重大度別システムヘルスおよびネットワーク診断メッセージリスト

この付録の内容は、次のとおりです。

アラート メッセージ、重大度 1

次のメッセージが重大度 1（アラート）で表示されます。

- %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-1-103008: Mate hwdib index is not compatible.
- %Threat Defense-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %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-1-105022: (host) Config replication failed with reason = (reason)
- %FTD-1-105031: Failover LAN interface is up
- %FTD-1-105032: 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 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 0xf132e03b, corrective action at 0xca1961a0
- %Threat Defense-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
- %FTD-1-735020: CPU var1: Temp: var2 var3 OK
- %FTD-1-735021: Chassis var1: Temp: var2 var3 OK
- %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.
- %FTD-1-735024: IO Hub var1: Temp: var2 var3, OK
- %FTD-1-735025: IO Hub var1: Temp: var2 var3, Critical
- %FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。
- %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.
- %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.
- %FTD-1-743001: Backplane health monitoring detected link failure
- %FTD-1-743002: Backplane health monitoring detected link OK
- %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
- %Threat Defense-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.

クリティカル メッセージ、重大度 2

次のメッセージが重大度 2（クリティカル）で表示されます。

- %Threat Defense-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
- %Threat Defense-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
- %Threat Defense-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %Threat Defense-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.
- %Threat Defense-2-106013: Dropping echo request from IP_address to PAT address IP_address
- %Threat Defense-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- %Threat Defense-2-106017: Deny IP due to Land Attack from IP_address to IP_address

- %Threat Defense-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
- %Threat Defense-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
- %Threat Defense-2-106024: Access rules memory exhausted
- %Threat Defense-2-108003: Terminating ESMTP/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
- %Threat Defense-2-109011: Authen Session Start: user 'user', sid number
- %Threat Defense-2-112001: (string:dec) Clear complete.
- %Threat Defense-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
- %Threat Defense-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %Threat Defense-2-113027: Username could not be found in certificate
- %Threat Defense-2-115000: Critical assertion in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %Threat Defense-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.
- %Threat Defense-2-199014: syslog
- %Threat Defense-2-199020: System memory utilization has reached X%. System will reload if memory usage reaches the configured trigger level of Y%.
- %Threat Defense-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
- %Threat Defense-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %Threat Defense-2-215001:Bad route_compress() call, sdb= number
- %Threat Defense-2-217001: No memory for string in string
- %Threat Defense-2-218001: Failed Identification Test in slot# [fail#/res].
- %Threat Defense-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %Threat Defense-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.
- %Threat Defense-2-218004: Failed Identification Test in slot# [fail#/res]
- %Threat Defense-2-218005: Inconsistency detected in the system information programmed in non-volatile memory
- %Threat Defense-2-321005: System CPU utilization reached utilization %

- %Threat Defense-2-321006: System memory usage reached utilization %
- %Threat Defense-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
- %Threat Defense-2-709007: Configuration replication failed for command command
- %Threat Defense-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
- %Threat Defense-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %Threat Defense-2-713901: Descriptive_text_string.
- %Threat Defense-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %Threat Defense-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %Threat Defense-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %Threat Defense-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %Threat Defense-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %Threat Defense-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %Threat Defense-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER
- %Threat Defense-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %Threat Defense-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %Threat Defense-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %Threat Defense-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
- %Threat Defense-2-716520: internal error in: function: OCCAM pool has no block list
- %Threat Defense-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %Threat Defense-2-716522: internal error in: function: OCCAM corrupted standalone block
- %Threat Defense-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED
- %Threat Defense-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL
- %Threat Defense-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAI
- %Threat Defense-2-717008: Insufficient memory to process_requiring_memory.
- %Threat Defense-2-717011: Unexpected event event event_ID
- %Threat Defense-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.

- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.
- %Threat Defense-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name.
- %Threat Defense-2-747011: Clustering: Memory allocation error.
- %Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record.
- %Threat Defense-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number; traffic may be black holed
- %Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record.
- %Threat Defense-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %Threat Defense-2-772006: REAUTH: user username failed authentication
- %Threat Defense-2-774001: POST: unspecified error
- %Threat Defense-2-774002: POST: error err, func func, engine eng, algorithm alg, mode mode, dir dir, key len len

エラー メッセージ、重大度 3

次のメッセージが重大度 3（エラー）で表示されます。

- %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-3-109203: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed adding entry.
- %FTD-3-109205: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed applying filter.
- %FTD-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.
- %FTD-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.
- %FTD-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.
- %FTD-3-109212: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed removing entry.
- %FTD-3-109213: UAUTH Session *session*, User *username*, Assigned IP *IP Address* Failed removing entry.
- %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
- %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:outside_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 - nameif-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 network IP_address mask netmask protocol hex attr hex net-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 occured when attemtping 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
- %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 vnewver (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 firware 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 desination_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 rdbs
- %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. 終了するまでに数分かかる場合があります。
- %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_adddress/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
- %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
- %Threat Defense-3-520025: No memory for radix initialization: error_msg
- %Threat Defense-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
- %Threat Defense-3-613029: Router-ID IP_address is in use by ospf process number
- %Threat Defense-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.
- %Threat Defense-3-613032: Init failed for interface inside, area is being deleted. 再度お試しください。
- %Threat Defense-3-613033: Interface inside is attached to more than one area
- %FTD-3-613034: Neighbor IP_address not configured
- %Threat Defense-3-613035: Could not allocate or find neighbor IP_address
- %Threat Defense-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
- %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: Invalid certificate handle
- %FTD-3-713084: Received invalid phase 1 port value (port) in ID payload
- %FTD-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %FTD-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %FTD-3-713088: Set Cert file handle failure: no IPSec SA in group group_name
- %FTD-3-713098: Aborting: No identity cert specified in IPSec SA (SA_name)!
- %FTD-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %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: Failed to process CONNECTED notify (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-3-713118: Detected invalid Diffie-Helmann group_descriptor group_number, in IKE area
- %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-3-713132: 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-3-713138: 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: 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
- %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
- %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-3-713198: User Authorization failed: user User authorization failed.
- %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
- %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_dh_cb = 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-3-713258: 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.
- %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_addres>, 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 IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection
- %FTD-3-716158: Failed to create SAML logout request, initiated by SP. Reason: *reason*
- %FTD-3-716159: Failed to process SAML logout request, initiated by SP. Reason: *reason*
- %FTD-3-716160: Failed to create SAML authentication request. Reason: *reason*
- %FTD-3-716162: Failed to consume SAML assertion. Reason: *reason*

- %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 onthe 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-3-717009: Certificate validation failed. 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.
- %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-3-717032: OCSP status check failed. Reason: 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 IP ip 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: POOLIP: 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-3-747001: Clustering: Recovered from state machine event queue depleted. Event (event-id, ptr-in-hex, ptr-in-hex) dropped. Current state state-name, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex
- %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-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed. Session ID: sessionID, Error: error

- %FTD-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed. Error: error
- %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-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start/rem-ts-end/rem-ts.startport/rem-ts.endport/rem-ts.protocol local traffic selector local-ts-start/local-ts-end/local-ts.startport/local-ts.endport/local-ts.protocol!
- %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>
- %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>
- %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)
- %FTD-3-8300003: Failed to send session redistribution message to <variable 1>
- %FTD-3-8300005: Failed to receive session move response from <variable 1>

警告メッセージ、重大度 4

次のメッセージが重大度 4（警告）で表示されます。

- %Threat Defense-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]
- %Threat Defense-4-106027: Deny src [source address] dst [destination address] by access-group “access-list name”.
- %Threat Defense-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
- %Threat Defense-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %Threat Defense-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.

