



APPENDIX **A**

Messages Listed by Severity Level

This appendix contains the following sections:

- [Alert Messages, Severity 1, page A-1](#)
- [Critical Messages, Severity 2, page A-4](#)
- [Error Messages, Severity 3, page A-6](#)
- [Warning Messages, Severity 4, page A-18](#)
- [Notification Messages, Severity 5, page A-28](#)
- [Informational Messages, Severity 6, page A-36](#)
- [Debugging Messages, Severity 7, page A-49](#)
- [Variables Used in Syslog Messages, page A-57](#)



Note

The Cisco ASA 5500 Series Security Appliance does not send severity 0, emergency messages to the syslog server. These are analogous to a UNIX panic message, and denote an unstable system.

Alert Messages, Severity 1

The following messages appear at severity 1, alerts:

- %PIX|ASA-1-101001: (Primary) Failover cable OK.
- %PIX|ASA-1-101002: (Primary) Bad failover cable.
- %PIX|ASA-1-101003: (Primary) Failover cable not connected (this unit).
- %PIX|ASA-1-101004: (Primary) Failover cable not connected (other unit).
- %PIX|ASA-1-101005: (Primary) Error reading failover cable status.
- %PIX|ASA-1-102001: (Primary) Power failure/System reload other side.
- %PIX|ASA-1-103001: (Primary) No response from other firewall (reason code = code).
- %PIX|ASA-1-103002: (Primary) Other firewall network interface interface_number OK.
- %PIX|ASA-1-103003: (Primary) Other firewall network interface interface_number failed.
- %PIX|ASA-1-103004: (Primary) Other firewall reports this firewall failed.
- %PIX|ASA-1-103005: (Primary) Other firewall reporting failure.
- %PIX|ASA-1-104001: (Primary) Switching to ACTIVE (cause: string).

- %PIXIASA-1-104002: (Primary) Switching to STNDBY (cause: string).
- %PIXIASA-1-104003: (Primary) Switching to FAILED.
- %PIXIASA-1-104004: (Primary) Switching to OK.
- %PIXIASA-1-105001: (Primary) Disabling failover.
- %PIXIASA-1-105002: (Primary) Enabling failover.
- %PIXIASA-1-105003: (Primary) Monitoring on interface interface_name waiting
- %PIXIASA-1-105004: (Primary) Monitoring on interface interface_name normal
- %PIXIASA-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %PIXIASA-1-105006: (Primary) Link status 'Up' on interface interface_name.
- %PIXIASA-1-105007: (Primary) Link status 'Down' on interface interface_name.
- %PIXIASA-1-105008: (Primary) Testing interface interface_name.
- %PIXIASA-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %PIXIASA-1-105011: (Primary) Failover cable communication failure
- %PIXIASA-1-105020: (Primary) Incomplete/slow config replication
- %PIXIASA-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name
- %PIXIASA-1-105031: Failover LAN interface is up
- %PIXIASA-1-105032: LAN Failover interface is down
- %PIXIASA-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %PIXIASA-1-105035: Receive a LAN failover interface down msg from peer.
- %PIXIASA-1-105036: dropped a LAN Failover command message.
- %PIXIASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %PIXIASA-1-105038: (Primary) Interface count mismatch
- %PIXIASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %PIXIASA-1-105040: (Primary) Mate failover version is not compatible.
- %PIXIASA-1-105042: (Primary) Failover interface OK
- %PIXIASA-1-105043: (Primary) Failover interface failed
- %PIXIASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %PIXIASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %PIXIASA-1-105046 (Primary|Secondary) Mate has a different chassis
- %PIXIASA-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
- %ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)
- %PIXIASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name

- %PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name
- %PIX|ASA-1-106101 The number of ACL log deny-flows has reached limit (number).
- %PIX|ASA-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name
- %PIX|ASA-1-107002: RIP pkt failed from IP_address: version=number on interface interface_name
- %PIX|ASA-1-111111 error_message
- %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).
- %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).
- %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string).
- %ASA-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
- %ASA-n-216001: internal error in: function: message
- %ASA-1-216005: ERROR: Duplex-mismatch on interface_name resulted in transmitter lockup. A soft reset of the switch was performed.
- %ASA-1-323006: Module in slot slot experienced a data channel communication failure, data channel is DOWN.
- %ASA|PIX-1-332004: Web Cache IP_address/service_ID lost
- %ASA-1-413005: prod_id Module in slot slot, application is not supported app_name version app_vers type app_type
- %ASA-1-505011: Type Module in slot slot data channel communication is UP.
- %ASA-1-505014: prod_id Module in slot slot, application down name, version version reason
- %ASA-1-505015: SSM model Module in slot number, application up application version, version
- %PIX|ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %PIX|ASA-1-709004: (Primary) End Configuration Replication (ACT)
- %PIX|ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %PIX|ASA-1-709006: (Primary) End Configuration Replication (STB)
- %ASA-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.
- %ASA-1-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber. Cannot continue terminating
- %ASA-1-716509: internal error in: function: Fiber scheduler is scheduling alien fiber. Cannot continue terminating
- %ASA-1-716510: internal error in: function: Fiber scheduler is scheduling finished fiber. Cannot continue terminating
- %ASA-1-716516: internal error in: function: OCCAM has corrupted ROL array. Cannot continue terminating
- %ASA-1-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating
- %ASA-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition

- %ASA-1-717049: Local CA Server certificate is due to expire in number days and a replacement certificate is available for export.

Critical Messages, Severity 2

The following messages appear at severity 2, critical:

- %PIXIASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
- %PIXIASA-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
- %PIXIASA-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %PIXIASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.
- %PIXIASA-2-106013: Dropping echo request from IP_address to PAT address IP_address
- %PIXIASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- %PIXIASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address
- %PIXIASA-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
- %PIXIASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
- %PIXIASA-2-106024: Access rules memory exhausted
- %PIXIASA-2-108002: SMTP replaced string: out source_address in inside_address data: string
- %PIXIASA-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
- %PIXIASA-2-109011: Authen Session Start: user 'user', sid number
- %PIXIASA-2-112001: (string:dec) Clear complete.
- %ASA-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
- %ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %ASA-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.
- %PIXIASA-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
- %PIXIASA-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %PIXIASA-2-215001:Bad route_compress() call, sdb= number
- %ASA-n-216001: internal error in: function: message
- %PIXIASA-2-217001: No memory for string in string
- %PIXIASA-2-218001: Failed Identification Test in slot# [fail#/res].

- %PIX|ASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %PIX|ASA-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.
- %PIX|ASA-2-218004: Failed Identification Test in slot# [fail#/res]
- %PIX|ASA-2-304007: URL Server IP_address not responding, ENTERING ALLOW mode.
- %PIX|ASA-2-304008: LEAVING ALLOW mode, URL Server is up.
- %PIX|ASA-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
- %ASA-2-444004: Temporary license key key has expired. Applying permanent license key permkey
- %ASA-2-444007: Timebased activation key activation-key has expired. Reverting to [permanent | timebased] license key. The following features will be affected: feature, feature
- %PIX|ASA-2-709007: Configuration replication failed for command command
- %PIX|ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
- %PIX|ASA-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %ASA-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %ASA-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %ASA-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %ASA-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %ASA-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %ASA-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %ASA-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER
- %ASA-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %ASA-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %ASA-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %ASA-2-716517: internal error in: function: OCCAM cached block has no associated arena
- %ASA-2-716518: internal error in: function: OCCAM pool has no associated arena
- %ASA-2-716520: internal error in: function: OCCAM pool has no block list
- %ASA-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %ASA-2-716522: internal error in: function: OCCAM corrupted standalone block
- %ASA-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED
- %ASA-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL
- %ASA-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAIL
- %PIX|ASA-2-717008: Insufficient memory to process_requiring_memory.
- %PIX|ASA-2-717011: Unexpected event event event_ID
- %ASA-2-717040: Local CA Server has failed and is being disabled. Reason: reason.
- %ASA-2-800000: DSI: Unable to allocate memory

Error Messages, Severity 3

The following messages appear at severity 3, errors:

- %PIXIASA-3-105010: (Primary) Failover message block alloc failed
- %PIXIASA-3-106010: Deny inbound protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port
- %PIXIASA-3-106011: Deny inbound (No xlate) string
- %PIXIASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
- %PIX-3-107003: RIP: Attempted reference of stale data encountered in function, line: line_num
- %PIXIASA-3-109010: Auth from inside_address/inside_port to outside_address/outside_port failed (too many pending auths) on interface interface_name.
- %PIXIASA-3-109013: User must authenticate before using this service
- %PIXIASA-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %PIXIASA-3-109018: Downloaded ACL acl_ID is empty
- %PIXIASA-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %PIXIASA-3-109020: Downloaded ACL has config error; ACE
- %PIXIASA-3-109023: User from source_address/source_port to dest_address/dest_port on interface outside_interface must authenticate before using this service.
- %PIXIASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %PIXIASA-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.
- %ASA-3-109035: Exceeded maximum number (999) of DAP attribute instances for user string
- %ASA-3-109036: RADIUS Server has received a request from unconfigured ip address src_ip_addr, dropping the request.
- %PIXIASA-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %PIXIASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action
- %PIXIASA-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds
- %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).
- %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).
- %ASA-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.
- %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string).
- %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string).
- %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).
- %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).
- %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).
- %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).

- %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).
- %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).
- %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).
- %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).
- %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).
- %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %ASA-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string
- %PIX|ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.
- %ASA-3-120010: Notify command command to SCH client 'client' failed. Reason 'reason'.
- %PIX|ASA-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %PIX|ASA-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit
- %PIX|ASA-3-201005: FTP data connection failed for IP_address IP_address
- %PIX|ASA-3-201006: RCMD back connection failed for IP_address/port.
- %PIX|ASA-3-201008: The security appliance is disallowing new connections.
- %PIX|ASA-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded
- %PIX|ASA-3-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
- %PIX|ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
- %ASA-3-201013: Per-client connection limit exceeded curr num/limit for [input|output] packet from ip/port to ip/port on interface interface_name
- %PIX|ASA-3-202001: Out of address translation slots!
- %PIX|ASA-3-202005: Non-embryonic in embryonic list outside_address/outside_port inside_address/inside_port
- %PIX|ASA-3-202011: Connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
- %PIX|ASA-3-208005: (function:line_num) clear command return code
- %PIX|ASA-3-210001: LU sw_module_name error = number
- %PIX|ASA-3-210002: LU allocate block (bytes) failed.
- %PIX|ASA-3-210003: Unknown LU Object number
- %PIX|ASA-3-210005: LU allocate connection failed
- %PIX|ASA-3-210006: LU look NAT for IP_address failed
- %PIX|ASA-3-210007: LU allocate xlate failed
- %PIX|ASA-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %PIX|ASA-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed
- %PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.

