VPN-unit) VPN failover client is being disabled
%FTD-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.
%FTD-6-722013: Group group Useruser-nameIPIP_addressSVCMessage:type-num/INFO:message
%FTD-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
%FTD-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his).
%FTD-6-720023: (VPN-unit) HA status callback: Peer is not present.
%FTD-6-720024: (VPN-unit) HA status callback: Control channel is status.
%FTD-6-720025: (VPN-unit) HA status callback: Data channel is status.
%FTD-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
%FTD-6-720027: (VPN-unit) HA status callback: My state state.
%FTD-6-720028: (VPN-unit) HA status callback: Peer state state.
%FTD-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
%FTD-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
%FTD-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence #, grp=group, event=event, op=operand, my=my_state, peer=peer_state.
%FTD-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence number,grp=group,event=event,op=operand, my=my_state,peer=peer_state.
%FTD-6-720039: (VPN-unit) VPN failover client is transitioning to active state
%FTD-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
%FTD-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
%FTD-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
%FTD-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
%FTD-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
%FTD-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
%FTD-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
%FTD-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
%FTD-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
%FTD-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
%FTD-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
%FTD-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
%FTD-6-721002: (device) HA status change: event event, my state my_state, peer state peer.
%FTD-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.
%FTD-6-721004: (device) Create access list list_name on standby unit.
%FTD-6-721005: (device) Fail to create access list list_name on standby unit.
%FTD-6-721006: (device) Update access list list_name on standby unit.
%FTD-6-721008: (device) Delete access list list_name on standby unit.
%FTD-6-721009: (device) Fail to delete access list list_name on standby unit.
%FTD-6-721010: (device) Add access list rule list_name, line line_no on standby unit.
%FTD-6-721012: (device) Enable APCF XML file file_name on the standby unit.
%FTD-6-721014: (device) Disable APCF XML file file_name on the standby unit.
%FTD-6-721016: (device) WebVPN session for client user_user_name, IP ip_address has been created.
%FTD-6-721018: (device) WebVPN session for client user_user_name, IP ip_address has been deleted.
%FTD-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
%FTD-6-722014: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
%FTD-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
%FTD-6-722053: Group g User u IP ip Unknown client user-agent connection.
%FTD-6-722055: Group group-policy User username IP public-ip Client Type: user-agent
%FTD-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.
%FTD-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.
%FTD-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session.
%FTD-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session
%FTD-6-725003: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port request to resume previous session.
%FTD-6-725004: Device requesting certificate from SSL peer-type interface:src-ip/src-port to dst-ip/dst-port for authentication.
%FTD-6-725005: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port requesting our device certificate for authentication.
%FTD-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port
%FTD-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated.
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc:/sip/sport to dest_ifc:/dip/dport Action: action Matched Class class_map_id class_map_name
- %FTD-6-725016: Device selects trust-point <trustpoint> for peer-type interface:src-ip/src-port to dst-ip/dst-port
- %FTD-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %FTD-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %FTD-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %FTD-6-737009: IPAA: AAA assigned address ip-address, request failed
- %FTD-6-737010: IPAA: AAA assigned address ip-address, request succeeded
- %FTD-6-737014: IPAA: Freeing AAA address ip-address
- %FTD-6-737015: IPAA: Freeing DHCP address ip-address
- %FTD-6-737016: IPAA: Freeing local pool address ip-address
- %FTD-6-737017: IPAA: DHCP request attempt num succeeded
- %FTD-6-737026: IPAA: Client assigned ip-address from local pool
- %FTD-6-737029: IPAA: Adding ip-address to standby: succeeded
- %FTD-6-737031: IPAA: Removing %m from standby: succeeded
- %FTD-6-737036: IPAA: Session=<session>, Client assigned <address> from DHCP
- % FTD-6-737205: VPNFIP: Pool=pool, INFO: message
- % FTD-6-737406: POOLIP: Pool=pool, INFO: message
- %FTD-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB
- %FTD-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB
- %FTD-6-741002: Coredump log and filesystem contents cleared on variable 1
- %FTD-6-741003: Coredump filesystem and its contents removed on variable 1
- %FTD-6-741004: Coredump configuration reset to default values
- %FTD-6-747004: Clustering: state machine changed from state state-name to state-name.
- %FTD-6-747044: Clustering: Configuration Hash string verification <result>.
- %FTD-6-748008: [CPU load percentage | memory load percentage ] of module slot_number in chassis chassis_number (member-name ) exceeds overflow protection threshold [CPU percentage | memory percentage ]. System may be oversubscribed on member failure.
- %FTD-6-748009: [CPU load percentage | memory load percentage] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage]. System may be oversubscribed on chassis failure.
- %FTD-6-751023: Local a:p Remote: a:p Username:n Unknown client connection
- %FTD-6-767001: Inspect-name: Dropping an unsupported IPv6/IP46/IP64 packet from interface:IP Addr to interface:IP Addr (fail-close)
- %FTD-6-769007: UPDATE: Image version is version_number
- %FTD-6-772005: REAUTH: user username passed authentication
- %FTD-6-776251: CTS SGT-MAP: Binding binding IP - SName (SGT ) from source name added to binding manager.
• %FTD-6-776253: CTS SGT-MAP: Binding binding IP - new SGname (SGT) from new source name changed from old sgt: old SGname (SGT) from old source old source name.