- %Threat Defense-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol connections
- %Threat Defense-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
- %Threat Defense-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id
- %Threat Defense-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %Threat Defense-4-113026: Error error while executing Lua script for group tunnel group
- %Threat Defense-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached
- %Threat Defense-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.
- %Threat Defense-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.
- %Threat Defense-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.
- %Threat Defense-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.
- %Threat Defense-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
- %Threat Defense-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.
- %Threat Defense-4-113038: Group group User user IP ipaddr Unable to create AnyConnect p0arent session.
- %Threat Defense-4-113040: Terminating the VPN connection attempt from attempted group. Reason: This connection is group locked to locked group.
- %Threat Defense-4-113041: Redirect ACL configured for assigned IP does not exist on the device.
- %Threat Defense-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.
- %Threat Defense-4-115002: Warning in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %Threat Defense-4-199016: syslog
- %Threat Defense-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
- %Threat Defense-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number

- %Threat Defense-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %Threat Defense-4-209006: Fragment queue threshold exceeded, dropped TCP fragment from IP address/port to IP address/port on outside interface.
- %Threat Defense-4-216004: prevented: error in function at file(line) - stack trace
- %Threat Defense-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign address/foreign-port to laddr interface:local-address/local-port
- %Threat Defense-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].
- %Threat Defense-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address
- %Threat Defense-4-313004: Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- %Threat Defense-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/dest_port [(idfw_user|FQDN_string), sg_info]
- %Threat Defense-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
- %Threat Defense-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-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

- %Threat Defense-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
- %Threat Defense-4-401001: Shuns cleared
- %Threat Defense-4-401002: Shun added: IP_address IP_address port port
- %Threat Defense-4-401003: Shun deleted: IP_address
- %Threat Defense-4-401004: Shunned packet: IP_address = IP_address on interface interface_name
- %Threat Defense-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port
- %Threat Defense-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.
- %Threat Defense-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.
- %Threat Defense-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.
- %Threat Defense-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed authentication.
- %Threat Defense-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).
- %Threat Defense-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).
- %Threat Defense-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command.
- %Threat Defense-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).
- %Threat Defense-4-402125: The ASA hardware accelerator ring timed out (parameters).
- %Threat Defense-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.

- %Threat Defense-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.
- %Threat Defense-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.
- %Threat Defense-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
- %Threat Defense-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name
- %Threat Defense-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
- %Threat Defense-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
- %Threat Defense-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name, MAC_address.
- %Threat Defense-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %Threat Defense-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %Threat Defense-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex
- %Threat Defense-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP
- %Threat Defense-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest
- %Threat Defense-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name
- %Threat Defense-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
- %Threat Defense-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded
- %Threat Defense-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
- %Threat Defense-4-407003: Established limit for RPC services exceeded number
- %Threat Defense-4-408001: IP route counter negative - reason, IP_address Attempt: number
- %Threat Defense-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %Threat Defense-4-408003: can't track this type of object hex

- %Threat Defense-4-408101: KEYMAN : Type <encrption_type> encryption unknown. Interpreting keystring as literal.
- %Threat Defense-4-408102: KEYMAN : Bad encrypted keystring for key id <key id>
- %Threat Defense-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls
- %Threat Defense-4-409002: db_free: external LSA IP_address netmask
- %Threat Defense-4-409003: Received invalid packet: reason from IP_address, interface_name
- %Threat Defense-4-409004: Received reason from unknown neighbor IP_address
- %Threat Defense-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name
- %Threat Defense-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name
- %Threat Defense-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask
- %Threat Defense-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string
- %Threat Defense-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %Threat Defense-4-409010: Virtual link information found in non-backbone area: string
- %Threat Defense-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %Threat Defense-4-409012: Detected router with duplicate router ID IP_address in area string
- %Threat Defense-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %Threat Defense-4-409014: No valid authentication *send* key is available on interface *nameif*.
- %Threat Defense-4-409015: Key ID *key-id received* on interface *nameif*.
- %Threat Defense-4-409016: Key chain name *key-chain-name* on *nameif* is invalid.
- %Threat Defense-4-409017: Key ID *key-id* in key chain *key-chain-name* is invalid.
- %Threat Defense-4-409023: Attempting AAA Fallback method method_name for request_type request for user user:Auth-server group server_tag unreachable
- %Threat Defense-4-409101: Received invalid packet: %s from %P, %s
- %Threat Defense-4-409102: Received packet with incorrect area from %P, %s, area %AREA_ID_STR, packet area %AREA_ID_STR
- %Threat Defense-4-409103: Received %s from unknown neighbor %i
- %Threat Defense-4-409104: Invalid length %d in OSPF packet type %d from %P (ID %i), %s
- %Threat Defense-4-409105: Invalid lsa: %s: Type 0x%x, Length 0x%x, LSID %u from %i

- %Threat Defense-4-409106: Found generating default LSA with non-zero mask LSA type: 0x%x Mask: %i metric: %lu area: %AREA_ID_STR
- %Threat Defense-4-409107: OSPFv3 process %d could not pick a router-id, please configure manually
- %Threat Defense-4-409108: Virtual link information found in non-backbone area: %AREA_ID_STR
- %Threat Defense-4-409109: OSPF detected duplicate router-id %i from %P on interface %IF_NAME
- %Threat Defense-4-409110: Detected router with duplicate router ID %i in area %AREA_ID_STR
- %Threat Defense-4-409111: Multiple interfaces (%IF_NAME /%IF_NAME) on a single link detected.
- %Threat Defense-4-409112: Packet not written to the output queue
- %Threat Defense-4-409113: Doubly linked list linkage is NULL
- %Threat Defense-4-409114: Doubly linked list prev linkage is NULL %x
- %Threat Defense-4-409115: Unrecognized timer %d in OSPF %s
- %Threat Defense-4-409116: Error for timer %d in OSPF process %s
- %Threat Defense-4-409117: Can't find LSA database type %x, area %AREA_ID_STR, interface %x
- %Threat Defense-4-409118: Could not allocate DBD packet
- %Threat Defense-4-409119: Invalid build flag %x for LSA %i, type 0x%x
- %Threat Defense-4-409120: Router-ID %i is in use by ospf process %d
- %Threat Defense-4-409121: Router is currently an ASBR while having only one area which is a stub area
- %Threat Defense-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.
- %Threat Defense-4-409123: Neighbor command allowed only on NBMA networks
- %Threat Defense-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %Threat Defense-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
- %Threat Defense-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.
- %Threat Defense-4-411001: Line protocol on interface interface_name changed state to up
- %Threat Defense-4-411002: Line protocol on interface interface_name changed state to down
- %Threat Defense-4-411003: Configuration status on interface interface_name changed state to downup
- %Threat Defense-4-411004: Configuration status on interface interface_name changed state to up
- %Threat Defense-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
- %Threat Defense-4-412001: MAC MAC_address moved from interface_1 to interface_2

- %Threat Defense-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
- %Threat Defense-4-413001: Module module_id is not able to shut down. Module Error: errnum message
- %Threat Defense-4-413002: Module module_id is not able to reload. Module Error: errnum message
- %Threat Defense-4-413003: Module module_id is not a recognized type
- %Threat Defense-4-413004: Module module_id failed to write software vnewver (currently vver), reason. Trying again.
- %Threat Defense-4-413005: Module module_id, application is not supported app_name version app_vers type app_type
- %Threat Defense-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.
- %Threat Defense-4-415016: policy-map map_name:Maximum number of unanswered HTTP requests exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %Threat Defense-4-417001: Unexpected event received: number
- %Threat Defense-4-417004: Filter violation error: conn number (string:string) in string
- %Threat Defense-4-417006: No memory for string) in string. Handling: string
- %Threat Defense-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]
- %Threat Defense-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
- %Threat Defense-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.
- %Threat Defense-4-419003: Cleared TCP urgent flag from out_ifc:src_ip/src_port to in_ifc:dest_ip/dest_port.
- %Threat Defense-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1
- %Threat Defense-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %Threat Defense-4-422006: IP SLA Monitor Probe number: string
- %Threat Defense-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.
- %Threat Defense-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port
- %Threat Defense-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).