- %PIXIASA-3-210020: LU PAT port port reserve failed
- %PIXIASA-3-210021: LU create static xlate global_address ifc interface_name failed
- %PIXIASA-3-211001: Memory allocation Error
- %PIXIASA-3-211003: CPU utilization for number seconds = percent
- %PIXIASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %PIXIASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %PIXIASA-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %PIXIASA-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %PIXIASA-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %PIXIASA-3-212006: Dropping SNMP request from source_address/source_port to interface_name:dest_address/dest_port because: reason.
- %PIXIASA-3-213001: PPTP control daemon socket io string, errno = number.
- %PIXIASA-3-213002: PPTP tunnel hash table insert failed, peer = IP_address.
- %PIXIASA-3-213003: PPP virtual interface interface_number isn't opened.
- %PIXIASA-3-213004: PPP virtual interface interface_number client ip allocation failed.
- %ASA-n-216001: internal error in: function: message
- %PIXIASA-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num
- %PIXIASA-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num
- %ASA-3-219002: I2C_API_name error, slot = slot_number, device = device_number, address = address, byte count = count. Reason: reason_string
- %PIXIASA-3-302019: H.323 library_name ASN Library failed to initialize, error code number
- %PIXIASA-3-302302: ACL = deny; no sa created
- %PIXIASA-3-304003: URL Server IP_address timed out URL url
- %PIXIASA-3-304006: URL Server IP_address not responding
- %PIXIASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name: dest_address/dest_port
- %PIXIASA-3-305006: {outbound static|identity|portmap|regular} translation creation failed for protocol src interface_name:source_address/source_port dst interface_name:dest_address/dest_port
- %PIXIASA-3-305008: Free unallocated global IP address.
- %PIXIASA-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
- %PIXIASA-3-313008: Denied ICMPv6 type=number, code=code from IP_address on interface interface_name
- %PIXIASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

- %PIX|ASA-3-316001: Denied new tunnel to IP_address. VPN peer limit (platform_vpn_peer_limit) exceeded
- %ASA-3-316002: VPN Handle error: protocol=protocol, src in_if_num:src_addr, dst out_if_num:dst_addr
- %PIX|ASA-3-317001: No memory available for limit_slow
- %PIX|ASA-3-317002: Bad path index of number for IP_address, number max
- %PIX|ASA-3-317003: IP routing table creation failure - reason
- %PIX|ASA-3-317004: IP routing table limit warning
- %PIX|ASA-3-317005: IP routing table limit exceeded - reason, IP_address netmask
- %PIX|ASA-3-317006: Pdb index error pdb, pdb_index, pdb_type
- %PIX|ASA-3-318001: Internal error: reason
- %PIX|ASA-3-318002: Flagged as being an ABR without a backbone area
- %PIX|ASA-3-318003: Reached unknown state in neighbor state machine
- %PIX|ASA-3-318004: area string lsid IP_address mask netmask adv IP_address type number
- %PIX|ASA-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
- %PIX|ASA-3-318006: if interface_name if_state number
- %PIX|ASA-3-318007: OSPF is enabled on interface_name during idb initialization
- %PIX|ASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %PIX|ASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line_num
- %PIX|ASA-3-319001: Acknowledge for arp update for IP address dest_address not received (number).
- %PIX|ASA-3-319002: Acknowledge for route update for IP address dest_address not received (number).
- %PIX|ASA-3-319003: Arp update for IP address address to NPn failed.
- %PIX|ASA-3-319004: Route update for IP address dest_address failed (number).
- %PIX|ASA-3-320001: The subject name of the peer cert is not allowed for connection
- %PIX|ASA-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %PIX|ASA-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.
- %PIX|ASA-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.
- %ASA-3-323001: Module in slot slotnum experienced a control channel communications failure.
- %ASA-3-323002: Module in slot slotnum is not able to shut down, shut down request not answered.
- %ASA-3-323003: Module in slot slotnum is not able to reload, reload request not answered.

- %ASA-3-323004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.
- %ASA-3-323005: Module in slot slotnum can not be powered on completely
- %ASA-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.
- %PIXIASA-3-324000: Drop GTPv version message msg_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port Reason: reason
- %PIXIASA-3-324001: GTPv0 packet parsing error from source_interface:source_address/source_port to dest_interface:dest_address/dest_port, TID: tid_value, Reason: reason
- %PIXIASA-3-324002: No PDP[MCB] exists to process GTPv0 msg_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port, TID: tid_value
- %PIXIASA-3-324003: No matching request to process GTPv version msg_type from source_interface:source_address/source_port to source_interface:dest_address/dest_port
- %PIXIASA-3-324004: GTP packet with version%d from source_interface:source_address/source_port to dest_interface:dest_address/dest_port is not supported
- %PIXIASA-3-324005: Unable to create tunnel from source_interface:source_address/source_port to dest_interface:dest_address/dest_port
- %PIXIASA-3-324006:GSN IP_address tunnel limit tunnel_limit exceeded, PDP Context TID tid failed
- %PIXIASA-3-324007: Unable to create GTP connection for response from:source_address/0 to dest_address/dest_port
- %PIX-3-324300: Radius Accounting Request from from_addr has an incorrect request authenticator
- %PIXIASA-3-324301: Radius Accounting Request has a bad header length hdr_len, packet length pkt_len
- %PIXIASA-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings
- %PIX-3-325003: EUI-64 source address check failed. Dropped packet from interface_in:source_address/source_port to dest_address/dest_port with source MAC address MAC_address.
- %PIXIASA-3-326001: Unexpected error in the timer library: error_message
- %PIXIASA-3-326002: Error in error_message: error_message
- %PIXIASA-3-326004: An internal error occurred while processing a packet queue
- %PIXIASA-3-326005: Mrib notification failed for (IP_address, IP_address)
- %PIXIASA-3-326006: Entry-creation failed for (IP_address, IP_address)
- %PIXIASA-3-326007: Entry-update failed for (IP_address, IP_address)
- %PIXIASA-3-326008: MRIB registration failed
- %PIXIASA-3-326009: MRIB connection-open failed
- %PIXIASA-3-326010: MRIB unbind failed
- %PIXIASA-3-326011: MRIB table deletion failed
- %PIXIASA-3-326012: Initialization of string functionality failed

- %PIX|ASA-3-326013: Internal error: string in string line %d (%s)
- %PIX|ASA-3-326014: Initialization failed: error_message error_message
- %PIX|ASA-3-326015: Communication error: error_message error_message
- %PIX|ASA-3-326016: Failed to set un-numbered interface for interface_name (string)
- %PIX|ASA-3-326017: Interface Manager error - string in string: string
- %PIX|ASA-3-326019: string in string: string
- %PIX|ASA-3-326020: List error in string: string
- %PIX|ASA-3-326021: Error in string: string
- %PIX|ASA-3-326022: Error in string: string
- %PIX|ASA-3-326023: string - IP_address: string
- %PIX|ASA-3-326024: An internal error occurred while processing a packet queue.
- %PIX|ASA-3-326025: string
- %PIX|ASA-3-326026: Server unexpected error: error_message
- %PIX|ASA-3-326027: Corrupted update: error_message
- %PIX|ASA-3-326028: Asynchronous error: error_message
- %PIX|ASA-3-327001: IP SLA Monitor: Cannot create a new process
- %PIX|ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %PIX|ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %PIX|ASA-3-328001: Attempt made to overwrite a set stub function in string.
- %PIX|ASA-3-329001: The string0 subblock named string1 was not removed
- ASA|PIX-3-331001: Dynamic DNS Update for 'fqdn_name' <=> ip_address failed
- %ASA|PIX-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.
- %ASA|PIX-3-332002: Unable to allocate message buffer, WCCP V2 closing down.
- %ASA-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up
- %ASA-3-336002: Handle handle_id is not allocated in pool.
- %ASA-3-336003: No buffers available for bytes byte packet
- %ASA-3-336004: Negative refcount in pakdesc pakdesc.
- %ASA-3-336005: Flow control error, error, on interface_name.
- %ASA-3-336006: num peers exist on IIDB interface_name.
- %ASA-3-336007: Anchor count negative
- %ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str
- %ASA-3-336009 ddb_name as_id: Internal Error
- %ASA-3-337001: Phone Proxy SRTP: Encryption failed on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-3-337002: Phone Proxy SRTP: Decryption failed on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port

- %ASA-3-337003: Phone Proxy SRTP: Authentication tag generation failed on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-3-337004: Phone Proxy SRTP: Authentication tag validation failed on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-3-337005: Phone Proxy SRTP: Media session not found on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-3-337006: Phone Proxy SRTP: Failed to sign file filename requested by UDP client cifc:caddr/cport for sifc:saddr/sport
- %ASA-3-337007: Phone Proxy SRTP: Failed to find configuration file filename for UDP client cifc:caddr/cport by server sifc:saddr/sport
- %ASA-3-337008: Phone Proxy: Unable to allocate media port from media-termination address phone_proxy_ifc:media_term_IP for client_ifc:client_IP/client_port; call failed.
- %ASA-3-337009: Unable to create secure phone entry, interface:IPaddr is already configured for the same MAC mac_addr.
- %ASA-3-339001: UC-IME-SIG: Ticket not found in SIP %s from %s:%A/%d to %s:%A/%d, packet dropped
- %ASA-3-339002: UC-IME-SIG: Invalid ticket in SIP %s from %s:%A/%d to %s:%A/%d, packet dropped, %s
- %ASA-3-339003: UC-IME-SIG: Non-dialog forming SIP %s received from %s:%A/%d to %s:%A/%d, packet dropped
- %ASA-3-339004: UC-IME-SIG: Dropping SIP %s received from %s:%A/%d to %s:%A/%d, route header validation failed, %s
- %ASA-3-339005: UC-IME-SIG: Message received from %s:%A/%d to %s:%A/%d does not contain SRTP, message dropped
- %ASA-3-339006: UC-IME-Offpath: Failed to map remote UCM address %A:%d on %s interface, request from local UCM %A:%d on %s interface, reason %s
- %PIXIASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface_name AC:ac_name
- %PIXIASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface_name AC:ac_name
- %PIXIASA-3-403503: PPPoE:PPP link down:reason
- %PIXIASA-3-403504: PPPoE:No 'vpdn group group_name' for PPPoE is created
- %PIXIASA-3-403507:PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name
- %PIXIASA-3-404102: ISAKMP: Exceeded embryonic limit
- %PIXIASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
- %PIXIASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
- %ASA-3-414003: TCP Syslog Server intf: IP_Address/port not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.
- %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc_in:SIP to ifc_out:DIP (typeICMP_TYPE, code ICMP_CODE)"

- %ASA-3-420006 : Virtual Sensor not present and fail-close mode used, dropping protocol packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT\n
- %ASA-3-421001: TCPIUDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.
- %ASA-3-421003: Invalid data plane encapsulation.
- %ASA-3-421007: TCPIUDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.
- %ASA-3-505016: prod_id Module in slot slot application changed from: name version version state state to: name version state state.
- %ASA-3-500005: connection terminated from in_ifc_name:src_address/src_port to out_ifc_name:dest_address/dest_port due to invalid combination of inspections on same flow. Inspect inspect_name is not compatible with inspect inspect_name_2
- %ASA-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
- %PIX|ASA-3-610001: NTP daemon interface interface_name: Packet denied from IP_address
- %PIX|ASA-3-610002: NTP daemon interface interface_name: Authentication failed for packet from IP_address
- %PIX|ASA-3-611313: VPNClient: Backup Server List Error: reason
- %PIX|ASA-3-702305: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to sequence number rollover.
- %PIX|ASA-3-702307: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.
- %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %PIX|ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %PIX|ASA-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %PIX|ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIX|ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %PIX|ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %PIX|ASA-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %PIX|ASA-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %PIX|ASA-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %PIX|ASA-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %PIX|ASA-3-713033: Received invalid remote Proxy Range IP_address - IP_address
- %PIX|ASA-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address
- %PIX|ASA-3-713043: Cookie/peer address IP_address session already in progress
- %PIX|ASA-3-713048: Error processing payload: Payload ID: id
- %PIX|ASA-3-713051: Terminating connection attempt: IPSEC not permitted for group (group_name)
- %PIX|ASA-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!

- %PIXIASA-3-713059: Tunnel Rejected: User (user) matched with group name, group-lock check failed.
- %PIXIASA-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.
- %PIXIASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!
- %PIXIASA-3-713062: IKE Peer address same as our interface address IP_address
- %PIXIASA-3-713063: IKE Peer address not configured for destination IP_address
- %PIXIASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %PIXIASA-3-713072: Password for user (user) too long, truncating to number characters
- %PIXIASA-3-713081: Unsupported certificate encoding type encoding_type
- %PIXIASA-3-713082: Failed to retrieve identity certificate
- %PIXIASA-3-713083: Invalid certificate handle
- %PIXIASA-3-713084: Received invalid phase 1 port value (port) in ID payload
- %PIXIASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %PIXIASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %PIXIASA-3-713088: Set Cert filehandle failure: no IPSec SA in group group_name
- %PIXIASA-3-713098: Aborting: No identity cert specified in IPSec SA (SA_name)!
- %PIXIASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %PIXIASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %PIXIASA-3-713107: IP_Address request attempt failed!
- %PIXIASA-3-713109: Unable to process the received peer certificate
- %PIXIASA-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!
- %PIXIASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIXIASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %PIXIASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %PIXIASA-3-713118: Detected invalid Diffie-Hellman group_descriptor group_number, in IKE area
- %PIXIASA-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)
- %PIXIASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)
- %PIXIASA-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %PIXIASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %PIXIASA-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %PIXIASA-3-713132: Cannot obtain an IP_address for remote peer

- %PIX|ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number)
- %PIX|ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %PIX|ASA-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
- %PIX|ASA-3-713140: Split Tunneling Policy requires network list but none configured
- %PIX|ASA-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
- %PIX|ASA-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
- %PIX|ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
- %PIX|ASA-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
- %PIX|ASA-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
- %PIX|ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %PIX|ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %PIX|ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %PIX|ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %PIX|ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %PIX|ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %PIX|ASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %PIX|ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %PIX|ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
- %PIX|ASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %PIX|ASA-3-713185: Error: Username too long - connection aborted
- %PIX|ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value) is illegal
- %PIX|ASA-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.
- %PIX|ASA-3-713193: Received packet with missing payload, Expected payload: payload_id
- %PIX|ASA-3-713194: IKE|IPSec Delete With Reason message: termination_reason
- %PIX|ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %PIX|ASA-3-713198: User Authorization failed: user User authorization failed.