• %FTD-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port).

• %FTD-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.

• %FTD-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.

• %FTD-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.

• %FTD-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.

• %FTD-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.

• %FTD-6-778007: VXLAN: Packet from ifc-name:IP-address/port to IP-address/port was discarded due to invalid NVE peer.

• %FTD-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name:IP-address/port to IP-address/port.

• %FTD-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id, protocol from ifc-name:IP-address/port to IP-address/port

• %FTD-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction

• %FTD-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction

• %FTD-6-780003: RULE ENGINE: Started compilation for nat transaction - description of the transaction

• %FTD-6-780004: RULE ENGINE: Finished compilation for nat transaction - description of the transaction

• %FTD-6-802005: IP ip_address Received MDM request details.

• %FTD-6-803001: Bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

• %FTD-6-803002: No protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

• %FTD-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2

• %FTD-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted

• %FTD-6-804002: Interface GigabitEthernet1/3 SFP has been removed

• %FTD-6-805001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol

• %FTD-6-805002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol

• %FTD-6-805003: Flow could not be offloaded: connection <conn_id> <outside_ifc>:<outside_addr>/<outside_port> (<mapped_addr>/<mapped_port>) <inside_ifc>:<inside_addr>/<inside_port> (<mapped_addr>/<mapped_port>) <Protocol>

• %FTD-6-852001: Received Lightweight to Full Proxy event from application Snort for TCP flow ip-address/port to ip-address/port

• %FTD-6-852002: Received Full Proxy to Lightweight event from application Snort for TCP flow ip-address/port to ip-address/port

• %FTD-6-8300001: VPN session redistribution <variable 1>

• %FTD-6-8300002: Moved <variable 1> sessions to <variable 2>
• %FTD-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