- %Threat Defense-4-429008: Unable to respond to VPN query from CX for session 0x%x. Reason %s
- %Threat Defense-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
- %Threat Defense-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)
- %Threat Defense-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.
- %Threat Defense-4-447001: ASP DP to CP queue_name was full. Queue length length, limit limit
- %Threat Defense-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
- %Threat Defense-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %Threat Defense-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %Threat Defense-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
- %Threat Defense-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.
- %Threat Defense-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too small
- %Threat Defense-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too large
- %Threat Defense-4-612002: Auto Update failed:filename, version:number, reason:reason
- %Threat Defense-4-612003: Auto Update failed to contact:url, reason:reason
- %Threat Defense-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address
- %Threat Defense-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs
- %Threat Defense-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs
- %Threat Defense-4-613021: Packet not written to the output queue
- %Threat Defense-4-613022: Doubly linked list linkage is NULL
- %Threat Defense-4-613023: Doubly linked list prev linkage is NULL number
- %Threat Defense-4-613024: Unrecognized timer number in OSPF string
- %Threat Defense-4-613025: Invalid build flag number for LSA IP_address, type number

- %Threat Defense-4-613026: Can not allocate memory for area structure
- %Threat Defense-4-613030: Router is currently an ASBR while having only one area which is a stub area
- %Threat Defense-4-613031: No IP address for interface inside
- %Threat Defense-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network
- %Threat Defense-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %Threat Defense-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network
- %Threat Defense-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks
- %Threat Defense-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
- %Threat Defense-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-4-709013: Failover configuration replication hash comparison timeout expired.
- %Threat Defense-4-711002: Task ran for elapsed_time msecs, process = process_name, PC = PC Tracebeback = traceback
- %Threat Defense-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call stack
- %Threat Defense-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %Threat Defense-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %Threat Defense-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %Threat Defense-4-713240: Received DH key with bad length: received length=rlength expected length=elength
- %Threat Defense-4-713241: IE Browser Proxy Method setting_number is Invalid
- %Threat Defense-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %Threat Defense-4-713243: META-DATA Unable to find the requested certificate

- %Threat Defense-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %Threat Defense-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %Threat Defense-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %Threat Defense-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %Threat Defense-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %Threat Defense-4-713249: META-DATA Received unsupported authentication results: result
- %Threat Defense-4-713251: META-DATA Received authentication failure message
- %Threat Defense-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name
- %Threat Defense-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.
- %Threat Defense-4-716007: Group group User user WebVPN Unable to create session.
- %Threat Defense-4-716022: Unable to connect to proxy server reason.
- %Threat Defense-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.
- %Threat Defense-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.
- %Threat Defense-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.
- %Threat Defense-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.
- %Threat Defense-4-716047: Group group-name User user-name IP IP_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %Threat Defense-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.
- %Threat Defense-4-716052: Group group-name User user-name IP IP_address Pending session terminated.
- %Threat Defense-4-717026: Name lookup failed for hostname hostname during PKI operation.
- %Threat Defense-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string
- %Threat Defense-4-717035: OCSP status is being checked for certificate. certificate_identifier.
- %Threat Defense-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.

- %Threat Defense-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
- %Threat Defense-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %Threat Defense-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %Threat Defense-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %Threat Defense-4-720009: (VPN-unit) Failed to create version control block.
- %Threat Defense-4-720011: (VPN-unit) Failed to allocate memory
- %Threat Defense-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name
- %Threat Defense-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %Threat Defense-4-720033: (VPN-unit) Failed to queue add to message queue.
- %Threat Defense-4-720038: (VPN-unit) Corrupted message from active unit.
- %Threat Defense-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %Threat Defense-4-720044: (VPN-unit) Failed to receive message from active unit
- %Threat Defense-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.
- %Threat Defense-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %Threat Defense-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %Threat Defense-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port
- %Threat Defense-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.
- %Threat Defense-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %Threat Defense-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.
- %Threat Defense-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %Threat Defense-4-720066: (VPN-unit) Failed to activate IKE database.
- %Threat Defense-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %Threat Defense-4-720068: (VPN-unit) Failed to parse peer message.
- %Threat Defense-4-720069: (VPN-unit) Failed to activate cTCP database.
- %Threat Defense-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %Threat Defense-4-720073: VPN Session failed to replicate - ACL acl_name not found
- %Threat Defense-4-721007: (device) Fail to update access list list_name on standby unit.

- %Threat Defense-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.
- %Threat Defense-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.
- %Threat Defense-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.
- %Threat Defense-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.
- %Threat Defense-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.
- %Threat Defense-4-722001: IP IP_address Error parsing SVC connect request.
- %Threat Defense-4-722002: IP IP_address Error consolidating SVC connect request.
- %Threat Defense-4-722003: IP IP_address Error authenticating SVC connect request.
- %Threat Defense-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
- %Threat Defense-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num
- %Threat Defense-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length
- %Threat Defense-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
- %Threat Defense-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version
- %Threat Defense-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length
- %Threat Defense-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection
- %Threat Defense-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
- %Threat Defense-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
- %Threat Defense-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
- %Threat Defense-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
- %Threat Defense-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
- %Threat Defense-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
- %Threat Defense-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.

- %Threat Defense-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.
- %Threat Defense-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
- %Threat Defense-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.
- %Threat Defense-4-733102: Threat-detection adds host %I to shun list
- %Threat Defense-4-733103: Threat-detection removes host %I from shun list
- %Threat Defense-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED
- %Threat Defense-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED
- %Threat Defense-4-735015: CPU var1: Temp: var2 var3, Warm
- %Threat Defense-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm
- %Threat Defense-4-735018: Power Supply var1: Temp: var2 var3, Critical
- %Threat Defense-4-735019: Power Supply var1: Temp: var2 var3, Warm
- %Threat Defense-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.
- %Threat Defense-4-737012: IPAA: Address assignment failed
- %Threat Defense-4-737013: IPAA: Error freeing address ip-address, not found
- %Threat Defense-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
- %Threat Defense-4-737028: IPAA: Adding ip-address to standby: failed
- %Threat Defense-4-737030: IPAA: Adding %m to standby: address already in use
- %Threat Defense-4-737032: IPAA: Removing ip-address from standby: not found
- %Threat Defense-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
- %Threat Defense-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3
- %Threat Defense-4-741006: Unable to write Coredump Helper configuration, reason variable 1

- %Threat Defense-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.
- %Threat Defense-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
- %Threat Defense-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.
- %Threat Defense-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
- %Threat Defense-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).
- %Threat Defense-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
- %Threat Defense-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
- %Threat Defense-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).
- %Threat Defense-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.
- %Threat Defense-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).
- %Threat Defense-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.
- %Threat Defense-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled
- %Threat Defense-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure
- %Threat Defense-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
- %Threat Defense-4-748012: Mismatched module type with Master. Master: <PID>, MINE: <PID>
- %Threat Defense-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error
- %Threat Defense-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %Threat Defense-4-750014: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 Session aborted. Reason: Initial Contact received for Local ID: <self ID>, Remote ID: <peer ID> from remote peer:<peer ip>:<peer port> to <self ip>:<self port>
- %Threat Defense-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
- %Threat Defense-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC. Reason: reason

- %Threat Defense-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!
- %Threat Defense-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-4-752009: IKEv2 Doesn't support Multiple Peers
- %Threat Defense-4-752010: IKEv2 Doesn't have a proposal specified
- %Threat Defense-4-752011: IKEv1 Doesn't have a transform set specified
- %Threat Defense-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number. Unsupported configuration.
- %Threat Defense-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>
- %Threat Defense-4-768003: SSH: connection timed out: username username, IP ip
- %Threat Defense-4-769009: UPDATE: Image booted image_name is different from boot images.
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-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
- %Threat Defense-4-802006: IP ip_address MDM request details has been rejected: details.