- %PIXIASA-3-713203: IKE Receiver: Error reading from socket.
- %PIXIASA-3-713205: Could not add static route for client address: IP_address
- %PIXIASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %PIXIASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id
- %PIXIASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %PIXIASA-3-713210: Cannot create dynamic map for Backup L2L entry rule_id
- %PIXIASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %PIXIASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %PIXIASA-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version
- %PIXIASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %PIXIASA-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group
- %PIXIASA-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
- %PIXIASA-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type
- %PIXIASA-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type
- %PIXIASA-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
- %PIXIASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %PIXIASA-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
- %PIXIASA-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
- %PIXIASA-3-713902 descriptive_event_string
- %ASA-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason
- %ASA-3-716057: Group group User user IP ip Session terminated, no type license available.
- %PIXIASA-3-717001: Querying keypair failed.
- %PIXIASA-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.
- %PIXIASA-3-717009: Certificate validation failed. Reason: reason_string.
- %PIXIASA-3-717010: CRL polling failed for trustpoint trustpoint_name.
- %PIXIASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure

- %PIX|ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %PIX|ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %PIX|ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)
- %PIX|ASA-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.
- %PIX|ASA-3-717020: Failed to install device certificate for trustpoint label. Reason: reason_string.
- %PIX|ASA-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.
- %PIX|ASA-3-717023: SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason_string.
- %PIX|ASA-3-717027: Certificate chain failed validation. reason_string.
- %PIX-3-717032: OCSP status check failed. Reason: reason_string.
- %ASA-3-717039: Local CA Server internal error detected: error.
- %ASA-3-717042: Failed to enable Local CA Server.Reason: reason.
- %ASA-3-717044: Local CA server certificate enrollment related error for user: user. Error: error.
- %ASA-3-717046: Local CA Server CRL error: error.
- %ASA-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.
- %ASA-3-719008: Email Proxy service is shutting down.
- %ASA-3-722007: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722008: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722009: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection
- %ASA-3-722021: Group group User user-name IP IP_address Unable to start compression due to lack of memory resources
- %ASA-3-722035: Group group User user-name IP IP_address Received large packet length (threshold num) .
- %ASA-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).
- %ASA-3-722045: Connection terminated: no SSL tunnel initialization data.
- %ASA-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.
- %ASA-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.
- %ASA-3-7340004: DAP: Processing error: Code number
- %ASA-3-737002: IPAA: Received unknown message 'num'
- %ASA-3-737023: IPAA: Unable to allocate memory to store local pool address ip-address

- %ASA-3-737027: IPAA: No data for address request
- %ASA-3-742001: failed to read master key for password encryption from persistent store
- %ASA-3-742002: failed to set master key for password encryption
- %ASA-3-742003: failed to save master key for password encryption, reason reason_text
- %ASA-3-742004: failed to sync master key for password encryption, reason reason_text
- %ASA-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with
- %ASA-3-742006: password decryption failed due to unavailable memory
- %ASA-3-742007: password encryption failed due to unavailable memory
- %ASA-3-742008: password enc_pass decryption failed due to decoding error
- %ASA-3-742009: password encryption failed due to decoding error
- %ASA-3-742010: encrypted password enc_pass is not well formed
- %ASA-3-800001: DSI: Internal Structure Error
- %ASA-3-800002: DSI: Execution error on CLI command *cmd_string*

Warning Messages, Severity 4

The following messages appear at severity 4, warning:

- %PIXIASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID
- %PIXIASA-4-106027:Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC
- %PIXIASA-4-108004: action_class: action ESMTP req_resp from src_ifc:siplsport to dest_ifc:dipldport;further_info, page 1-23
- %PIXIASA-4-109017: User at IP_address exceeded auth proxy connection limit (max)
- %PIXIASA-4-109022: exceeded HTTPS proxy process limit
- %PIXIASA-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %PIXIASA-4-109028: aaa bypassed for same-security traffic from ingress_ interface:source_address/source_port to egress_interface:dest_address/dest_port
- %PIXIASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.
- %PIXIASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username.
- %PIXIASA-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol connections
- %PIXIASA-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
- %PIXIASA-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %ASA-4-120004: Event group 'title' was dropped. Reason 'reason'.

- %ASA-4-120005: Message group to 'destination' was dropped. Reason 'reason'.
- %ASA-4-120006: Delivering message group to 'destination' failed. Reason: 'reason'
- %PIX|ASA-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
- %PIX|ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number
- %PIX|ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %PIX|ASA-4-216004:prevented: error in function at file(line) - stack trace
- %PIX|ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign address/foreign-port to laddr interface:local-address/local-port
- %PIX|ASA-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address
- %PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface interface_name to dest_address:no matching session
- %PIX|ASA-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 dst dest_interface_name:dest_address (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address/source_port dst dest_address/dest_port
- %PIX|ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %PIX|ASA-4-335005: NAC Downloaded ACL parse failure - host-address
- %ASA-4-337004: Phone Proxy SRTP: Authentication tag validation failed on packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-4-338005: Dynamic filter dropped black listed 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-level: level_value, category: category_name
- %ASA-4-338006: Dynamic filter dropped black listed 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-level: level_value, category: category_name
- %ASA-4-338007: Dynamic filter dropped black listed 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: ip address/netmask, threat-level: level_value, category: category_name
- %ASA-4-338008: Dynamic filter dropped black listed 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, threat-level: level_value, category: category_name
- %ASA-4-338201: Dynamic filter monitored grey listed 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-level: level_value, category: category_name

- %ASA-4-338202: Dynamic filter monitored grey listed 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-level: level_value, category: category_name
- %ASA-4-338203: Dynamic filter dropped grey listed 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-level: level_value, category: category_name
- %ASA-4-338204: Dynamic filter dropped grey listed 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-level: level_value, category: category_name
- %PIXIASA-4-4000nn: IPS:number string from IP_address to IP_address on interface interface_name
- %PIXIASA-4-401001: Shuns cleared
- %PIXIASA-4-401002: Shun added: IP_address IP_address port port
- %PIXIASA-4-401003: Shun deleted: IP_address
- %PIXIASA-4-401004: Shunned packet: IP_address ==> IP_address on interface interface_name
- %PIXIASA-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port
- %PIXIASA-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.
- %PIXIASA-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.
- %PIXIASA-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 .
- %PIXIASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
- %PIXIASA-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.
- %PIXIASA-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.
- %PIXIASA-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed authentication.
- %PIXIASA-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).
- %PIXIASA-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).
- %PIXIASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command .

- %ASA-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).
- %ASA-4-402125: The ASA hardware accelerator ring timed out (parameters).
- %ASA-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.
- %ASA-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.
- %PIX|ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel_id=number, session_id=number
- %PIX|ASA-4-403102: PPP virtual interface interface_name rcvd pkt with invalid protocol: protocol, reason: reason.
- %PIX|ASA-4-403103: PPP virtual interface max connections reached.
- %PIX|ASA-4-403104: PPP virtual interface interface_name requires mschap for MPPE.
- %PIX|ASA-4-403106: PPP virtual interface interface_name requires RADIUS for MPPE.
- %PIX|ASA-4-403107: PPP virtual interface interface_name missing aaa server group info
- %PIX|ASA-4-403108: PPP virtual interface interface_name missing client ip address option
- %PIX|ASA-4-403109: Rec'd packet not an PPTP packet. (ip) dest_address= dest_address, src_addr= source_address, data: string.
- %PIX|ASA-4-403110: PPP virtual interface interface_name, user: user missing MPPE key from aaa server.
- %PIX|ASA-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
- %PIX|ASA-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name
- %PIX|ASA-4-404101: ISAKMP: Failed to allocate address for client from pool string
- %PIX|ASA-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
- %PIX|ASA-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
- %PIX|ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %PIX|ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %PIX|ASA-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex
- %PIX|ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP
- %PIX|ASA-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest
- %PIX|ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s\n
- %PIX|ASA-4-405201: ILS ILS_message_type from inside_interface:source_IP_address to outside_interface:/destination_IP_address has wrong embedded address embedded_IP_address
- %PIX|ASA-4-405300: Radius Accounting Request received from from_addr is not allowed

- %PIXIASA-4-405301: Attribute attribute_number does not match for user user_ip
- %PIXIASA-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name
- %PIXIASA-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
- %PIXIASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded
- %PIXIASA-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
- %PIXIASA-4-407003: Established limit for RPC services exceeded number
- %PIXIASA-4-408001: IP route counter negative - reason, IP_address Attempt: number
- %PIXIASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %PIXIASA-4-408003: can't track this type of object hex
- %PIXIASA-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls
- %PIXIASA-4-409002: db_free: external LSA IP_address netmask
- %PIXIASA-4-409003: Received invalid packet: reason from IP_address, interface_name
- %PIXIASA-4-409004: Received reason from unknown neighbor IP_address
- %PIXIASA-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name
- %PIXIASA-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name
- %PIXIASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask
- %PIXIASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric : number area : string
- %PIXIASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %PIXIASA-4-409010: Virtual link information found in non-backbone area: string
- %PIXIASA-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %PIXIASA-4-409012: Detected router with duplicate router ID IP_address in area string
- %PIXIASA-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %PIXIASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user :Auth-server group server_tag unreachable
- %PIXIASA-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.
- %PIXIASA-4-410003: action_class: action DNS query_response from src_ifc:sip/sport to dest_ifc:dip/dport; further_info
- %PIXIASA-4-411001: Line protocol on interface interface_name changed state to up

- %PIX|ASA-4-411002: Line protocol on interface interface_name changed state to down
- %PIX|ASA-4-411003: Configuration status on interface interface_name changed state to downup
- %PIX|ASA-4-411004: Configuration status on interface interface_name changed state to up
- %ASA-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
- %PIX|ASA-4-412001: MAC MAC_address moved from interface_1 to interface_2
- %PIX|ASA-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
- %ASA-4-413001: Module in slot slotnum is not able to shut down. Module Error: errnum message
- %ASA-4-413002: Module in slot slotnum is not able to reload. Module Error: errnum message
- %ASA-4-413003: Module in slot slotnum is not a recognized type
- %ASA-4-413004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Trying again.
- %ASA-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.
- %PIX|ASA-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
- %PIX|ASA-4-416001: Dropped UDP SNMP packet from source_interface :source_IP/source_port to dest_interface:dest_address/dest_port; version (prot_version) is not allowed through the firewall
- %PIX|ASA-4-417001: Unexpected event received: number
- %PIX|ASA-4-417004: Filter violation error: conn number (string:string) in string
- %PIX|ASA-4-417006: No memory for string) in string. Handling: string
- %PIX-4-417008 AutoRP: removed string embedded group address1/mask1 on interface interface-name from address2 due to overlap address3/mask2
- %PIX-4-417009 AutoRp: discarded string on interface interface-name from address due to malformed packet
- %PIX|ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) to interface_name IP_address (port)
- %PIX|ASA-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
- %ASA-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.
- ASA-4-419003: Cleared TCP urgent flag from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port.
- %ASA-4-420002 : IPS requested to drop ICMP packets ifc_in:SIP to ifc_out:DIP (typeICMP_TYPE, code ICMP_CODE)"
- %ASA-4-420003 : IPS requested to reset TCP connection from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT"
- %ASA-4-420007: application-string cannot be enabled for the module in slot slot_id. The module's current software version does not support this feature. Please upgrade the software on the module in slot slot_id to support this feature. Received backplane header version version_number, required backplane header version version_number or higher.
- %PIX|ASA-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1