• %FTD-7-110009: User user executed cmd:string
• %FTD-7-113028: Extraction of username from VPN client certificate has string. [Request num]
• %FTD-7-199019: syslog
• %FTD-7-333004: EAP-SQ response invalid - context:EAP-context
• %FTD-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
• %FTD-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
• %FTD-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
• %FTD-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
• %FTD-7-609001: Built local-host zone_name/*/ip_address
• %FTD-7-609002: Teardown local-host zone_name/*/ ip_address duration time
• %FTD-7-701001: alloc_user() out of Tcp_user objects
• %FTD-7-701002: alloc_user() out of Tcp_proxy objects
• %FTD-7-702307: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.
• %FTD-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
• %FTD-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
• %FTD-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d
• %FTD-7-709001: FO replication failed: cmd=command returned=code
• %FTD-7-709002: FO unreplicable: cmd=command
• %FTD-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
• %FTD-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
• %FTD-7-710004: TCP connection limit exceeded from Src_ip/Src_port to In_name:Dest_ip/Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)
• %FTD-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
• %FTD-7-710006: protocol request discarded from source_address to interface_name:dest_address
• %FTD-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500
• %FTD-7-711001: debug_trace_msg
• %FTD-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.
• %FTD-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string.
• %FTD-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
• %FTD-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
• %FTD-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level
- %FTD-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port (“Received remote IP Proxy Subnet data in ID Payload: Address %a, Mask/%d, Protocol %u, Port %u”)
- %FTD-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed
- %FTD-7-713906: Descriptive_event_string.
- %FTD-7-714001: description_of_event_or_packet
- %FTD-7-714002: IKE Initiator starting QM: msg id = message_number
- %FTD-7-714003: IKE Responder starting QM: msg id = message_number
- %FTD-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %FTD-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %FTD-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %FTD-7-714007: IKE Initiator sending Initial Contact
- %FTD-7-714011: Description of received ID values
- %FTD-7-715001: Descriptive statement
- %FTD-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %FTD-7-715005: subroutine name() Bad message code: Code (message_code)
- %FTD-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %FTD-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %FTD-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %FTD-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %FTD-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %FTD-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name
- %FTD-7-715020: construct_cfg_set: Attribute name = name
- %FTD-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %FTD-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %FTD-7-715027: IPSec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPSec SA entry # crypto_map_index
- %FTD-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index
- %FTD-7-715033: Processing CONNECTED notify (MsgId message_number)
- %FTD-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %FTD-7-715035: Starting IOS keepalive monitor: seconds sec.
- %FTD-7-715036: Sending keep-alive of type notify_type (seq number number)
- %FTD-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %FTD-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %FTD-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %FTD-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %FTD-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %FTD-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %FTD-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %FTD-7-715045: ERROR: malformed Keepalive payload
- %FTD-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload
- %FTD-7-715047: processing payload_description payload
• %FTD-7-715048: Send VID_type VID
• %FTD-7-715049: Received VID_type VID
• %FTD-7-715050: Claims to be IOS but failed authentication
• %FTD-7-715051: Received unexpected TLV_type TLV_type while processing FWTYPE ModeCfg Reply
• %FTD-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centres
• %FTD-7-715053: MODE_CFG: Received request for attribute_info!
• %FTD-7-715054: MODE_CFG: Received attribute_name reply: value
• %FTD-7-715055: Send attribute_name
• %FTD-7-715056: Client is configured for TCP_transparency
• %FTD-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
• %FTD-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
• %FTD-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
• %FTD-7-715060: Dropped received IKE fragment. Reason: reason
• %FTD-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
• %FTD-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
• %FTD-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
• %FTD-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false
  Aggressive Mode: true/false
• %FTD-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
• %FTD-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
• %FTD-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
• %FTD-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
• %FTD-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
• %FTD-7-715069: Invalid ESP SPI size of SPI_size
• %FTD-7-715070: Invalid IPComp SPI size of SPI_size
• %FTD-7-715071: AH proposal not supported
• %FTD-7-715072: Received proposal with unknown protocol ID protocol_ID
• %FTD-7-715074: Could not retrieve authentication attributes for peer IP_address
• %FTD-7-715075: Group = group_name, IP = IP_address Received keep-alive of type message_type (seq number number)
• %FTD-7-715076: Computing hash for ISAKMP
• %FTD-7-715077: Pitcher: msg string, spi spi
• %FTD-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.
• %FTD-7-716008: WebVPN ACL: action
• %FTD-7-716010: Group group User user Browse network.
• %FTD-7-716011: Group group User user Browse domain domain.
• %FTD-7-716012: Group group User user Browse directory directory.
• %FTD-7-716013: Group group User user Close file filename.
• %FTD-7-716014: Group group User user View file filename.
• %FTD-7-716015: Group group User user Remove file filename.
• %FTD-7-716016: Group group User user Rename file old_filename to new_filename.
• %FTD-7-716017: Group group User user Modify file filename.
Cisco Firepower Threat Defense Syslog Messages