通知メッセージ、重大度 5

次のメッセージが重大度 5（通知）で表示されます。

- %FTD-5-106029: New reverse carrier <protocol> <ingress_ifc>:<source_addr> to <egress_ifc>:<destination_addr> overshadows existing <ingress_ifc2>:<source_addr2> to <egress_ifc2>:<destination_addr2>
- %FTD-5-109012: Authen Session End: 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-5-109201: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded adding entry.
- %FTD-5-109204: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded applying filter.
- %FTD-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.
- %FTD-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.
- %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-5-199001: Reload command executed from Telnet (remote IP_address).
- %FTD-5-199017: 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_interface
- %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

- %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.
- %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

- %Threat Defense-5-503002: The last key has expired for interface *nameif*, packets sent using last valid key.
- %Threat Defense-5-503003: Packet *sent* | *received* on interface *nameif* with expired Key ID *key-id*.
- %Threat Defense-5-503004: Key ID *key-id* in key chain *key-chain-name* does not have a key.
- Threat Defense-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: newapplication version newversion.
- %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 %d, Nbr %i on %s from %s to %s, %s
- %FTD-5-611104: 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=msg_id)
- %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 Originate 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. アクション
- %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: SAML Server added: name: name Type: SP
- %FTD-5-716054: SAML Server deleted: name: name Type: SP
- %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 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.
- %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
- %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-5-747002: Clustering: Recovered from state machine dropped event (event-id, ptr-in-hex, ptr-in-hex). Intended state: state-name. Current state: state-name.
- %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-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex.
- %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 IP: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-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason
- %FTD-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason
- %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>
- %FTD-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2. Attribute: attribute
- %FTD-5-751025: Local: local IP:local port Remote: remote IP:remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.
- %FTD-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-769001: UPDATE: ASA image src was added to system boot list
- %FTD-5-769002: UPDATE: ASA image src was copied to dest
- %FTD-5-769003: UPDATE: ASA image src was renamed to dest
- %FTD-5-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason
- %FTD-5-769005: UPDATE: ASA image image_name passed image verification
- %FTD-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGname (SGT) from source name deleted from binding manager.
- %FTD-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

情報メッセージ、重大度 6

次のメッセージが重大度 6（情報）で表示されます。

- %Threat Defense-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %Threat Defense-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %Threat Defense-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})

- %Threat Defense-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
- %Threat Defense-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username.
- %Threat Defense-6-109100: Received CoA update from *coa-source-ip* for user *username* , with session ID: *audit-session-id* , changing authorization attributes
- %Threat Defense-6-109101: Received CoA disconnect request from *coa-source-ip* for user *username* , with audit-session-id: *audit-session-id*
- %Threat Defense-6-109202: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded incrementing entry use.
- %Threat Defense-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %Threat Defense-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %Threat Defense-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)
- %Threat Defense-6-113003: AAA group policy for user user is being set to policy_name.
- %Threat Defense-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %Threat Defense-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user: user IP = user_ip
- %Threat Defense-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %Threat Defense-6-113007: User user unlocked by administrator
- %Threat Defense-6-113008: AAA transaction status ACCEPT: user = user
- %Threat Defense-6-113009: AAA retrieved default group policy policy for user user
- %Threat Defense-6-113010: AAA challenge received for user user from server server_IP_address
- %Threat Defense-6-113011: AAA retrieved user specific group policy policy for user user
- %Threat Defense-6-113012: AAA user authentication Successful: local database: user = user
- %Threat Defense-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %Threat Defense-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %Threat Defense-6-113015: AAA user authentication Rejected: reason = reason: local database: user = user: user IP =xxx.xxx.xxx.xxx
- %Threat Defense-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user: user IP = xxx.xxx.xxx.xxx

- %Threat Defense-6-113017: AAA credentials rejected: reason = reason: local database: user = user: user IP = user_ip=xxx.xxx.xxx.xxx
- %Threat Defense-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. ACL parse error.
- %Threat Defense-6-113037: Reboot pending, new sessions disabled. Denied user login.
- %Threat Defense-6-113039: Group group User user IP ipaddr AnyConnect parent session started.
- %Threat Defense-6-114004: 4GE SSM I/O Initialization start.
- %Threat Defense-6-114005: 4GE SSM I/O Initialization end.
- %Threat Defense-6-199002: startup completed. Beginning operation.
- %Threat Defense-6-199003: Reducing link MTU dec.
- %Threat Defense-6-199005: Startup begin
- %Threat Defense-6-199018: syslog
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-6-210022: LU missed number updates
- %Threat Defense-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
- %Threat Defense-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %Threat Defense-6-302010: connections in use, connections most used
- %Threat Defense-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
- %Threat Defense-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)]
- %Threat Defense-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)]
- %Threat Defense-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)]
- %Threat Defense-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 bytes [(user)]
- %Threat Defense-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)

- %Threat Defense-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 bytes [(user)]
- %Threat Defense-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)]
- %Threat Defense-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)]
- %Threat Defense-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)
- %Threat Defense-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
- %Threat Defense-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)
- %Threat Defense-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
- %Threat Defense-6-302026: Built role stub ICMP connection for interface:real-address/real-port (mapped-address) to interface:real-address/real-port (mapped-address)
- %Threat Defense-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
- %Threat Defense-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- %Threat Defense-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)
- %Threat Defense-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface:ip/port to responder_interface:ip/port duration, bytes, teardown reason.
- %Threat Defense-6-303002: FTP connection from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port, user username action file filename
- %Threat Defense-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user)] to interface_name:mapped_address
- %Threat Defense-6-305010: Teardown {dynamic|static} translation from interface_name:real_address [(idfw_user)] to interface_name:mapped_address duration time
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-6-305014: Allocated block of ports for translation from real_interface : real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port.

- %Threat Defense-6-305015: Released block of ports for translation from real_interface : real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port.
- %Threat Defense-6-308001: console enable password incorrect for number tries (from IP_address)
- %Threat Defense-6-311001: LU loading standby start
- %Threat Defense-6-311002: LU loading standby end
- %Threat Defense-6-311003: LU recv thread up
- %Threat Defense-6-311004: LU xmit thread up
- %Threat Defense-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name
- %Threat Defense-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.
- %Threat Defense-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port: reason_string.
- %Threat Defense-6-317007: Added route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %Threat Defense-6-317008: Deleted route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %Threat Defense-6-321003: Resource var1 log level of var2 reached.
- %Threat Defense-6-321004: Resource var1 rate log level of var2 reached
- %Threat Defense-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
- %Threat Defense-6-333001: EAP association initiated - context:EAP-context
- %Threat Defense-6-333003: EAP association terminated - context:EAP-context
- %Threat Defense-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %Threat Defense-6-334001: EAPoUDP association initiated - host-address
- %Threat Defense-6-334004: Authentication request for NAC Clientless host - host-address
- %Threat Defense-6-334007: EAPoUDP association terminated - host-address
- %Threat Defense-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %Threat Defense-6-334009: Audit request for NAC Clientless host - Assigned_IP.
- %Threat Defense-6-336011: event event
- %Threat Defense-6-337000: Created BFD session with local discriminator id on real_interface with neighbor real_host_ip.
- %Threat Defense-6-337001: Terminated BFD session with local discriminator id on real_interface with neighbor real_host_ip due to failure_reason.