- %PIXIASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %PIXIASA-4-422006: IP SLA Monitor Probe number: string
- %ASA-4-423001: { Allowed | Dropped } invalid NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
- %ASA-4-423002: { Allowed | Dropped } mismatched NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
- %ASA-4-423003: { Allowed | Dropped } invalid NBDGM pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
- %ASA-4-423004: { Allowed | Dropped } mismatched NBDGM pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
- %ASA-4-423005: { Allowed | Dropped } NBDGM pkt_type_name fragment with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
- %ASA-4-424001: Packet denied protocol_string intf_in:src_ip/src_port intf_out:dst_ip/dst_port. [Ingress|Egress] interface is in a backup state.
- %ASA-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port
- %PIXIASA-4-431001: RTP conformance: Dropping RTP packet from in_ifc:src_ip/src_port to out_ifc:dst_ip/dst_port, Drop reason: drop_reason value
- %PIXIASA-4-431002: RTCP conformance: Dropping RTCP packet from in_ifc:src_ip/src_port to out_ifc:dst_ip/dst_port, Drop reason: drop_reason value
- %ASA-4-444005: Temporary license key key will expire in days days
- %ASA-4-446001: Maximum TLS Proxy session limit of max_sess reached.
- %ASA-4-446002: Denied TLS Proxy session from src_ifc: src_ip/src_port to dest_ifc: dest_ip/dst_port, licensed UC Proxy session limit of lic_num exceeded.
- %ASA-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.
- %ASA-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
- %ASA-4-450001: Deny traffic for protocol protocol_id src interface_name:IP_address/port dst interface_name:IP_address/port, licensed host limit of num exceeded.
- %ASA-4-466002: Denied TLS Proxy session from src_ifc: src_ip/src_port to src_ifc: dest_ip/dst_port, licensed UC Proxy session limit of lic_num exceeded
- %PIXIASA-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %PIXIASA-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %PIXIASA-4-607002: action_class: action SIP req_resp req_resp_info from src_ifc:sip/sport to dest_ifc:dip/dport; further_info
- %PIXIASA-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dst_ip/dst_port, SCCPPrefix length value too small
- %PIXIASA-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dst_ip/dst_port, SCCPPrefix length value too large
- %PIXIASA-4-608004: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dst_ip/dst_port, message id value not allowed

- %PIX|ASA-4-608005: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, message id value registration not complete
- %PIX|ASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %PIX|ASA-4-612003:Auto Update failed to contact:url, reason:reason
- %PIX|ASA-4-620002: Unsupported CTIQBE version: hex: from interface_name:IP_address/port to interface_name:IP_address/port
- %ASA-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call stack
- %PIX|ASA-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %PIX|ASA-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %ASA-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %ASA-4-713240: Received DH key with bad length: received length=rlength expected length=length
- %ASA-4-713241: IE Browser Proxy Method setting_number is Invalid
- %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %ASA-4-713243: META-DATA Unable to find the requested certificate
- %ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %ASA-4-713249: META-DATA Received unsupported authentication results: result
- %ASA-4-713251: META-DATA Received authentication failure message
- %ASA-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name 'group-name'
- %PIX|ASA-4-713903:descriptive_event_string.
- %ASA-4-716007: Group group User user WebVPN Unable to create session.
- %ASA-4-716022: Unable to connect to proxy server reason.
- %ASA-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.
- %ASA-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.
- %ASA-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.
- %ASA-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.
- %ASA-4-716047: Group group-name User user-name IP IP_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.

- %ASA-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.
- %ASA-4-716052: Group group-name User user-name IP IP_address Pending session terminated.
- %PIXIASA-4-717026: Name lookup failed for hostname hostname during PKI operation.
- %PIXIASA-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string
- %PIXIASA-4-717035: OCSP status is being checked for certificate. certificate_identifier.
- %PIXIASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.
- %ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %ASA-4-720009: (VPN-unit) Failed to create version control block.
- %ASA-4-720011: (VPN-unit) Failed to allocate memory
- %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name
- %ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.
- %ASA-4-720038: (VPN-unit) Corrupted message from active unit.
- %ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %ASA-4-720044: (VPN-unit) Failed to receive message from active unit
- %ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.
- %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port
- %ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.
- %ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.
- %ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %ASA-4-720066: (VPN-unit) Failed to activate IKE database.
- %ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %ASA-4-720068: (VPN-unit) Failed to parse peer message.
- %ASA-4-720069: (VPN-unit) Failed to activate cTCP database.
- %ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %ASA-4-720073: (VPN-unit) Fail to insert certificate in trust point trustpoint on the standby unit.
- %ASA-4-721007: (device) Fail to update access list list_name on standby unit.
- %ASA-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.

- %ASA-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.
- %ASA-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.
- %ASA-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.
- %ASA-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.
- %ASA-4-722001: IP IP_address Error parsing SVC connect request.
- %ASA-4-722002: IP IP_address Error consolidating SVC connect request.
- %ASA-4-722003: IP IP_address Error authenticating SVC connect request.
- %ASA-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
- %ASA-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num
- %ASA-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length
- %ASA-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
- %ASA-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version
- %ASA-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length
- %ASA-4-722039: Group group, User user, IP ip, SVC 'vpn-filter acl' is an IPv6 ACL; ACL not applied.
- %ASA-4-722040: Group group, User user, IP ip, SVC 'ipv6-vpn-filter acl' is an IPv4 ACL; ACL not applied
- %ASA-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection\n.
- %ASA-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
- %ASA-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
- %ASA-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
- %ASA-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
- %ASA-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
- %ASA-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.
- %ASA-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.
- %ASA-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
- %ASA-4-733101: Object objectIP (is targetedlls 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.
- %ASA-4-733102:Threat-detection adds host %I to shun list

- %ASA-4-733103: Threat-detection removes host %I from shun list
- %ASA-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED
- %ASA-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED
- %ASA-4-737012: IPAA: Address assignment failed
- %ASA-4-737013: IPAA: Error freeing address ip-address, not found
- %ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
- %ASA-4-737025: IPAA: Not releasing local pool ip-address, due to local pool duplicate issue
- %ASA-4-737028: IPAA: Adding ip-address to standby: failed
- %ASA-4-737030: IPAA: Adding %m to standby: address already in use
- %ASA-4-737032: IPAA: Removing ip-address from standby: not found

Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

- %PIXIASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %PIXIASA-5-109029: Parsing downloaded ACL: string
- %PIXIASA-5-111002: Begin configuration: IP_address reading from device
- %PIXIASA-5-111003: IP_address Erase configuration
- %PIXIASA-5-111004: IP_address end configuration: {FAILED|OK}
- %PIXIASA-5-111005: IP_address end configuration: OK
- %PIXIASA-5-111007: Begin configuration: IP_address reading from device.
- %PIXIASA-5-111008: User user executed the command string
- %ASA-5-111010: User username, running application-name from IP ip addr, executed cmd
- %ASA-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate
- %ASA-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip
- %ASA-5-120001: Smart Call Home Module was started.
- %ASA-5-120002: Smart Call Home Module was terminated.
- %ASA-5-120008: SCH client 'client' was activated.
- %ASA-5-120009: SCH client 'client' was deactivated.
- %PIXIASA-5-199001: Reload command executed from telnet (remote IP_address).
- %PIX-5-199006: Orderly reload started at when by whom. Reload reason: reason
- %PIX-5-199007: Reload scheduled for when by whom at when-command-issued. Reload reason: reason
- %PIX-5-199008: Scheduled reload for when-reload-is-supposed-to-happen cancelled by whom at when.
- %PIXIASA-5-303003: FTP cmd_string command denied - failed strict inspection, terminating connection from %s:%A/%d to %s:%A/%d\n.

- %PIX|ASA-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
- %PIX|ASA-5-304001: user source_address Accessed {JAVA URL|URL} dest_address: url.
- %PIX|ASA-5-304002: Access denied URL chars SRC IP_address DEST IP_address: chars
- %PIX|ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name:source_address/source_port dest interface_name:dest_address/dest_port denied due to NAT reverse path failure.
- %PIX|ASA-5-321001: Resource var1 limit of var2 reached.
- %PIX|ASA-5-321002: Resource var1 rate limit of var2 reached.
- ASA|PIX-5-331002: Dynamic DNS type RR for ('fqdn_name' -> ip_address | ip_address -> 'fqdn_name') successfully updated in DNS server dns_server_ip
- %ASA|PIX-5-332003: Web Cache IP_address/service_ID acquired
- %PIX|ASA-5-333002: Timeout waiting for EAP response - context:EAP-context
- %PIX|ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %PIX|ASA-5-334002: EAPoUDP association successfully established - host-address
- %PIX|ASA-5-334003: EAPoUDP association failed to establish - host-address
- %PIX|ASA-5-334005: Host put into NAC Hold state - host-address
- %PIX|ASA-5-334006: EAPoUDP failed to get a response from host - host-address
- %PIX|ASA-5-335002: Host is on the NAC Exception List - host-address, OS:oper-sys
- %PIX|ASA-5-335003: NAC Default ACL applied, ACL:ACL-name - host-address
- %PIX|ASA-5-335008: NAC IPsec terminate from dynamic ACL:ACL-name - host-address
- %ASA-5-336010 EIGRP-<ddb_name> tableid as_id: Neighbor address (%interface) is event_msg: msg
- %ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %PIX|ASA-5-415004: HTTP - matched matched_string in policy-map map_name, content-type verification failed connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415005: HTTP - matched matched_string in policy-map map_name, URI length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415006: HTTP - matched matched_string in policy-map map_name, URI matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415007: HTTP - matched matched_string in policy-map map_name, Body matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415008: HTTP - matched matched_string in policy-map map_name, header matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415009: HTTP - matched matched_string in policy-map map_name, method matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIX|ASA-5-415010: matched matched_string in policy-map map_name, transfer encoding matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num

- %PIXIASA-5-415011: HTTP - policy-map map_name:Protocol violation connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415012: HTTP - matched matched_string in policy-map map_name, Unknown mime-type connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415013: HTTP - policy-map map_name:Malformed chunked encoding connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415014: HTTP - matched matched_string in policy-map map_name, Mime-type in response wasn't found in the accept-types of the request connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415015: HTTP - matched matched_string in policy-map map_name, transfer-encoding unknown connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415018: HTTP - matched matched_string in policy-map map_name, Header length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415019: HTTP - matched matched_string in policy-map map_name, status line matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-415020: HTTP - matched matched_string in policy-map map_name, a non-ASCII character was matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-5-500001: ActiveX content modified src IP_address dest IP_address on interface interface_name.
- %PIXIASA-5-500002: Java content modified src IP_address dest IP_address on interface interface_name.
- %PIXIASA-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
- %PIXIASA-5-501101: User transitioning priv level
- %PIXIASA-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %PIXIASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %PIXIASA-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %PIXIASA-5-502111: New group policy added: name: policy_name Type: policy_type
- %PIXIASA-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %PIXIASA-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason
- %PIXIASA-5-504001: Security context context_name was added to the system
- %PIXIASA-5-504002: Security context context_name was removed from the system
- %ASA-5-505001: Module in slot slotnum is shutting down. Please wait...
- %ASA-5-505002: Module in slot slotnum is reloading. Please wait...
- %ASA-5-505003: Module in slot slotnum is resetting. Please wait...
- %ASA-5-505004: Module in slot slotnum shutdown is complete.
- %ASA-5-505005: Module in slot slotnum is initializing control communication. Please wait...