System Health and Network Diagnostic Messages Listed by Severity Level

- %FTD-7-716018: Group group User user Create file filename.
- %FTD-7-716019: Group group User user Create directory directory.
- %FTD-7-716020: Group group User user Remove directory directory.
- %FTD-7-716021: File access DENIED, filename.
- %FTD-7-716024: Group name User user Unable to browse the network. Error: description
- %FTD-7-716025: Group name User user Unable to browse domain domain. Error: description
- %FTD-7-716026: Group name User user Unable to browse directory directory. Error: description
- %FTD-7-716027: Group name User user Unable to view file filename. Error: description
- %FTD-7-716028: Group name User user Unable to remove file filename. Error: description
- %FTD-7-716029: Group name User user Unable to rename file filename. Error: description
- %FTD-7-716030: Group name User user Unable to modify file filename. Error: description
- %FTD-7-716031: Group name User user Unable to create file filename. Error: description
- %FTD-7-716032: Group name User user Unable to create folder folder. Error: description
- %FTD-7-716033: Group name User user Unable to remove folder folder. Error: description
- %FTD-7-716034: Group name User user Unable to write to file filename.
- %FTD-7-716035: Group name User user Unable to read file filename.
- %FTD-7-716036: Group name User user File Access: User user logged into the server server.
- %FTD-7-716037: Group name User user File Access: User user failed to login into the server server.
- %FTD-7-716038: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %FTD-7-716039: Found a suitable trustpoint trustpoint name to validate certificate.
- %FTD-7-716040: No-check extension found in certificate. OCSP check bypassed.
- %FTD-7-716041: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %FTD-7-716042: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %FTD-7-716043: Internal interprocess communication queue send failure: code error_code
- %FTD-7-716044: Got timeout for unknown peer IP_address msg type message_type
- %FTD-7-716045: Send KEEPALIVE request failure to IP_address msg type message_type
- %FTD-7-716046: Sent KEEPALIVE request to IP_address
- %FTD-7-716047: Sent KEEPALIVE response failure to IP_address
- %FTD-7-716048: Sent KEEPALIVE response to IP_address
- %FTD-7-716049: Received KEEPALIVE request from IP_address
- %FTD-7-716050: Received KEEPALIVE response from IP_address
- %FTD-7-716051: Sent CFG UPDATE to IP_address
- %FTD-7-716052: Sent CFG UPDATE from IP_address
- %FTD-7-716053: Sent OOS indicator to IP_address
- %FTD-7-716054: Sent TOPOLOGY indicator to IP_address
- %FTD-7-716055: Received TOPOLOGY indicator from IP_address
- %FTD-7-716056: Process timeout for req-type type_value, exid exchange_ID, peer IP_address
- %FTD-7-716057: Timeout [msgType=type] processed with no callback
- %FTD-7-716058: Create group policy policy_name
- %FTD-7-716059: Fail to create group policy policy_name
• %FTD-7-718049: Created secure tunnel to peer IP_address
• %FTD-7-718056: Deleted Master peer, IP IP_address
• %FTD-7-718058: State machine return code: actionRoutine, returnCode
• %FTD-7-718059: State machine function trace: state=state_name, event=event_name, func=actionRoutine
• %FTD-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.
• %FTD-7-719005: FSM NAME has been created using protocol for session pointer from source_address.
• %FTD-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.
• %FTD-7-719007: Email Proxy session pointer cannot be found for source_address.
• %FTD-7-719009: Email Proxy service is starting.
• %FTD-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server
• %FTD-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass = ******
• %FTD-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.
• %FTD-7-720034: (VPN-unit) Invalid type (type) for message handler.
• %FTD-7-720041: (VPN-unit) Sending type message id to standby unit
• %FTD-7-720042: (VPN-unit) Receiving type message id from active unit
• %FTD-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=func.
• %FTD-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=func.
• %FTD-7-720050: (VPN-unit) Failed to remove timer. ID = id.
• %FTD-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets
• %FTD-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops
• %FTD-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.
• %FTD-7-723003: No memory for WebVPN Citrix ICA connection connection.
• %FTD-7-723004: WebVPN Citrix encountered bad flow control flow.
• %FTD-7-723005: No channel to set up WebVPN Citrix ICA connection.
• %FTD-7-723006: WebVPN Citrix SOCKS errors.
• %FTD-7-723007: WebVPN Citrix ICA connection connection list is broken.
• %FTD-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
• %FTD-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.
• %FTD-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.
• %FTD-7-723011: Group group-name, User user-name, IP IP_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.
• %FTD-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.
• %FTD-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
• %FTD-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
Variables Used in Syslog Messages

Syslog messages often include variables. The following table lists most variables that are used in this guide to describe syslog messages. Some variables that appear in only one syslog message are not listed.