- %Threat Defense-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
- %Threat Defense-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr
- %Threat Defense-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_add
- %Threat Defense-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no
- %Threat Defense-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %Threat Defense-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.
- %Threat Defense-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>
- %Threat Defense-6-421006: There are number users of application accounted during the past 24 hours.
- %Threat Defense-6-425001 Redundant interface redundant_interface_name created.
- %Threat Defense-6-425002 Redundant interface redundant_interface_name removed.
- %Threat Defense-6-425003 Interface interface_name added into redundant interface redundant_interface_name.
- %Threat Defense-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.
- %Threat Defense-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface Port-channel num
- %Threat Defense-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface Port-channel num
- %Threat Defense-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface Port-channel num
- %Threat Defense-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP

- %Threat Defense-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP
- %Threat Defense-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP
- %Threat Defense-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP
- %FTD-6-430001: *Intrusion event syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの IDを参照してください。
- %FTD-6-430002: *Connection event logged at beginning of connection syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの IDを参照してください。
- %FTD-6-430003: *Connection event logged at end of connection syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの IDを参照してください。
- %FTD-6-430004: *File events syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの IDを参照してください。
- %FTD-6-430005: *File malware events syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの IDを参照してください。
- %FTD-6-430006: *File events from AMP for endpoints syslog*.
- %Threat Defense-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address, src_addr=source_address, prot=protocol
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.
- %Threat Defense-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.
- %Threat Defense-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %Threat Defense-6-604102: DHCP client interface interface_name: address released
- %Threat Defense-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %Threat Defense-6-604104: DHCP daemon interface interface_name: address released build_name (IP_address)
- %Threat Defense-6-605004: Login denied from source-address/source-port to interface:destination/service for user “username”

- %Threat Defense-6-605005: Login permitted from source-address/source-port to interface:destination/service for user “username”
- %Threat Defense-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
- %Threat Defense-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message
- %Threat Defense-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %Threat Defense-6-611301: VPN Client: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address
- %Threat Defense-6-611302: VPN Client: NAT exemption configured for Network Extension Mode with no split tunneling
- %Threat Defense-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
- %Threat Defense-6-611304: VPN Client: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %Threat Defense-6-611305: VPN Client: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
- %Threat Defense-6-611306: VPN Client: Perfect Forward Secrecy Policy installed
- %Threat Defense-6-611307: VPN Client: Head end: IP_address
- %Threat Defense-6-611308: VPN Client: Split DNS Policy installed: List of domains: string string
- %Threat Defense-6-611309: VPN Client: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address
- %Threat Defense-6-611310: VNP Client: XAUTH Succeeded: Peer: IP_address
- %Threat Defense-6-611311: VNP Client: XAUTH Failed: Peer: IP_address
- %Threat Defense-6-611312: VPN Client: Backup Server List: reason
- %Threat Defense-6-611314: VPN Client: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address
- %Threat Defense-6-611315: VPN Client: Disconnecting from Load Balancing Cluster member IP_address
- %Threat Defense-6-611316: VPN Client: Secure Unit Authentication Enabled
- %Threat Defense-6-611317: VPN Client: Secure Unit Authentication Disabled
- %Threat Defense-6-611318: VPN Client: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time
- %Threat Defense-6-611319: VPN Client: User Authentication Disabled
- %Threat Defense-6-611320: VPN Client: Device Pass Thru Enabled
- %Threat Defense-6-611321: VPN Client: Device Pass Thru Disabled

- %Threat Defense-6-611322: VPN Client: Extended XAUTH conversation initiated when SUA disabled
- %Threat Defense-6-611323: VPN Client: Duplicate split nw entry
- %Threat Defense-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
- %Threat Defense-6-613002: interface interface_name has zero bandwidth
- %Threat Defense-6-613003: IP_address netmask changed from area string to area string
- %Threat Defense-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string
- %Threat Defense-6-613027: OSPF process number removed from interface interface_name
- %Threat Defense-6-613028: Unrecognized virtual interface intetface_name. Treat it as loopback stub route
- %Threat Defense-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge
- %Threat Defense-6-613043:
- %Threat Defense-6-613101: Checksum Failure in database in area %s\n Link State Id %i Old Checksum %#x New Checksum %#x\n
- %Threat Defense-6-613102: interface %s has zero bandwidth
- %Threat Defense-6-613103: %i%m changed from area %AREA_ID_STR to area %AREA_ID_STR
- %Threat Defense-6-613104: Unrecognized virtual interface %IF_NAME.
- %Threat Defense-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
- %Threat Defense-6-614002: Split DNS: reply from server: IP_address reverse patched back to original server: IP_address
- %Threat Defense-6-615001: vlan number not available for firewall interface
- %Threat Defense-6-615002: vlan number available for firewall interface
- %Threat Defense-6-621001: Interface interface_name does not support multicast, not enabled
- %Threat Defense-6-621002: Interface interface_name does not support multicast, not enabled
- %Threat Defense-6-621003: The event queue size has exceeded number
- %Threat Defense-6-621006: Mrib disconnected, (IP_address, IP_address) event cancelled
- %Threat Defense-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %Threat Defense-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %Threat Defense-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries

- %Threat Defense-6-622102: Completed regex table compilation for match_command; table size = num bytes
- %Threat Defense-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
- %Threat Defense-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed <time-elapsed> ms
- %Threat Defense-6-709010: Configuration between units doesn't match. Going for config sync (%d). Time elapsed <time-elapsed> ms.
- %Threat Defense-6-709011: Total time to sync the config *time* ms.
- %Threat Defense-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.
- %Threat Defense-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
- %Threat Defense-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %Threat Defense-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %Threat Defense-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is_not behind a NAT device
- %Threat Defense-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %Threat Defense-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %Threat Defense-6-713202: Duplicate IP_addr packet detected.
- %Threat Defense-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %Threat Defense-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %Threat Defense-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %Threat Defense-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
- %Threat Defense-6-713228: Assigned private IP address assigned_private_IP
- %Threat Defense-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %Threat Defense-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
- %Threat Defense-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len

- %Threat Defense-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %Threat Defense-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: /prefix_len
- %Threat Defense-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: /prefix_len
- %Threat Defense-6-713905: Descriptive_event_string.
- %Threat Defense-6-716001: Group group User user WebVPN session started.
- %Threat Defense-6-716002: Group group User user WebVPN session terminated: reason.
- %Threat Defense-6-716003: Group group User user WebVPN access GRANTED: url
- %Threat Defense-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %Threat Defense-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %Threat Defense-6-716006: Group name User user WebVPN session terminated. Idle timeout.
- %Threat Defense-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %Threat Defense-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %Threat Defense-6-716039: Authentication: rejected, group = name user = user, Session Type: %s
- %Threat Defense-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %Threat Defense-6-716041: access-list acl_ID action url url hit_cnt count
- %Threat Defense-6-716042: access-list acl_ID action tcp source_interface/source_address (source_port) - dest_interface/dest_address(dest_port) hit-cnt count
- %Threat Defense-6-716043 Group group-name, User user-name, IP IP_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings
- %Threat Defense-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.
- %Threat Defense-6-716050: Error adding to ACL: ace_command_line
- %Threat Defense-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
- %Threat Defense-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded
- %Threat Defense-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.
- %Threat Defense-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2
- %Threat Defense-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.