- %ASA-5-505006: Module in slot slotnum is Up.
- %ASA-5-505007: Module in slot slotnum is recovering. Please wait...
- %ASA-5-505008: Module in slot slotnum software is being updated to vnewver (currently vver)
- %ASA-5-505009: Module in slot slotnum software was updated to vnewver (previously vver)
- %ASA-5-505010: Module in slot slot removed.
- %ASA-5-505012: Module in slot slot, application stopped application, version version
- %ASA-5-505013: Module in slot slot application changed from: application version version to: newapplication version newversion.
- %ASA-5-506001: event_source_string event_string
- %PIX|ASA-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
- %PIX|ASA-5-508001: DCERPC message_type non-standard version_type version version_number from src_if:src_ip/src_port to dest_if:dest_ip/dest_port, terminating connection.
- %PIX|ASA-5-508002: DCERPC response has low endpoint port port_number from src_if:src_ip/src_port to dest_if:dest_ip/dest_port, terminating connection.
- %ASA-5-509001: Connection attempt from src_intf:src_ip/src_port to dst_intf:dst_ip/dst_port was prevented by “no forward” command.
- %PIX|ASA-5-611103: User logged out: Uname: user
- %PIX|ASA-5-611104: Serial console idle timeout exceeded
- %PIX|ASA-5-612001: Auto Update succeeded:filename, version:number
- %ASA-5-711005: Traceback: call_stack
- %PIX|ASA-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
- %PIX|ASA-5-713010: IKE area: failed to find centry for message Id message_number
- %PIX|ASA-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)
- %PIX|ASA-5-713049: Security negotiation complete for tunnel_type type (group_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %PIX|ASA-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address
- %PIX|ASA-5-713068: Received non-routine Notify message: notify_type (notify_value)
- %PIX|ASA-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger_value to smaller_value seconds
- %PIX|ASA-5-713074: Responder forcing change of IPSec rekeying duration from larger_value to smaller_value Kbs
- %PIX|ASA-5-713075: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value seconds
- %PIX|ASA-5-713076: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value Kbs
- %PIX|ASA-5-713092: Failure during phase 1 rekeying attempt due to collision

- %PIXIASA-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %PIXIASA-3-713119: PHASE 1 COMPLETED
- %PIXIASA-5-713120: PHASE 2 COMPLETED (msgid=msg_id)
- %PIXIASA-5-713130: Received unsupported transaction mode attribute: attribute id
- %PIXIASA-5-713131: Received unknown transaction mode attribute: attribute_id
- %PIXIASA-5-713135: message received, redirecting tunnel to IP_address.
- %PIXIASA-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
- %PIXIASA-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
- %PIXIASA-5-713139: group_name not found, using BASE GROUP default preshared key
- %PIXIASA-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction
- %PIXIASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask
- %PIXIASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %PIXIASA-5-713156: Initializing Backup Server [server_name or IP_address]
- %PIXIASA-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %PIXIASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %PIXIASA-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload
- %PIXIASA-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!
- %PIXIASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.
- %PIXIASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
- %PIX-5-713201: Duplicate (Phase 1/Phase 2) packet detected.(Retransmitting test packet/No last packet to retransmit.)
- %PIXIASA-5-713216: Rule: action Client type: version Client: type version is/is not allowed
- %PIXIASA-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
- %PIXIASA-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %ASA-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
- %ASA-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.

- %ASA-5-713257: Phase var1 failure: Mismatched attribute types for class var2: Rcv'd: var3 Cfg'd: var4
- %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason
- %PIX|ASA-5-713904:descriptive_event_string.
- %ASA-5-716053: SSO Server added: name: name Type: type
- %ASA-5-716054: SSO Server deleted: name: name Type: type
- %PIX|ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %PIX|ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %PIX|ASA-5-718002: Create peer IP_address failure, already at maximum of number_of_peers
- %PIX|ASA-5-718005: Fail to send to IP_address, port port
- %PIX|ASA-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]
- %PIX|ASA-5-718007: Socket open failure failure_code
- %PIX|ASA-5-718008: Socket bind failure failure_code
- %PIX|ASA-5-718009: Send HELLO response failure to IP_address
- %PIX|ASA-5-718010: Sent HELLO response to IP_address
- %PIX|ASA-5-718011: Send HELLO request failure to IP_address
- %PIX|ASA-5-718012: Sent HELLO request to IP_address
- %PIX|ASA-5-718014: Master peer IP_address is not answering HELLO
- %PIX|ASA-5-718015: Received HELLO request from IP_address
- %PIX|ASA-5-718016: Received HELLO response from IP_address
- %PIX|ASA-5-718024: Send CFG UPDATE failure to IP_address
- %PIX|ASA-5-718028: Send OOS indicator failure to IP_address
- %PIX|ASA-5-718031: Received OOS obituary for IP_address
- %PIX|ASA-5-718032: Received OOS indicator from IP_address
- %PIX|ASA-5-718033: Send TOPOLOGY indicator failure to IP_address
- %PIX|ASA-5-718042: Unable to ARP for IP_address
- %PIX|ASA-5-718043: Updating/removing duplicate peer entry IP_address
- %PIX|ASA-5-718044: Deleted peer IP_address
- %PIX|ASA-5-718045: Created peer IP_address
- %PIX|ASA-5-718048: Create of secure tunnel failure for peer IP_address
- %PIX|ASA-5-718050: Delete of secure tunnel failure for peer IP_address
- %PIX|ASA-5-718052: Received GRAT-ARP from duplicate master MAC_address
- %PIX|ASA-5-718053: Detected duplicate master, mastership stolen MAC_address
- %PIX|ASA-5-718054: Detected duplicate master MAC_address and going to SLAVE
- %PIX|ASA-5-718055: Detected duplicate master MAC_address and staying MASTER
- %PIX|ASA-5-718057: Queue send failure from ISR, msg type failure_code

- %PIXIASA-5-718060: Inbound socket select fail: context=context_ID.
- %PIXIASA-5-718061: Inbound socket read fail: context=context_ID.
- %PIXIASA-5-718062: Inbound thread is awake (context=context_ID).
- %PIXIASA-5-718063: Interface interface_name is down.
- %PIXIASA-5-718064: Admin. interface interface_name is down.
- %PIXIASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB_state, master=IP_address, session=Enable/Disable).
- %PIXIASA-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.
- %PIXIASA-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.
- %PIXIASA-5-718068: Start VPN Load Balancing in context context_ID.
- %PIXIASA-5-718069: Stop VPN Load Balancing in context context_ID.
- %PIXIASA-5-718070: Reset VPN Load Balancing in context context_ID.
- %PIXIASA-5-718071: Terminate VPN Load Balancing in context context_ID.
- %PIXIASA-5-718072: Becoming master of Load Balancing in context context_ID.
- %PIXIASA-5-718073: Becoming slave of Load Balancing in context context_ID.
- %PIXIASA-5-718074: Fail to create access list for peer context_ID.
- %PIXIASA-5-718075: Peer IP_address access list not set.
- %PIXIASA-5-718076: Fail to create tunnel group for peer IP_address.
- %PIXIASA-5-718077: Fail to delete tunnel group for peer IP_address.
- %PIXIASA-5-718078: Fail to create crypto map for peer IP_address.
- %PIXIASA-5-718079: Fail to delete crypto map for peer IP_address.
- %PIXIASA-5-718080: Fail to create crypto policy for peer IP_address.
- %PIXIASA-5-718081: Fail to delete crypto policy for peer IP_address.
- %PIXIASA-5-718082: Fail to create crypto ipsec for peer IP_address.
- %PIXIASA-5-718083: Fail to delete crypto ipsec for peer IP_address.
- %PIXIASA-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address
- %PIXIASA-5-718085: Interface interface_name has no IP address defined.
- %PIXIASA-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.
- %PIXIASA-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.
- %ASA-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.
- %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %ASA-5-720017: (VPN-unit) Failed to update LB runtime data
- %ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %ASA-5-720020: (VPN-unit) Failed to send type timer message.

- %ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number. HA error code.
- %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %ASA-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %ASA-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.
- %ASA-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.
- %ASA-5-722010: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %ASA-5-722011: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %ASA-5-722012: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.
- %ASA-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.
- %ASA-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.
- %ASA-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.
- %ASA-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %ASA-5-722043: Group <group> User <user> IP <ip> DTLS disabled: unable to negotiate cipher.
- %ASA-5-722044: Group <group> User <user> IP <ip> Unable to request ver address for SSL tunnel.
- %ASA-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names
- %ASA-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'
- %ASA-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'
- %ASA-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'
- %ASA-5-737008: IPAA: 'tunnel-group' not found
- %ASA-5-737009: IPAA: requested address ip-address, request failed
- %ASA-5-737011: IPAA: requested address ip-address, not permitted, retrying
- %ASA-5-737018: IPAA: DHCP request attempt num failed

- %ASA-5-737021: IPAA: Address from local pool (ip-address) duplicates address from DHCP
- %ASA-5-737022: IPAA: Address from local pool (ip-address) duplicates address from AAA
- %ASA-5-737024: IPAA: Local pool assignment failed for suggested IP ip-address, retrying

Informational Messages, Severity 6

The following messages appear at severity 6, informational:

- %PIXIASA-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %PIXIASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %PIXIASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol
- %PIXIASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol
- %ASA-6-106102: access-list acl_ID {permitted|denied} protocol interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number {first hit|number-second interval}
- %PIXIASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port) -> interface_name/dest_address(dest_port) hit-cnt number ({first hit | number-second interval})
- %PIXIASA-6-108005: action_class: Received ESMTP req_resp from src_ifc:sipSPORT to dest_ifc:dipSPORT;further_info
- %ASA-6-108007: TLS started on ESMTP session between client client-side interface-name: clientIP address/client port and server server-side interface-name: server IP address/server port
- %PIXIASA-6-109001: Auth start for user user from inside_address/inside_port to outside_address/outside_port
- %PIXIASA-6-109002: Auth from inside_address/inside_port to outside_address/outside_port failed (server IP_address failed) on interface interface_name.
- %PIXIASA-6-109003: Auth from inside_address to outside_address/outside_port failed (all servers failed) on interface interface_name, >, so marking all servers ACTIVE again.
- %PIXIASA-6-109005: Authentication succeeded for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %PIXIASA-6-109006: Authentication failed for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %PIXIASA-6-109007: Authorization permitted for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %PIXIASA-6-109008: Authorization denied for user user from outside_address/outside_port to inside_address/ inside_port on interface interface_name.
- %PIXIASA-6-109024: Authorization denied from source_address/source_port to dest_address/dest_port (not authenticated) on interface interface_name using protocol
- %PIXIASA-6-109025: Authorization denied (acl=acl_ID) for user 'user' from source_address/source_port to dest_address/dest_port on interface interface_name using protocol

- %ASA-6-109037: RADIUS Server has sent an Access Accept message to the client ip-address, user = username
- %ASA-6-109038: RADIUS Server has sent an Access Reject message to the client ip-address, user = username
- %PIX|ASA-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %PIX|ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %PIX|ASA-6-113003: AAA group policy for user user is being set to policy_name.
- %PIX|ASA-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %PIX|ASA-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user
- %PIX|ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %PIX|ASA-6-113007: User user unlocked by administrator
- %PIX|ASA-6-113008: AAA transaction status ACCEPT: user = user
- %PIX|ASA-6-113009: AAA retrieved default group policy policy for user user
- %PIX|ASA-6-113010: AAA challenge received for user user from server server_IP_address
- %PIX|ASA-6-113011: AAA retrieved user specific group policy policy for user user
- %PIX|ASA-6-113012: AAA user authentication Successful: local database : user = user
- %PIX|ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %PIX|ASA-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %PIX|ASA-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user
- %PIX|ASA-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user
- %PIX|ASA-6-113017: AAA credentials rejected: reason = reason: local database: user = user\
- %ASA-6-114004: 4GE SSM I/O Initialization start.
- %ASA-6-114005: 4GE SSM I/O Initialization end.
- %ASA-6-120003: Process event group 'title'.
- %ASA-6-120007: Message group to 'destination' delivered.
- %PIX|ASA-6-199002: startup completed. Beginning operation.
- %PIX|ASA-6-199003: Reducing link MTU dec.
- %PIX|ASA-6-199005: Startup begin
- %ASA-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
- %PIX|ASA-6-210022: LU missed number updates
- %PIX|ASA-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port