Variable Fields in Syslog Messages

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| acl_ID   | An ACL name.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>The number of bytes.</td>
</tr>
<tr>
<td>code</td>
<td>A decimal number returned by the syslog message to indicate the cause or source of the error, according to the syslog message generated.</td>
</tr>
<tr>
<td>command</td>
<td>A command name.</td>
</tr>
</tbody>
</table>
| command_modifier | The **command_modifier** is one of the following strings:  
|               | • cmd (this string means the command has no modifier)  
|               | • clear  
|               | • no  
|               | • show |
| connections   | The number of connections.                                                  |
| connection_type | The connection type:  
|               | • SIGNALLING UDP  
|               | • SIGNALLING TCP  
|               | • SUBSCRIBE UDP  
|               | • SUBSCRIBE TCP  
|               | • Via UDP  
|               | • Route  
|               | • RTP  
<p>|               | • RTCP |
| dec           | Decimal number.                                                             |
| dest_address  | The destination address of a packet.                                        |
| dest_port     | The destination port number.                                                |
| device        | The memory storage device. For example, the floppy disk, internal flash memory, TFTP, the failover standby unit, or the console terminal. |
| econns        | Number of embryonic connections.                                            |
| elimit        | Number of embryonic connections specified in the <strong>static</strong> or <strong>nat</strong> command. |
| filename      | A filename of the type ASAimage, ASDM file, or configuration.               |
| ftp-server    | External FTP server name or IP address.                                     |
| gateway_address | The network gateway IP address.                                           |
| global_address | Global IP address, an address on a lower security level interface.          |
| global_port   | The global port number.                                                    |
| hex           | Hexadecimal number.                                                         |
| inside_address | Inside (or local) IP address, an address on a higher security level interface. |</p>
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inside_port</td>
<td>The inside port number.</td>
</tr>
<tr>
<td>interface_name</td>
<td>The name of the interface.</td>
</tr>
<tr>
<td>IP_address</td>
<td>IP address in the form n n n n , where n is an integer from 1 to 255.</td>
</tr>
<tr>
<td>MAC_address</td>
<td>The MAC address.</td>
</tr>
<tr>
<td>mapped_address</td>
<td>The translated IP address.</td>
</tr>
<tr>
<td>mapped_port</td>
<td>The translated port number.</td>
</tr>
<tr>
<td>message_class</td>
<td>Category of syslog message associated with a functional area of the ASA.</td>
</tr>
<tr>
<td>message_list</td>
<td>Name of a file you create containing a list of syslog message ID numbers, classes, or severity levels.</td>
</tr>
<tr>
<td>message_number</td>
<td>The syslog message ID.</td>
</tr>
<tr>
<td>nconns</td>
<td>Number of connections permitted for the static or xlate table.</td>
</tr>
<tr>
<td>netmask</td>
<td>The subnet mask.</td>
</tr>
<tr>
<td>number</td>
<td>A number. The exact form depends on the syslog message.</td>
</tr>
<tr>
<td>octal</td>
<td>Octal number.</td>
</tr>
<tr>
<td>outside_address</td>
<td>Outside (or foreign) IP address, an address of a syslog server typically on a lower security level interface in a network beyond the outside router.</td>
</tr>
<tr>
<td>outside_port</td>
<td>The outside port number.</td>
</tr>
<tr>
<td>port</td>
<td>The TCP or UDP port number.</td>
</tr>
<tr>
<td>privilege_level</td>
<td>The user privilege level.</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol of the packet, for example, ICMP, TCP, or UDP.</td>
</tr>
<tr>
<td>real_address</td>
<td>The real IP address, before NAT.</td>
</tr>
<tr>
<td>real_port</td>
<td>The real port number, before NAT.</td>
</tr>
<tr>
<td>reason</td>
<td>A text string describing the reason for the syslog message.</td>
</tr>
<tr>
<td>service</td>
<td>The service specified by the packet, for example, SNMP or Telnet.</td>
</tr>
<tr>
<td>severity_level</td>
<td>The severity level of a syslog message.</td>
</tr>
<tr>
<td>source_address</td>
<td>The source address of a packet.</td>
</tr>
<tr>
<td>source_port</td>
<td>The source port number.</td>
</tr>
<tr>
<td>string</td>
<td>Text string (for example, a username).</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>tcp_flags</td>
<td>Flags in the TCP header such as:</td>
</tr>
<tr>
<td></td>
<td>• ACK</td>
</tr>
<tr>
<td></td>
<td>• FIN</td>
</tr>
<tr>
<td></td>
<td>• PSH</td>
</tr>
<tr>
<td></td>
<td>• RST</td>
</tr>
<tr>
<td></td>
<td>• SYN</td>
</tr>
<tr>
<td></td>
<td>• URG</td>
</tr>
<tr>
<td>time</td>
<td>Duration, in the format hh mm ss</td>
</tr>
<tr>
<td>url</td>
<td>A URL.</td>
</tr>
<tr>
<td>user</td>
<td>A username.</td>
</tr>
</tbody>
</table>
INDEX