- %Threat Defense-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
- %Threat Defense-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
- %Threat Defense-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
- %Threat Defense-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
- %Threat Defense-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
- %Threat Defense-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %Threat Defense-6-717022: Certificate was successfully validated. certificate_identifiers
- %Threat Defense-6-717028: Certificate chain was successfully validated additional info.
- %Threat Defense-6-717033: OCSP response status - Successful.
- %Threat Defense-6-717056: Attempting type revocation check from Src Interface:Src IP/Src Port to Dst IP/Dst Port using protocol
- %Threat Defense-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number
- %Threat Defense-6-718004: Got unknown internal message message_number
- %Threat Defense-6-718013: Peer IP_address is not answering HELLO
- %Threat Defense-6-718027: Received unexpected KEEPALIVE request from IP_address
- %Threat Defense-6-718030: Received planned OOS from IP_address
- %Threat Defense-6-718037: Master processed number_of_timeouts timeouts
- %Threat Defense-6-718038: Slave processed number_of_timeouts timeouts
- %Threat Defense-6-718039: Process dead peer IP_address
- %Threat Defense-6-718040: Timed-out exchange ID exchange_ID not found
- %Threat Defense-6-718051: Deleted secure tunnel to peer IP_address
- %Threat Defense-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
- %Threat Defense-6-719003: Email Proxy session pointer resources have been freed for source_address.
- %Threat Defense-6-719004: Email Proxy session pointer has been successfully established for source_address.
- %Threat Defense-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
- %Threat Defense-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.
- %Threat Defense-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %Threat Defense-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %Threat Defense-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %Threat Defense-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found

- %Threat Defense-6-719019: WebVPN user: vpnuser authorization failed.
- %Threat Defense-6-719020: WebVPN user vpnuser authorization completed successfully.
- %Threat Defense-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %Threat Defense-6-719022: WebVPN user vpnuser has been authenticated.
- %Threat Defense-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %Threat Defense-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
- %Threat Defense-6-719025: Email Proxy DNS name resolution failed for hostname.
- %Threat Defense-6-719026: Email Proxy DNS name hostname resolved to IP_address.
- %Threat Defense-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %Threat Defense-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %Threat Defense-6-720004: (VPN-unit) VPN failover main thread started.
- %Threat Defense-6-720005: (VPN-unit) VPN failover timer thread started.
- %Threat Defense-6-720006: (VPN-unit) VPN failover sync thread started.
- %Threat Defense-6-720010: (VPN-unit) VPN failover client is being disabled
- %Threat Defense-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.
- %Threat Defense-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
- %Threat Defense-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his).
- %Threat Defense-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %Threat Defense-6-720024: (VPN-unit) HA status callback: Control channel is status.
- %Threat Defense-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %Threat Defense-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %Threat Defense-6-720027: (VPN-unit) HA status callback: My state state.
- %Threat Defense-6-720028: (VPN-unit) HA status callback: Peer state state.
- %Threat Defense-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %Threat Defense-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %Threat Defense-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence_#, grp=group, event=event, op=operand, my=my_state, peer=peer_state.
- %Threat Defense-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence_number,grp=group,event=event,op=operand, my=my_state,peer=peer_state.

- %Threat Defense-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %Threat Defense-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %Threat Defense-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %Threat Defense-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %Threat Defense-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %Threat Defense-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %Threat Defense-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %Threat Defense-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %Threat Defense-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %Threat Defense-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %Threat Defense-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %Threat Defense-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %Threat Defense-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
- %Threat Defense-6-721002: (device) HA status change: event event, my state my_state, peer state peer.
- %Threat Defense-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.
- %Threat Defense-6-721004: (device) Create access list list_name on standby unit.
- %Threat Defense-6-721005: (device) Fail to create access list list_name on standby unit.
- %Threat Defense-6-721006: (device) Update access list list_name on standby unit.
- %Threat Defense-6-721008: (device) Delete access list list_name on standby unit.
- %Threat Defense-6-721009: (device) Fail to delete access list list_name on standby unit.
- %Threat Defense-6-721010: (device) Add access list rule list_name, line line_no on standby unit.
- %Threat Defense-6-721012: (device) Enable APCF XML file file_name on the standby unit.
- %Threat Defense-6-721014: (device) Disable APCF XML file file_name on the standby unit.
- %Threat Defense-6-721016: (device) WebVPN session for client user user_name, IP ip_address has been created.
- %Threat Defense-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.
- %Threat Defense-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message

- %Threat Defense-6-722014: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %Threat Defense-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
- %Threat Defense-6-722053: Group g User u IP ip Unknown client user-agent connection.
- %Threat Defense-6-722055: Group group-policy User username IP public-ip Client Type: user-agent
- %Threat Defense-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.
- %Threat Defense-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.
- %Threat Defense-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session.
- %Threat Defense-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session
- %Threat Defense-6-725003: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port request to resume previous session.
- %Threat Defense-6-725004: Device requesting certificate from SSL peer-type interface:src-ip/src-port to dst-ip/dst-port for authentication.
- %Threat Defense-6-725005: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port requesting our device certificate for authentication.
- %Threat Defense-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port
- %Threat Defense-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated.
- %Threat Defense-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
- %Threat Defense-6-725016: Device selects trust-point <trustpoint> for peer-type interface:src-ip/src-port to dst-ip/dst-port
- %Threat Defense-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %Threat Defense-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %Threat Defense-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %Threat Defense-6-737009: IPAA: AAA assigned address ip-address, request failed
- %Threat Defense-6-737010: IPAA: AAA assigned address ip-address, request succeeded
- %Threat Defense-6-737014: IPAA: Freeing AAA address ip-address
- %Threat Defense-6-737015: IPAA: Freeing DHCP address ip-address

- %Threat Defense-6-737016: IPAA: Freeing local pool address ip-address
- %Threat Defense-6-737017: IPAA: DHCP request attempt num succeeded
- %Threat Defense-6-737026: IPAA: Client assigned ip-address from local pool
- %Threat Defense-6-737029: IPAA: Adding ip-address to standby: succeeded
- %Threat Defense-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
- %Threat Defense-6-737406: POOLIP: Pool=pool, INFO: message
- %Threat Defense-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB
- %Threat Defense-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB
- %Threat Defense-6-741002: Coredump log and filesystem contents cleared on variable 1
- %Threat Defense-6-741003: Coredump filesystem and its contents removed on variable 1
- %Threat Defense-6-741004: Coredump configuration reset to default values
- %Threat Defense-6-747004: Clustering: state machine changed from state state-name to state-name.
- %FTD-6-747044: Clustering: Configuration Hash string verification <result>.
- %Threat Defense-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.
- %Threat Defense-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.
- %Threat Defense-6-751023: Local a:p Remote: a:p Username:n Unknown client connection
- %Threat Defense-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version
- %Threat Defense-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
- %Threat Defense-6-772005: REAUTH: user username passed authentication
- %FTD-6-776251: CTS SGT-MAP: Binding binding IP - SGname (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.
- %Threat Defense-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port).
- %Threat Defense-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.

- %Threat Defense-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.
- %Threat Defense-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %Threat Defense-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.
- %Threat Defense-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %Threat Defense-6-778007: VXLAN: Packet from ifc-name:IP-address/port to IP-address/port was discarded due to invalid NVE peer.
- %Threat Defense-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name:IP-address/port to IP-address/port.
- %Threat Defense-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
- %Threat Defense-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction
- %Threat Defense-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction
- %Threat Defense-6-780003: RULE ENGINE: Started compilation for nat transaction -description of the transaction
- %Threat Defense-6-780004: RULE ENGINE: Finished compilation for nat transaction -description of the transaction
- %Threat Defense-6-802005: IP ip_address Received MDM request details.
- %Threat Defense-6-803001:Bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %Threat Defense-6-803002: No protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %Threat Defense-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2
- %Threat Defense-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted
- %Threat Defense-6-804002: Interface GigabitEthernet1/3 SFP has been removed
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-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-6-802005: IP ip_address Received MDM request details.