- %PIXIASA-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %PIXIASA-6-302009: Rebuilt TCP connection number for foreign_address outside_address/outside_port global_address global_address/global_port local_address inside_address/inside_port
- %PIXIASA-6-302010: connections in use, connections most used
- %PIXIASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
- %PIXIASA-6-302013: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]
- %PIXIASA-6-302014: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]
- %PIXIASA-6-302015: Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) to interface_name:real_address/real_port (mapped_address/mapped_port) [(user)]
- %PIXIASA-6-302016: Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]
- %PIXIASA-6-302017: Built {inbound|outbound} GRE connection id from interface:real_address (translated_address) to interface:real_address/real_cid (translated_address/translated_cid)[(user)]
- %PIXIASA-6-302018: Teardown GRE connection id from interface:real_address (translated_address) to interface:real_address/real_cid (translated_address/translated_cid) duration hh:mm:ss bytes bytes [(user)]
- %PIXIASA-6-302020: Built ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]
- %PIXIASA-6-302021: Teardown ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]
- %PIXIASA-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- PIX-6-303002: FTP connection from src_ifc:src_ip/src_port to
- %PIXIASA-6-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc:sip/sport to dest_ifc:dip/dport
- %PIXIASA-6-304004: URL Server IP_address request failed URL url
- %PIXIASA-6-305007: addrpool_free(): Orphan IP IP_address on interface interface_number
- %PIXIASA-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address to interface_name:mapped_address
- %PIXIASA-6-305010: Teardown {dynamic|static} translation from interface_name:real_address to interface_name:mapped_address duration time
- %PIXIASA-6-305011: Built {dynamic|static} {TCPIUDP|ICMP} translation from interface_name:real_address/real_port to interface_name:mapped_address/mapped_port
- %PIXIASA-6-305012: Teardown {dynamic|static} {TCPIUDP|ICMP} translation from interface_name [(acl-name)]:real_address/{real_port|real_ICMP_ID} to interface_name:mapped_address/{mapped_port|mapped_ICMP_ID} duration time

- %PIX|ASA-6-308001: console enable password incorrect for number tries (from IP_address)
- %PIX|ASA-6-311001: LU loading standby start
- %PIX|ASA-6-311002: LU loading standby end
- %PIX|ASA-6-311003: LU recv thread up
- %PIX|ASA-6-311004: LU xmit thread up
- %PIX|ASA-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name
- %PIX|ASA-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.
- %PIX|ASA-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port : reason_string.
- %PIX|ASA-6-314003: Dropped RTSP traffic from src_intf:src_ip due to: reason.
- %PIX|ASA-6-314004: RTSP client src_intf:src_IP accessed RTSP URL RTSP_URL
- %PIX|ASA-6-314005: RTSP client src_intf:src_IP denied access to URL RTSP_URL.
- %PIX|ASA-6-314006: RTSP client src_intf:src_IP exceeds configured rate limit of rate for request_method messages.
- %PIX|ASA-6-315011: SSH session from IP_address on interface interface_name for user user disconnected by SSH server, reason: reason
- %PIX|ASA-6-321003: Resource var1 log level of var2 reached.
- %PIX|ASA-6-321004: Resource var1 rate log level of var2 reached
- %PIX|ASA-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
- %PIX|ASA-6-333001: EAP association initiated - context: EAP-context
- %PIX|ASA-6-333003: EAP association terminated - context: EAP-context
- %PIX|ASA-6-333009: EAP-SQ response MAC TLV is invalid - context: EAP-context
- %PIX|ASA-6-334001: EAPoUDP association initiated - <host-address>
- %PIX|ASA-6-334004: Authentication request for NAC Clientless host - host-address
- %PIX|ASA-6-334007: EAPoUDP association terminated - host-address
- %PIX|ASA-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %PIX|ASA-6-334009: Audit request for NAC Clientless host - Assigned_IP.
- %PIX|ASA-6-335001: NAC session initialized - host-address
- %PIX|ASA-6-335004: NAC is disabled for host - host-address
- %PIX|ASA-6-335006: NAC Applying ACL:ACL-name - host-address
- %PIX|ASA-6-335009: NAC 'Revalidate' request by administrative action - host-address
- %PIX|ASA-6-335010: NAC 'Revalidate All' request by administrative action - num sessions
- %PIX|ASA-6-335011: NAC 'Revalidate Group' request by administrative action for group-name group - num sessions
- %PIX|ASA-6-335012: NAC 'Initialize' request by administrative action - host-address
- %PIX|ASA-6-335013: NAC 'Initialize All' request by administrative action - num sessions

- %PIXIASA-6-335014: NAC 'Initialize Group' request by administrative action for group-name group - num sessions
- %ASA-6-336011: event event
- %ASA-6-339007: UC-IME-Offpath: Mapped address %A:%d on %s interface for remote UCM %A:%d on %s interface, request from local UCM %A:%d on %s interface
- %ASA-6-339008: UC-IME-Media: Media session with Call-ID %s and Session-ID %s terminated. RTP monitoring parameters: Failover state: %s, Refer msgs sent: %d, Codec payload format: %s, RTP ptime (ms): %d, Max RBLR pct(x100): %d, Max ITE count in 8 secs: %d, Max BLS (ms): %d, Max span PDV (usec): %d, Min span PDV (usec): %d, Mov avg span PDV (usec): %d, Total ITE count: %d, Total sec count: %d, Concealed sec count: %d, Severely concealed sec count: %d, Max call interval (ms): %d
- %ASA-6-339009: UC-IME: Ticket Password changed. Please update the same on UC-IME server.
- %ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %ASA-6-402129: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number= 0x7B) from 75.2.96.101 (user= user) to 85.2.96.10 with incorrect IPsec padding.
- %PIXIASA-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name.
- %ASA-6-410004: action_class: action DNS query_response from src_ifc:sip/sport to dest_ifc:dip/dport; further_info
- %ASA-6-414004: TCP Syslog Server intf: IP_Address/port - Connection restored
- %PIXIASA-6-415001: HTTP - matched matched_string in policy-map map_name, header field count exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-6-415002: HTTP - matched matched_string in policy-map map_name, header field length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-6-415003: HTTP - matched matched_string in policy-map map_name, body length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %PIXIASA-6-415017: HTTP - matched_string in policy-map map_name, arguments matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %ASA-6-420004 : Virtual Sensor sensor_name was added on the AIP SSM\n
- %ASA-6-420005 : Virtual Sensor sensor_name was deleted from the AIP SSM\n
- %ASA-6-421002: TCPIUDP flow from interface_name:IP_address/port to interface_nam:IP_address/port bypassed application checking because the protocol is not supported.
- %ASA-6-421005: interface_name:IP_address is counted as a user of application
- %ASA-6-421006: There are number users of application accounted during the past 24 hours.
- %ASA-6-425001 Redundant interface redundant_interface_name created.
- %ASA-6-425002 Redundant interface redundant_interface_name removed.
- %ASA-6-425003 Interface interface_name added into redundant interface redundant_interface_name.
- %ASA-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.

- %ASA-6-425005 Interface interface_name become active in redundant interface redundant_interface_name
- %ASA-6-425006 Redundant interface redundant_interface_name switch active member to interface_name failed.
- %ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.
- %PIX|ASA-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address, src_addr=source_address, prot=protocol
- %PIX|ASA-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.%PIX|ASA-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %PIX|ASA-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.
- %PIX|ASA-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.
- %PIX|ASA-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.
- %PIX|ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl_id=number, sess_id=number, seq=number.
- %PIX|ASA-6-603102: PPP virtual interface interface_name - user: user aaa authentication started.
- %PIX|ASA-6-603103: PPP virtual interface interface_name - user: user aaa authentication status
- %PIX|ASA-6-603104: PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, client_dynamic_ip is IP_address, username is user, MPPE_key_strength is string
- %PIX|ASA-6-603105: PPTP Tunnel deleted, tunnel_id = number, remote_peer_ip= remote_address
- %PIX|ASA-6-603106: L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, client_dynamic_ip is IP_address, username is user
- %PIX|ASA-6-603107: L2TP Tunnel deleted, tunnel_id = number, remote_peer_ip = remote_address
- %PIX|ASA-6-603108: Built PPTP Tunnel at interface_name, tunnel-id = number, remote-peer = IP_address, virtual-interface = number, client-dynamic-ip = IP_address, username = user, MPPE-key-strength = number
- %PIX|ASA-6-603109: Teardown PPPOE Tunnel at interface_name, tunnel-id = number, remote-peer = IP_address
- %PIX|ASA-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %PIX|ASA-6-604102: DHCP client interface interface_name: address released
- %PIX|ASA-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %PIX|ASA-6-604104: DHCP daemon interface interface_name: address released

- %PIXIASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"
- %PIXIASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
- %PIXIASA-6-606001: ASDM session number number from IP_address started
- %PIXIASA-6-606002: ASDM session number number from IP_address ended
- %PIXIASA-6-606003: ASDM logging session number id from IP_address started id session ID assigned
- %PIXIASA-6-606004: ASDM logging session number id from IP_address ended
- %PIXIASA-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
- %PIXIASA-6-607003: action_class: Received SIP req_resp req_resp_info from src_ifc:sip/sport to dest_ifc:dip/dport; further_info
- %PIXIASA-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address/port from string message
- %PIXIASA-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %PIXIASA-6-611101: User authentication succeeded: Uname: user
- %PIXIASA-6-611102: User authentication failed: Uname: user
- %PIXIASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address
- %PIXIASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling
- %PIXIASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %PIXIASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %PIXIASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
- %PIXIASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed
- %PIXIASA-6-611307: VPNClient: Head end: IP_address
- %PIXIASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string
- %PIXIASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address
- %PIXIASA-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address
- %PIXIASA-6-611311: VNPClient: XAUTH Failed: Peer: IP_address
- %PIXIASA-6-611312: VPNClient: Backup Server List: reason
- %PIXIASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address
- %PIXIASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address
- %PIXIASA-6-611316: VPNClient: Secure Unit Authentication Enabled
- %PIXIASA-6-611317: VPNClient: Secure Unit Authentication Disabled

- %PIX|ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time
- %PIX|ASA-6-611319: VPNClient: User Authentication Disabled
- %PIX|ASA-6-611320: VPNClient: Device Pass Thru Enabled
- %PIX|ASA-6-611321: VPNClient: Device Pass Thru Disabled
- %PIX|ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled
- %PIX|ASA-6-611323: VPNClient: Duplicate split nw entry
- %PIX|ASA-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
- %PIX|ASA-6-613002: interface interface_name has zero bandwidth
- %PIX|ASA-6-613003: IP_address netmask changed from area string to area string
- %PIX|ASA-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
- %PIX|ASA-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address
- %PIX|ASA-6-615001: vlan number not available for firewall interface
- %PIX|ASA-6-615002: vlan number available for firewall interface
- %PIX|ASA-6-616001:Pre-allocate MGCP data_channel connection for inside_interface:inside_address to outside_interface:outside_address/port from message_type message
- %PIX|ASA-6-617001: GTPv version msg_type from source_interface:source_address/source_port not accepted by source_interface:dest_address/dest_port
- %PIX|ASA-6-617002: Removing v1 PDP Context with TID tid from GGSN IP_address and SGSN IP_address, Reason: reason or Removing v1 primary/secondary PDP Context with TID tid from GGSN IP_address and SGSN IP_address, Reason: reason
- %PIX|ASA-6-617003: GTP Tunnel created from source_interface:source_address/source_port to source_interface:dest_address/dest_port
- %PIX|ASA-6-617004: GTP connection created for response from source_interface:source_address/0 to source_interface:dest_address/dest_port
- %PIX|ASA-6-617100: Teardown num_conns connection(s) for user user_ip
- %PIX|ASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for interface_name:outside_address[/outside_port] to interface_name:inside_address[/inside_port] from CTIQBE_message_name message
- %PIX|ASA-6-621001: Interface interface_name does not support multicast, not enabled
- %PIX|ASA-6-621002: Interface interface_name does not support multicast, not enabled
- %PIX|ASA-6-621003: The event queue size has exceeded number
- %PIX|ASA-6-621006: Mrib disconnected, (IP_address,IP_address) event cancelled
- %PIX|ASA-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %PIX-6-621008 AutoRP: discard string on interface interface-name from address due to incorrect version.
- %PIX-6-621009 AutoRP: discard string on interface interface-name from address due to incorrect type number

- %PIX-6-621010 AutoRP: discard string on interface interface-name from address due to zero RP count
- %PIXIASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %PIXIASA-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries
- %PIXIASA-6-622102: Completed regex table compilation for match_command; table size = num bytes
- %ASA-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
- %PIXIASA-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
- %PIXIASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %PIXIASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %PIXIASA-6-713172: Automatic NAT Detection Status: Remote end is/is not behind a NAT device This end is/is not behind a NAT device
- %PIXIASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %PIXIASA-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %PIXIASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %PIXIASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %PIXIASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %PIXIASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %PIXIASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.
- %PIXIASA-6-713228: Assigned private IP address assigned_private_IP
- %PIXIASA-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %ASA-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
- %PIXIASA-6-713905: descriptive_event_string.
- %ASA-6-716001: Group group User user WebVPN session started.
- %ASA-6-716002: Group group User user WebVPN session terminated: reason.
- %ASA-6-716003: Group group User user WebVPN access GRANTED: url
- %ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %ASA-6-716006: Group name User user WebVPN session terminated. Idle timeout.