4GE SSM 64, 73

A

AAA v, 41, 42, 50, 51, 52, 53, 54, 171, 235, 352, 353, 354
authentication 53, 353
messages 41, 42, 50, 51, 52, 53, 54, 171, 235
server v, 42, 53, 352, 353, 354

ABR 118
without backbone area 118
access lists 309
See ACLs 309
access permittedUDP 238
access permittedTCP 238
access permitted
access requestedTCP 237
access requested
access-list command 39, 40, 41
deny-flow-max optionaccess-list deny-flow-max command 40
interval option 39
omitting 41
access-list commandaccess-list commandaccess-list commandaccess-list command
34, 39, 107
to permit traffic on UDP port 53 34
to permit traffic on UDP port 53access-list command 34, 39, 107
ACLs 38, 39, 40, 41, 42, 54, 107, 247, 257, 270, 302, 303, 309, 346, 348, 352, 353
ACL ID 309
compilation out of memory 38
configuration error 42
crypto map 247
deny 107
deny-flows 40
empty ACL downloaded 41
logging matches 39
no ACL configured 270
packet denied 38
parsing error 42
peer context ID 346
peer context IDaccess-list commandaccess-list commandaccess-list command
346
to permit traffic on UDP port 53 346
peer IP address not set 346
proxy ID mismatch 270
SoftNP error 348

ACLs (continued)

split tunneling policy 257
unsupported format 54
WebVPN 302, 303, 352, 353
ACL ID not found 353
parse error 302, 303, 352
user authorization failure 353
address translation slots 164
no more available 164
anchor count negative 142
area border router 118
See ABR 118
ARP packet mismatch 163
ARP poisoning attackattacks 163
ARP poisoning 163
ARP spoofing attack
asymmetric routing 37
attacks 127
ARP spoofing 127
spoofing 127
Authen Session End 41
authorization 217
user 217
Auto Update URL unreachable 223

B

backup server list 220
downloadedEasy VPN Remote 220
backup server list 220
downloaded 220
errorEasy VPN Remote 220
backup server list 220
error 220
bridge table 178
full 178
broadcast, invalid source address 36
built H245 connection 99

C

cannot specify PAT host 35
certificate data could not be verified 324
classes, logging v
message class variables v
classes, logging (continued)
types v
clear command 166
local-host option 166
config command config command 49
configuration 49, 177, 236
erase 49
replication 236
beginning 236
failed 236
status changed 177
configure command configure command 49
connection event 1
connection limit exceeded 82, 83
connection limit exceeded TCP 238, 534
connection limit exceeded