- %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
- %Threat Defense-6-8300001: VPN session redistribution <variable 1>
- %Threat Defense-6-8300002: Moved <variable 1> sessions to <variable 2>
- %Threat Defense-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

デバッグ メッセージ、重大度 7

次のメッセージが重大度 7（デバッグ）で表示されます。

- %Threat Defense-7-111009: User user executed cmd:string
- %Threat Defense-7-113028: Extraction of username from VPN client certificate has string. [Request num]
- %Threat Defense-7-199019: syslog
- %Threat Defense-7-333004: EAP-SQ response invalid - context:EAP-context
- %Threat Defense-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %Threat Defense-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %Threat Defense-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %Threat Defense-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %Threat Defense-7-609001: Built local-host zone_name/*: ip_address
- %Threat Defense-7-609002: Teardown local-host zone_name/*: ip_address duration time
- %Threat Defense-7-701001: alloc_user() out of Tcp_user objects
- %Threat Defense-7-701002: alloc_user() out of Tcp_proxy objects
- %Threat Defense-7-702307: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.
- %Threat Defense-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %Threat Defense-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
- %Threat Defense-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d\n
- %Threat Defense-7-709001: FO replication failed: cmd=command returned=code
- %Threat Defense-7-709002: FO unreplicable: cmd=command

- %Threat Defense-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-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)
- %Threat Defense-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %Threat Defense-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500
- %Threat Defense-7-711001: debug_trace_msg
- %Threat Defense-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.
- %Threat Defense-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string.
- %Threat Defense-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %Threat Defense-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %Threat Defense-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %Threat Defense-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %Threat Defense-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %Threat Defense-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %Threat Defense-7-713039: Send failure: Bytes (number), Peer: IP_address
- %Threat Defense-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %Threat Defense-7-713052: User (user) authenticated.
- %Threat Defense-7-713066: IKE Remote Peer configured for SA: SA_name
- %Threat Defense-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %Threat Defense-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %Threat Defense-7-713103: Invalid (NULL) secret key detected while computing hash
- %Threat Defense-7-713104: Attempt to get Phase 1 ID data failed while hash computation

- %Threat Defense-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count
- %Threat Defense-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match
- %Threat Defense-7-713117: Received Invalid SPI notify (SPI SPI_Value)!
- %Threat Defense-7-713121: Keep-alive type for this connection: keepalive_type
- %Threat Defense-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability_value, Version Number: version_number, Version String: version_text
- %Threat Defense-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %Threat Defense-7-713164: The Firewall Server has requested a list of active user sessions
- %Threat Defense-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count
- %Threat Defense-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id
- %Threat Defense-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %Threat Defense-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
- %Threat Defense-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)
- %Threat Defense-7-713204: Adding static route for client address: IP_address
- %Threat Defense-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...
- %Threat Defense-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
- %Threat Defense-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured
- %Threat Defense-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %Threat Defense-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match
- %Threat Defense-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %Threat Defense-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %Threat Defense-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen
- %Threat Defense-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port

- %Threat Defense-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"}
- %Threat Defense-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed
- %Threat Defense-7-713906: Descriptive_event_string.
- %Threat Defense-7-714001: description_of_event_or_packet
- %Threat Defense-7-714002: IKE Initiator starting QM: msg id = message_number
- %Threat Defense-7-714003: IKE Responder starting QM: msg id = message_number
- %Threat Defense-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %Threat Defense-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %Threat Defense-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %Threat Defense-7-714007: IKE Initiator sending Initial Contact
- %Threat Defense-7-714011: Description of received ID values
- %Threat Defense-7-715001: Descriptive statement
- %Threat Defense-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %Threat Defense-7-715005: subroutine name() Bad message code: Code (message_code)
- %Threat Defense-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %Threat Defense-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %Threat Defense-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %Threat Defense-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %Threat Defense-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %Threat Defense-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name
- %Threat Defense-7-715020: construct_cfg_set: Attribute name = name
- %Threat Defense-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %Threat Defense-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %Threat Defense-7-715027: IPSec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPSec SA entry # crypto_map_index
- %Threat Defense-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index
- %Threat Defense-7-715033: Processing CONNECTED notify (MsgId message_number)
- %Threat Defense-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.

- %Threat Defense-7-715035: Starting IOS keepalive monitor: seconds sec.
- %Threat Defense-7-715036: Sending keep-alive of type notify_type (seq number number)
- %Threat Defense-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %Threat Defense-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %Threat Defense-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %Threat Defense-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %Threat Defense-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %Threat Defense-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %Threat Defense-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %Threat Defense-7-715045: ERROR: malformed Keepalive payload
- %Threat Defense-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload
- %Threat Defense-7-715047: processing payload_description payload
- %Threat Defense-7-715048: Send VID_type VID
- %Threat Defense-7-715049: Received VID_type VID
- %Threat Defense-7-715050: Claims to be IOS but failed authentication
- %Threat Defense-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply
- %Threat Defense-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %Threat Defense-7-715053: MODE_CFG: Received request for attribute_info!
- %Threat Defense-7-715054: MODE_CFG: Received attribute_name reply: value
- %Threat Defense-7-715055: Send attribute_name
- %Threat Defense-7-715056: Client is configured for TCP_transparency
- %Threat Defense-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %Threat Defense-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %Threat Defense-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %Threat Defense-7-715060: Dropped received IKE fragment. Reason: reason
- %Threat Defense-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %Threat Defense-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

- %Threat Defense-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %Threat Defense-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %Threat Defense-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
- %Threat Defense-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %Threat Defense-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %Threat Defense-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %Threat Defense-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %Threat Defense-7-715069: Invalid ESP SPI size of SPI_size
- %Threat Defense-7-715070: Invalid IPComp SPI size of SPI_size
- %Threat Defense-7-715071: AH proposal not supported
- %Threat Defense-7-715072: Received proposal with unknown protocol ID protocol_ID
- %Threat Defense-7-715074: Could not retrieve authentication attributes for peer IP_address
- %Threat Defense-7-715075: Group = group_name, IP = IP_address Received keep-alive of type message_type (seq number number)
- %Threat Defense-7-715076: Computing hash for ISAKMP
- %Threat Defense-7-715077: Pitcher: msg string, spi spi
- %Threat Defense-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.
- %Threat Defense-7-716008: WebVPN ACL: action
- %Threat Defense-7-716010: Group group User user Browse network.
- %Threat Defense-7-716011: Group group User user Browse domain domain.
- %Threat Defense-7-716012: Group group User user Browse directory directory.
- %Threat Defense-7-716013: Group group User user Close file filename.
- %Threat Defense-7-716014: Group group User user View file filename.
- %Threat Defense-7-716015: Group group User user Remove file filename.
- %Threat Defense-7-716016: Group group User user Rename file old_filename to new_filename.
- %Threat Defense-7-716017: Group group User user Modify file filename.
- %Threat Defense-7-716018: Group group User user Create file filename.
- %Threat Defense-7-716019: Group group User user Create directory directory.
- %Threat Defense-7-716020: Group group User user Remove directory directory.
- %Threat Defense-7-716021: File access DENIED, filename.

- %Threat Defense-7-716024: Group name User user Unable to browse the network.Error: description
- %Threat Defense-7-716025: Group name User user Unable to browse domain domain. Error: description
- %Threat Defense-7-716026: Group name User user Unable to browse directory directory. Error: description
- %Threat Defense-7-716027: Group name User user Unable to view file filename. Error: description
- %Threat Defense-7-716028: Group name User user Unable to remove file filename. Error: description
- %Threat Defense-7-716029: Group name User user Unable to rename file filename. Error: description
- %Threat Defense-7-716030: Group name User user Unable to modify file filename. Error: description
- %Threat Defense-7-716031: Group name User user Unable to create file filename. Error: description
- %Threat Defense-7-716032: Group name User user Unable to create folder folder. Error: description
- %Threat Defense-7-716033: Group name User user Unable to remove folder folder. Error: description
- %Threat Defense-7-716034: Group name User user Unable to write to file filename.
- %Threat Defense-7-716035: Group name User user Unable to read file filename.
- %Threat Defense-7-716036: Group name User user File Access: User user logged into the server server.
- %Threat Defense-7-716037: Group name User user File Access: User user failed to login into the server server.
- %Threat Defense-7-716603: Received size-recv KB Hostscan data from IP src-ip.
- %Threat Defense-7-717024: Checking CRL from trustpoint: trustpoint name for purpose
- %Threat Defense-7-717025: Validating certificate chain containing number of certs certificate(s).
- %Threat Defense-7-717029: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %Threat Defense-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.
- %Threat Defense-7-717034: No-check extension found in certificate. OCSP check bypassed.
- %Threat Defense-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.
- %Threat Defense-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %Threat Defense-7-718001: Internal interprocess communication queue send failure: code error_code
- %Threat Defense-7-718017: Got timeout for unknown peer IP_address msg type message_type
- %Threat Defense-7-718018: Send KEEPALIVE request failure to IP_address
- %Threat Defense-7-718019: Sent KEEPALIVE request to IP_address
- %Threat Defense-7-718020: Send KEEPALIVE response failure to IP_address