- %ASA-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %ASA-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: WebVPN
- %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %ASA-6-716041: access-list acl_ID action url url hit_cnt count
- %ASA-6-716042: access-list acl_ID action tcp source_interface/source_address (source_port) -> dest_interface/dest_address(dest_port) hit-cnt count
- %ASA-6-716043 Group group-name, User user-name, IP IP_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings.
- %ASA-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.
- %ASA-6-716050: Error adding to ACL: ace_command_line
- %ASA-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
- %ASA-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded
- %ASA-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.
- %ASA-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2
- %ASA-6-716060:Terminated AnyConnect session in waiting-to-resume state to accept a new connection. Group group User user IP ip License pre-empted.
- %PIX|ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
- %PIX|ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
- %PIX|ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
- %PIX|ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
- %PIX|ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
- %PIX|ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %PIX|ASA-6-717022: Certificate was successfully validated. certificate_identifiers
- %PIX|ASA-6-717028: Certificate chain was successfully validated additional info.
- %PIX|ASA-6-717033: OCSP response status - Successful.
- %ASA-6-717043: Local CA Server certificate enrollment related info for user: user. Info: info.
- %ASA-6-717047: Revoked certificate issued to user: username, with serial number serial number.
- %ASA-6-717048: Unrevoked certificate issued to user: username, with serial number serial number.
- %PIX|ASA-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number
- %PIX|ASA-6-718004: Got unknown internal message message_number
- %PIX|ASA-6-718013: Peer IP_address is not answering HELLO
- %PIX|ASA-6-718027: Received unexpected KEEPALIVE request from IP_address
- %PIX|ASA-6-718030: Received planned OOS from IP_address
- %PIX|ASA-6-718037: Master processed number_of_timeouts timeouts

- %PIXIASA-6-718038: Slave processed number_of_timeouts timeouts
- %PIXIASA-6-718039: Process dead peer IP_address
- %PIXIASA-6-718040: Timed-out exchange ID exchange_ID not found
- %PIXIASA-6-718051: Deleted secure tunnel to peer IP_address
- %ASA-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
- %ASA-6-719003: Email Proxy session pointer resources have been freed for source_address.
- %ASA-6-719004: Email Proxy session pointer has been successfully established for source_address.
- %ASA-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
- %ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.
- %ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %ASA-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found
- %ASA-6-719019: WebVPN user: vpnuser authorization failed.
- %ASA-6-719020: WebVPN user vpnuser authorization completed successfully.
- %ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %ASA-6-719022: WebVPN user vpnuser has been authenticated.
- %ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
- %ASA-6-719025: Email Proxy DNS name resolution failed for hostname.
- %ASA-6-719026: Email Proxy DNS name hostname resolved to IP_address.
- %ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %ASA-6-720004: (VPN-unit) VPN failover main thread started.
- %ASA-6-720005: (VPN-unit) VPN failover timer thread started.
- %ASA-6-720006: (VPN-unit) VPN failover sync thread started.
- %ASA-6-720010: (VPN-unit) VPN failover client is being disabled
- %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
- %ASA-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
- %ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number,my cookie=mine, his cookie=his).
- %ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.

- %ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %ASA-6-720027: (VPN-unit) HA status callback: My state state.
- %ASA-6-720028: (VPN-unit) HA status callback: Peer state state.
- %ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence_#, grp=group, event=event, op=operand, my=my_state, peer=peer_state.
- %ASA-6-720037: (VPN-unit) HA progression callback:
id=id,seq=sequence_number,grp=group,event=event,op=operand, my=my_state,peer=peer_state.
- %ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %ASA-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
- %ASA-6-721002: (device) HA status change: event event, my state my_state, peer state peer.
- %ASA-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.
- %ASA-6-721004: (device) Create access list list_name on standby unit.
- %ASA-6-721005: (device) Fail to create access list list_name on standby unit.
- %ASA-6-721006: (device) Update access list list_name on standby unit.
- %ASA-6-721008: (device) Delete access list list_name on standby unit.
- %ASA-6-721009: (device) Fail to delete access list list_name on standby unit.
- %ASA-6-721010: (device) Add access list rule list_name, line line_no on standby unit.
- %ASA-6-721012: (device) Enable APCF XML file file_name on the standby unit.
- %ASA-6-721014: (device) Disable APCF XML file file_name on the standby unit.
- %ASA-6-721016: (device) WebVPN session for client user user_name, IP ip_address has been created.
- %ASA-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.

- %ASA-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-722014: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-722022: Group group-name User user-name IP addr (TCP | UDP) connection established (with | without) compression
- %ASA-6-722023: Group group User user-name IP IP_address SVC connection terminated {with|without} compression
- %ASA-6-722024: SVC Global Compression Enabled
- %ASA-6-722025: SVC Global Compression Disabled
- %ASA-6-722026: Group group User user-name IP IP_address SVC compression history reset
- %ASA-6-722027: Group group User user-name IP IP_address SVC decompression history reset
- %ASA-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
- %ASA-6-722053: Group g User u IP ip Unknown client user-agent connection.
- %ASA-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.
- %ASA-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.
- %ASA-6-725001 Starting SSL handshake with remote_device interface_name:IP_address/port for SSL_version session.
- %ASA-6-725002 Device completed SSL handshake with remote_device interface_name:IP_address/port
- %ASA-6-725003 SSL client interface_name:IP_address/port requesting to resume previous session.
- %ASA-6-725004 Device requesting certificate from SSL client interface_name:IP_address/port for authentication.
- %ASA-6-725005 SSL server interface_name:IP_address/port requesting our device certificate for authentication.
- %ASA-6-725006 Device failed SSL handshake with remote_device interface_name:IP_address/port
- %ASA-6-725007 SSL session with remote_device interface_name:IP_address/port terminated.
- %PIX|ASA-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
- %ASA-6-730004 Group groupname User username IP ipaddr VLAN ID vlanid from AAA ignored.
- %ASA-6-730005 Group groupname User username IP ipaddr VLAN ID vlanid from AAA is invalid.
- %ASA-6-731001 NAC policy added: name: policyname Type: policytype.
- %ASA-6-731002 NAC policy deleted: name: policyname Type: policytype.
- %ASA-6-731003 nac-policy unused: name: policyname Type: policytype.
- %ASA-6-732001 Group groupname, User username, IP ipaddr, Fail to parse NAC-SETTINGS nac-settings-id, terminating connection.

- %ASA-6-732002 Group groupname, User username, IP ipaddr, NAC-SETTINGS settingsid from AAA ignored, existing NAC-SETTINGS settingsid_inuse used instead.
- %ASA-6-732003 Group groupname, User username, IP ipaddr, NAC-SETTINGS nac-settings-id from AAA is invalid, terminating connection.
- %ASA-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %ASA-6-722051: Group <group-policy> User <username> IP <public-ip> Address <assigned-ip> assigned to session
- %ASA-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737010: IPAA: requested address ip-address, request succeeded
- %ASA-6-737014: IPAA: Freeing AAA address ip-address
- %ASA-6-737015: IPAA: Freeing DHCP address ip-address
- %ASA-6-737016: IPAA: Freeing local pool address ip-address
- %ASA-6-737017: IPAA: DHCP request attempt num succeeded
- %ASA-6-737026: IPAA: Client assigned ip-address from local pool
- %ASA-6-737029: IPAA: Adding ip-address to standby: succeeded
- %ASA-6-737031: IPAA: Removing %m from standby: succeeded
- %ASA-6-800003: DSI: Incoming request on URI dsi_uri from ip_addr/port
- %ASA-6-800004: DSI: Incoming request on invalid URI dsi_uri from ip_addr/port

Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

- %PIX|ASA-7-109014: uauth_lookup_net fail for uauth_in()
- %PIX|ASA-7-109021: Uauth null proxy error
- %PIX|ASA-7-111009: User user executed cmd:string
- %PIX-7-199009: Reloaded at when by whom. Reload reason: reason
- %PIX|ASA-7-304005: URL Server IP_address request pending URL url
- %PIX|ASA-7-304009: Ran out of buffer blocks specified by url-block command
- %PIX|ASA-7-333004: EAP-SQ response invalid - context:EAP-context
- %PIX|ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %PIX|ASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %PIX|ASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %PIX|ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %PIX|ASA-7-335007: NAC Default ACL not configured - host-address
- %ASA-7-421004: Failed to inject {TCPIUDP} packet from IP_address/port to IP_address/port
- %ASA-7-603110: Multiple L2TP sessions added to the tunnel. tunnel_id: tunnel id, number_of_sessions: session_count

- %PIXIASA-7-609001: Built local-host interface_name:IP_address
- %PIXIASA-7-609002: Teardown local-host interface_name:IP_address duration time
- %PIXIASA-7-701001: alloc_user() out of Tcp_user objects
- %PIXIASA-7-701002: alloc_user() out of Tcp_proxy objects
- %PIXIASA-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %PIXIASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
- %PIXIASA-7-709001: FO replication failed: cmd=command returned=code
- %PIXIASA-7-709002: FO unreplicable: cmd=command
- %PIXIASA-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
- %PIXIASA-7-710002: {TCPIUDP} access permitted from source_address/source_port to interface_name:dest_address/service
- %PIXIASA-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)
- %PIXIASA-7-710005: {TCPIUDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %PIXIASA-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %PIXIASA-7-710007:NAT-T keepalive received from 86.1.161.1/1028 to outside:86.1.129.1/4500
- %PIXIASA-7-711001: debug_trace_msg
- %PIX/ASA-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.
- %PIXIASA-7-713024: Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIXIASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIXIASA-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIXIASA-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIXIASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIXIASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIXIASA-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIXIASA-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIXIASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIXIASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port

- %PIX|ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713039: Send failure: Bytes (number), Peer: IP_address
- %PIX|ASA-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %PIX|ASA-7-713052: User (user) authenticated.
- %PIX|ASA-7-713066: IKE Remote Peer configured for SA: SA_name
- %PIX|ASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %PIX|ASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %PIX|ASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %PIX|ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %PIX|ASA-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count
- %PIX|ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match
- %PIX|ASA-7-713117: Received Invalid SPI notify (SPI SPI_Value)!
- %PIX|ASA-7-713121: Keep-alive type for this connection: keepalive_type
- %PIX|ASA-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability_value, Version Number: version_number, Version String: version_text
- %PIX|ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %PIX|ASA-7-713164: The Firewall Server has requested a list of active user sessions
- %PIX|ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count
- %PIX|ASA-7-713170: IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id
- %PIX|ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %PIX|ASA-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
- %PIX|ASA-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)
- %PIX|ASA-7-713204: Adding static route for client address: IP_address
- %PIX|ASA-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...
- %PIX|ASA-7-713222: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, ACL does not match proxy IDs src:source_address dst:dest_address
- %PIX|ASA-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured
- %PIX|ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %PIX|ASA-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match