D
deny 34, 35, 36
inbound from outside 34
inbound ICMP 35
inbound UDP 34
inbound UDP due to query/response 34
IP from address to address 35
IP spoof 36
self route 35
TCP (no connection) 35
device pass through 222
disabled Easy VPN Remote 222
device pass through 222
disabled 222
enabled Easy VPN Remote 222
device pass through 222
enabled 222
DNS query or response is denied 34
DNS server too slow 34
DoS attack attacks 40, 85, 166
DoS 40, 85, 166

E
Easy VPN Remote 222
SUA 222
disabled 222
embryonic limit exceeded 81
event (security) 1
connection 1
intrusion 1
security intelligence 1

F
bad cable 23
block allocation failed 29
cable communication failed 29
cable not connected 23
cable status 24
configuration replication 29
configuration replication failed 237
continuous failovers 31
failover active command 360
failover command message dropped 30
incompatible software on mate 31
interface link down 32
LAN interface down 30
license mismatch with mate 32
lost communications with mate 28
mate card configuration mismatch 33
mate has different chassis 33
mate may be disabled 31
operational mode mismatch with mate 32
peer LAN link down 30
replication interrupted 31
show failover command 364
standby unit failed to sync 29
stateful error 86
stateful failover 86, 87, 88
VPN failover 355, 356, 357, 358, 359, 362, 363, 365
buffer error 358
client being disabled 356
CTCP flow handle error 362
failed to allocate chunk 356
failed to initialize 355
memory allocation error 357
non-block message not sent 359
registration failure 356
SDI node secret file failed to synchronize 365
standby unit received corrupted message from active
unit 363
state update message failure 362
timer error 358
trustpoint certification failure 357
trustpoint name not found 359
unable to add to message queue 362
version control block failure 356
failover command 26, 30, 360
active option 360
active option failover command 26
active option failover command
active option 26
failover command failover command 27
failover messages 23, 24, 236
failover message testing 28
interface 28
Flood Defender 235
flow control error 141
FTP 82
data connection failed 82

H
H.225 165
H.245 connection 99
foreign address H.245H.245 99
H.323 235
unsupported packet version 235
H.323H.323 99
back-connection, preallocated 99
handle not allocated 141
hello packet with duplicate router ID OSPF 170
hello packet with duplicate router ID 170
host limit 166
host move 177
hostile event 36
firewall circumvented hostile event 36

I
ICMP 35
packet denied conduit command 35
permit ICMP option 35
packet denied dropping echo request 35
IDB initialization OSPF 119
IDB initialization 119
inbound TCP connection denied 33
insufficient memory 164
error caused by 164
interface 224
zero bandwidth bandwidth 224
reported as zero 224
Internet phone, detecting use of detecting use of Internet phone 99
intrusion event 1
invalid source addresses 36
IP address 211
DHCP client 211
DHCP server 211
IP route counter decrement failure 167
IP routing table 40, 116, 119
attack 40
IP routing table 40
creation error 116
limit exceeded 116
limit warning 116
OSPF inconsistency OSPF 119
IP routing table inconsistency 119
ip verify reverse-path command 37
ip verify reverse-path command ip verify reverse-path command 37

IPSec 50, 51, 52, 53, 54, 107, 115, 242, 245, 246, 247, 248, 249, 250, 251,
252, 253, 260, 263, 264, 290, 291, 296, 298, 299, 322, 323, 341, 342,
367
connection entries 252
connections 51, 52, 53, 54, 323
failure 323
cTCP tunnel 367
encryption 290
fragmentation policy ignored 264
negotiation 247
over UDP 260, 296
over TCP 296
packet triggered IKE 245
proposal 299
SA 299
unsupported protocol 299
proxy mismatch 107
rekeying duration 248, 249
request rejected 253
SA 247, 250, 251, 253, 290, 291, 298
proposal 298
tunnels 50, 115, 246, 263, 322, 323, 341, 342

L
land attacks 36
land 36
link state advertisement 118
See LSA 118
link status Up or Down 28
load balancing cluster 220, 221
load balancing cluster 221
load balancing cluster 220
redirecited Easy VPN Remote 220
load balancing cluster 221
redirecited Easy VPN Remote 221
disconnected Easy VPN Remote 221
lost failover communications with mate 28
LSA 169
default with wrong mask OSPF 169
LSA 169
default with wrong mask 169
invalid type OSPF 169
LSA 169
invalid type 169