- %Threat Defense-7-718021: Sent KEEPALIVE response to IP_address
- %Threat Defense-7-718022: Received KEEPALIVE request from IP_address
- %Threat Defense-7-718023: Received KEEPALIVE response from IP_address
- %Threat Defense-7-718025: Sent CFG UPDATE to IP_address
- %Threat Defense-7-718026: Received CFG UPDATE from IP_address
- %Threat Defense-7-718029: Sent OOS indicator to IP_address
- %Threat Defense-7-718034: Sent TOPOLOGY indicator to IP_address
- %Threat Defense-7-718035: Received TOPOLOGY indicator from IP_address
- %Threat Defense-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address
- %Threat Defense-7-718041: Timeout [msgType=type] processed with no callback
- %Threat Defense-7-718046: Create group policy policy_name
- %Threat Defense-7-718047: Fail to create group policy policy_name
- %Threat Defense-7-718049: Created secure tunnel to peer IP_address
- %Threat Defense-7-718056: Deleted Master peer, IP IP_address
- %Threat Defense-7-718058: State machine return code: action_routine, return_code
- %Threat Defense-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine
- %Threat Defense-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.
- %Threat Defense-7-719005: FSM NAME has been created using protocol for session pointer from source_address.
- %Threat Defense-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.
- %Threat Defense-7-719007: Email Proxy session pointer cannot be found for source_address.
- %Threat Defense-7-719009: Email Proxy service is starting.
- %Threat Defense-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server
- %Threat Defense-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******
- %Threat Defense-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.
- %Threat Defense-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %Threat Defense-7-720041: (VPN-unit) Sending type message id to standby unit
- %Threat Defense-7-720042: (VPN-unit) Receiving type message id from active unit

- %Threat Defense-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %Threat Defense-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %Threat Defense-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %Threat Defense-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
- %Threat Defense-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
- %Threat Defense-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.
- %Threat Defense-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %Threat Defense-7-723004: WebVPN Citrix encountered bad flow control flow.
- %Threat Defense-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %Threat Defense-7-723006: WebVPN Citrix SOCKS errors.
- %Threat Defense-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %Threat Defense-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %Threat Defense-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.
- %Threat Defense-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %Threat Defense-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.
- %Threat Defense-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.
- %Threat Defense-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %Threat Defense-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %Threat Defense-7-725008: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port proposes the following n cipher(s).
- %Threat Defense-7-725009: Device proposes the following n cipher(s) peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %Threat Defense-7-725010: Device supports the following n cipher(s).
- %Threat Defense-7-725011: Cipher[order]: cipher_name
- %Threat Defense-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port.

- %Threat Defense-7-725013: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port chooses cipher cipher
- %Threat Defense-7-725014: SSL lib error. Function: function Reason: reason
- %Threat Defense-7-725017: No certificates received during the handshake with %s %s:%B/%d to %B/%d for %s session
- %FTD-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %FTD-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %Threat Defense-7-730002: Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed
- %Threat Defense-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value
- %Threat Defense-7-737001: IPAA: Received message ‘message-type’
- %Threat Defense-7-737035: IPAA: Session=<session>, '<message type>' message queued
- %FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool
- %FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message
- %FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool
- %FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %FTD-7-737407: POOLIP: Pool=pool, DEBUG: message
- %Threat Defense-7-747005: Clustering: State machine notify event event-name (event-id, ptr-in-hex, ptr-in-hex)
- %Threat Defense-7-747006: Clustering: State machine is at state state-name
- %Threat Defense-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer
- %Threat Defense-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-7-752008: Duplicate entry already in Tunnel Manager.
- %Threat Defense-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>.

Syslog メッセージで使用される変数

多くの場合、syslog メッセージには変数が含まれています。次の表に、syslog メッセージを説明するためにこのガイドで使用されているほとんどの変数を示します。1 つの syslog メッセージにしか現れない変数の中には省略したものがあります。

syslog メッセージの変数フィールド

変数	説明
acl_ID	ACL 名。
bytes	バイト数。
code	syslog メッセージによって返される 10 進数。生成される syslog メッセージに応じて、エラーの原因または発生源を示します。
command	コマンド名。
command_modifier	**command_modifier** は、次の文字列のいずれかです。 • cmd（この文字列は、コマンドに修飾子がないことを意味します） • clear • no • show
connections	接続数。
connection_type	接続タイプは次のとおりです。 • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • RTP • RTCP
dec	10 進数
dest_address	パケットの宛先アドレス。
dest_port	宛先ポート番号。

変数	説明
device	メモリ ストレージデバイス。たとえば、フロッピーディスク、内部フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末です。
econns	初期接続数。
elimit	**static** コマンドまたは **nat** コマンドで指定された初期接続数。
filename	ASAimage タイプ、ASDM ファイル、またはコンフィギュレーションのファイル名。
ftp-server	外部 FTP サーバー名または IP アドレス。
gateway_address	ネットワーク ゲートウェイ IP アドレス。
global_address	グローバル IP アドレス。セキュリティ レベルの低いインターフェイス上のアドレスです
global_port	グローバル ポート番号。
hex	16 進数
inside_address	内部（つまり、ローカル）IP アドレス。高セキュリティ レベル インターフェイス上のアドレス。
inside_port	内部ポート番号。
interface_name	インターフェイスの名前。
IP_address	IP アドレス。形式は *n n n n* で、*n* は 1 ～ 255 の整数です。
MAC_address	MAC アドレス。
mapped_address	変換済み IP アドレス。
mapped_port	変換済みポート番号。
message_class	ASA の機能エリアに関連付けられている syslog メッセージのカテゴリ。
message_list	syslog メッセージの ID 番号、クラス、または重大度のリストを含む作成ファイルの名前。
message_number	syslog メッセージ ID。
nconns	static テーブルまたは xlate テーブルに許可された接続数。
netmask	サブネット マスク。
number	数字。正確な形式は、syslog メッセージによって決まります。

変数	説明
octal	8 進数
outside_address	外側（つまり、外部）IP アドレス。通常は、外部ルータの先のネットワークにある低セキュリティ レベル インターフェイス上の syslog サーバーのアドレス。
outside_port	外部ポート番号。
port	TCP または UDP ポート番号。
privilege_level	ユーザー特権レベル。
protocol	パケットのプロトコル。たとえば、ICMP、TCP、または UDP。
real_address	NAT 前の実 IP アドレス。
real_port	NAT 前の実ポート番号。
reason	syslog メッセージの理由を記述するテキスト文字列。
service	パケットで指定されたサービス。たとえば、SNMP または Telnet。
severity_level	syslog メッセージの重大度。
source_address	パケットのソース アドレス。
source_port	ソース ポート番号。
string	テキスト文字列（ユーザー名など）
tcp_flags	TCP ヘッダー内のフラグ。たとえば、次に示すものです。 • ACK • FIN • PSH • RST • SYN • URG
time	継続時間（*hh mm ss* 形式）
url	URL。
user	ユーザー名。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。