MAC address mismatch 164
man in the middle attack attacks 125
man in the middle 125
memory 29, 116, 118, 223
block depleted 29
corruption OSPF 223
checksum error 223
leak LSA 118
not found OSPF 118
LSA 118
not found 118
low memory low memory 116
failed operation 116
message block alloc failed 29
messages 86, 87, 88, 540
stateful failover 86, 87, 88
variables used in 540
messages, logging v
classes v
list of v

N
no associated connection within connection table TCP 35
no associated connection in table 35

O
OSPF 118, 168, 169, 198, 224
ABR without backbone area 118
configuration change 224
database request from unknown neighbor OSPF 168
database description from unknown neighbor OSPF 168
hello from unknown neighbor 168
invalid packet 168
neighbor state changed 198
network range area changed 224
packet of invalid length 169
outbound deny command outbound deny command 34

P
packet 34, 35, 38
denied 34, 35, 38
PAT 35, 164
address 164
global address 35
host unspecified 35
pdb index error 116
preallocate H323 UDP back connection 99
privilege level, changed 197

R
RCMD, back connection failed 82
reload command reload command 49, 77
request discarded UDP 239
request discarded TCP 239
request discarded 239
router ID allocation failure OSPF 169
router ID allocation failure 169
rsh command rsh command rsh command 82

S
security 35, 38, 199
breach 35
c context 38, 199
added 199
context cannot be determined 38
removed 199
security event 1
security intelligence event 1
self route 35
SETUP message 165
Severity level 4 192
ASA-4-447001 192
show command 29, 34, 81, 82, 88, 166, 364
blocks option show command 29
blocks option 29
failover option 88, 364
local-host option 166
outbound option show command 34
outbound option 34
static option show command 81, 82
static option 82
static option show static command 81
version option 166
shuns 152
SIP connection 215
skinny connection 216
software version mismatch 179
split network entry duplicate Easy VPN Remote 222
split network entry duplicate 222
spoofing attack attacks 36, 37, 164
spoofing 36, 37, 164
SSM 4GE 64, 73
stateful failover 86, 87, 88
SUA 221
disabled Easy VPN Remote
SUA 221
disabled 221
enabled Easy VPN Remote
SUA 221
enabled 221
SYN 81
attack attacks 81
SYN 81
SYNSYN 35
flag 35

Cisco Firepower Threat Defense Syslog Messages
### T

- **TCP** 238
  - connections 238
- TCP state-bypass connection creation 107
- TCP state-bypass connection teardown 107
- timeout uauth command timeout uauth command 41
- timeouts, recommended values 166
- too many connections on static connection limit exceeded 81

### UDP

- 34, 109, 238
  - connections 238
  - messages 109
  - packet 34
- unsupported application 179
- user authentication 221
  - disabled EasyVPN Remote 221
  - user authentication disabled 221
  - enabled EasyVPN Remote 221
  - user authentication enabled 221
- user logged out 218
- username 197
  - created 197
  - deleted 197

### V

- variables 540
  - in messages 540
  - messages messages 540
  - variables used in list of 540
- virtual links OSPF 119
  - virtual links router-ID reset OSPF 119
  - router-id reset OSPF 119
  - process reset 119
- VPN 115
  - peer limit 115
  - tunnel 115
- VPN failover 355, 356, 357, 358, 359, 362, 363, 365
  - client being disabled 356
  - CTCP flow handle error 362
  - failed to allocate chunk 356
  - failed to initialize 355
  - memory allocation error 357
  - non-block message not sent 359
  - registration failure 356
  - SDI node secret file failed to synchronize 365
  - standby unit received corrupted message from active unit 363
  - state update message failure 362
  - timer error 358
  - trustpoint certification failure 357
  - trustpoint name not found 359
  - unable to add to message queue 362
  - version control block failure 356

### W

- write command 49, 87, 88
  - erase option 49
  - standby command 88
  - standby option 87
- write command write command 49
  - write erase command write erase command 49

### X

- XAUTH enabled EasyVPN Remote 222
  - XAUTH enabled 222