- %PIXIASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %PIXIASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %PIXIASA-7-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %PIXIASA-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen
- %PIXIASA-7-713900: Descriptive_event_string.
- %PIXIASA-7-713901: Descriptive_event_string.
- %PIXIASA-7-713906: descriptive_event_string.
- %PIXIASA-7-714001: description_of_event_or_packet
- %PIXIASA-7-714002: IKE Initiator starting QM: msg id = message_number
- %PIXIASA-7-714003: IKE Responder starting QM: msg id = message_number
- %PIXIASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %PIXIASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %PIXIASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %PIXIASA-7-714007: IKE Initiator sending Initial Contact
- %PIXIASA-7-714011: Description of received ID values
- %PIXIASA-7-715001: Descriptive statement
- %PIXIASA-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %PIXIASA-7-715005: subroutine name() Bad message code: Code (message_code)
- %PIXIASA-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %PIXIASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %PIXIASA-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %PIXIASA-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %PIXIASA-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %PIXIASA-7-715019: IKEGetUserAttributes: Attribute name = name
- %PIXIASA-7-715020: construct_cfg_set: Attribute name = name
- %PIXIASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %PIXIASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %PIXIASA-7-715027: IPsec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPsec SA entry # crypto_map_index
- %PIXIASA-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index
- %PIXIASA-7-715033: Processing CONNECTED notify (MsgId message_number)
- %PIXIASA-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %PIXIASA-7-715035: Starting IOS keepalive monitor: seconds sec.
- %PIXIASA-7-715036: Sending keep-alive of type notify_type (seq number number)

- %PIX|ASA-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %PIX|ASA-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %PIX|ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %PIX|ASA-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %PIX|ASA-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %PIX|ASA-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %PIX|ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %PIX|ASA-7-715045: ERROR: malformed Keepalive payload
- %PIX|ASA-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload
- %PIX|ASA-7-715047: processing payload_description payload
- %PIX|ASA-7-715048: Send VID_type VID
- %PIX|ASA-7-715049: Received VID_type VID
- %PIX|ASA-7-715050: Claims to be IOS but failed authentication
- %PIX|ASA-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply
- %PIX|ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %PIX|ASA-7-715053: MODE_CFG: Received request for attribute_info!
- %PIX|ASA-7-715054: MODE_CFG: Received attribute_name reply: value
- %PIX|ASA-7-715055: Send attribute_name
- %PIX|ASA-7-715056: Client is configured for TCP_transparency
- %PIX|ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %PIX|ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %PIX|ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %PIX|ASA-7-715060: Dropped received IKE fragment. Reason: reason
- %PIX|ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %PIX|ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %PIX|ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %PIX|ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %PIX|ASA-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
- %PIX|ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %PIX|ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

- %PIXIASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %PIXIASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %PIXIASA-7-715069: Invalid ESP SPI size of SPI_size
- %PIXIASA-7-715070: Invalid IPComp SPI size of SPI_size
- %PIXIASA-7-715071: AH proposal not supported
- %PIXIASA-7-715072: Received proposal with unknown protocol ID protocol_ID
- %PIXIASA-7-715074: Could not retrieve authentication attributes for peer IP_address
- %PIXIASA-7-715075: Group = group_name, Username = client, IP = IP_address Received keep-alive of type message_type (seq number number)
- %PIXIASA-7-715076: Computing hash for ISAKMP
- %PIXIASA-7-715077: Pitcher: msg string, spi spi
- %PIX-7-715078: META-DATA Received type LAM attribute.
- %PIX-7-715079: META-DATA INTERNAL_ADDRESS: Received request for type.
- %ASA-vpn-7-715080: Starting P2 rekey timer: 28800 seconds.
- %ASA-7-716008: WebVPN ACL: action
- %ASA-7-716010: Group group User user Browse network.
- %ASA-7-716011: Group group User user Browse domain domain.
- %ASA-7-716012: Group group User user Browse directory directory.
- %ASA-7-716013: Group group User user Close file filename.
- %ASA-7-716014: Group group User user View file filename.
- %ASA-7-716015: Group group User user Remove file filename.
- %ASA-7-716016: Group group User user Rename file old_filename to new_filename.
- %ASA-7-716017: Group group User user Modify file filename.
- %ASA-7-716018: Group group User user Create file filename.
- %ASA-7-716019: Group group User user Create directory directory.
- %ASA-7-716020: Group group User user Remove directory directory.
- %ASA-7-716021: File access DENIED, filename.
- %ASA-7-716024: Group name User user Unable to browse the network.Error: description
- %ASA-7-716025: Group name User user Unable to browse domain domain. Error: description
- %ASA-7-716026: Group name User user Unable to browse directory directory. Error: description
- %ASA-7-716027: Group name User user Unable to view file filename. Error: description
- %ASA-7-716028: Group name User user Unable to remove file filename. Error: description
- %ASA-7-716029: Group name User user Unable to rename file filename. Error: description
- %ASA-7-716030: Group name User user Unable to modify file filename. Error: description
- %ASA-7-716031: Group name User user Unable to create file filename. Error: description
- %ASA-7-716032: Group name User user Unable to create folder folder. Error: description
- %ASA-7-716033: Group name User user Unable to remove folder folder. Error: description
- %ASA-7-716034: Group name User user Unable to write to file filename.

- %ASA-7-716035: Group name User user Unable to read file filename.
- %ASA-7-716036: Group name User user File Access: User user logged into the server server.
- %ASA-7-716037: Group name User user File Access: User user failed to login into the server server.
- %PIX|ASA-7-717024: Checking CRL from trustpoint: trustpoint name for purpose
- %PIX|ASA-7-717025: Validating certificate chain containing number of certs certificate(s).
- %PIX|ASA-7-717029: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %PIX|ASA-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.
- %PIX|ASA-7-717034: No-check extension found in certificate. OCSP check bypassed.
- %PIX|ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.
- %PIX|ASA-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %ASA-7-717041: Local CA Server event: event info.
- %ASA-7-717045: Local CA Server CRL info: info
- %PIX|ASA-7-718001: Internal interprocess communication queue send failure: code error_code
- %PIX|ASA-7-718017: Got timeout for unknown peer IP_address msg type message_type
- %PIX|ASA-7-718018: Send KEEPALIVE request failure to IP_address
- %PIX|ASA-7-718019: Sent KEEPALIVE request to IP_address
- %PIX|ASA-7-718020: Send KEEPALIVE response failure to IP_address
- %PIX|ASA-7-718021: Sent KEEPALIVE response to IP_address
- %PIX|ASA-7-718022: Received KEEPALIVE request from IP_address
- %PIX|ASA-7-718023: Received KEEPALIVE response from IP_address
- %PIX|ASA-7-718025: Sent CFG UPDATE to IP_address
- %PIX|ASA-7-718026: Received CFG UPDATE from IP_address
- %PIX|ASA-7-718029: Sent OOS indicator to IP_address
- %PIX|ASA-7-718034: Sent TOPOLOGY indicator to IP_address
- %PIX|ASA-7-718035: Received TOPOLOGY indicator from IP_address
- %PIX|ASA-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address
- %PIX|ASA-7-718041: Timeout [msgType=type] processed with no callback
- %PIX|ASA-7-718046: Create group policy policy_name
- %PIX|ASA-7-718047: Fail to create group policy policy_name
- %PIX|ASA-7-718049: Created secure tunnel to peer IP_address
- %PIX|ASA-7-718056: Deleted Master peer, IP IP_address
- %PIX|ASA-7-718058: State machine return code: action_routine, return_code
- %PIX|ASA-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine
- %PIX|ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.

- %ASA-7-719005: FSM NAME has been created using protocol for session pointer from source_address.
- %ASA-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.
- %ASA-7-719007: Email Proxy session pointer cannot be found for source_address.
- %ASA-7-719009: Email Proxy service is starting.
- %ASA-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server
- %ASA-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = *****, vpnpass= *****
- %ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.
- %ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %ASA-7-720041: (VPN-unit) Sending type message id to standby unit
- %ASA-7-720042: (VPN-unit) Receiving type message id from active unit
- %ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %ASA-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %ASA-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
- %ASA-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
- %ASA-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.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-7-723004: WebVPN Citrix encountered bad flow control flow.
- %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %ASA-7-723006: WebVPN Citrix SOCKS errors.
- %ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %ASA-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.
- %ASA-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %ASA-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.
- %ASA-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.
- %ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.

- %ASA-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %ASA-7-725008 SSL client interface_name:IP_address/port proposes the following number cipher(s).
- %ASA-7-725009 Device proposes the following number cipher(s) to SSL server interface_name:IP_address/port.
- %ASA-7-725010 Device supports the following number cipher(s).
- %ASA-7-725011 Cipher[order]: cipher_name
- %ASA-7-725012 Device chooses cipher: cipher_name for SSL session with client interface_name:IP_address/port
- %ASA-7-725013 SSL Server interface_name:IP_address/port chooses cipher: cipher_name
- %ASA-7-725014 SSL lib error. Function: function Reason: reason
- %ASA-7-730001 Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid
- %ASA-7-730002 Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed
- %ASA-7-730010 Group groupname, User username, IP ipaddr, VLAN Mapping is enabled on VLAN <vlanid>.
- %ASA-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value
- %ASA-7-737001: IPAA: Received message 'message-type'

Variables Used in Syslog Messages

Syslog messages often include variables. [Table A-1](#) lists most variables that are used in this guide to describe syslog messages. Some variables that appear in only one syslog message are not listed.

Table A-1 Variable Fields in Syslog Messages

Variable	Description
<i>acl_ID</i>	An ACL name.
<i>bytes</i>	The number of bytes.
<i>code</i>	A decimal number returned by the syslog message to indicate the cause or source of the error, depending on the syslog message.
<i>command</i>	A command name.
<i>command_modifier</i>	The <i>command_modifier</i> is one of the following strings: <ul style="list-style-type: none"> • cmd (this string means the command has no modifier) • clear • no • show
<i>connections</i>	The number of connections.

Table A-1 Variable Fields in Syslog Messages (continued)

Variable	Description
<i>connection_type</i>	The connection type: <ul style="list-style-type: none"> • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • RTP • RTCP
<i>dec</i>	Decimal number.
<i>dest_address</i>	The destination address of a packet.
<i>dest_port</i>	The destination port number.
<i>device</i>	The memory storage device. For example, the floppy disk, internal Flash memory, TFTP, the failover standby unit, or the console terminal.
<i>econns</i>	Number of embryonic connections.
<i>elimit</i>	Number of embryonic connections specified in the static or nat command.
<i>filename</i>	A filename of the type Cisco ASA image, ASDM file, or configuration.
<i>ftp-server</i>	External FTP server name or IP address.
<i>gateway_address</i>	The network gateway IP address.
<i>global_address</i>	Global IP address, an address on a lower security level interface.
<i>global_port</i>	The global port number.
<i>hex</i>	Hexadecimal number.
<i>inside_address</i>	Inside (or local) IP address, an address on a higher security level interface.
<i>inside_port</i>	The inside port number.
<i>interface_name</i>	The name of the interface.
<i>IP_address</i>	IP address in the form <i>n.n.n.n</i> , where <i>n</i> is an integer from 1 to 255.
<i>MAC_address</i>	The MAC address.
<i>mapped_address</i>	The translated IP address.
<i>mapped_port</i>	The translated port number.
<i>message_class</i>	Category of syslog messages associated with a functional area of the security appliance.
<i>message_list</i>	Name of a file you create containing a list of syslog message ID numbers, classes, or severity levels.
<i>message_number</i>	The syslog message ID.
<i>nconns</i>	Number of connections permitted for the static or xlate table.
<i>netmask</i>	The subnet mask.
<i>number</i>	A number. The exact form depends on the syslog message.

Table A-1 Variable Fields in Syslog Messages (continued)

Variable	Description
<i>octal</i>	Octal number.
<i>outside_address</i>	Outside (or foreign) IP address, an address of a syslog server typically on a lower security level interface in a network beyond the outside router.
<i>outside_port</i>	The outside port number.
<i>port</i>	The TCP or UDP port number.
<i>privilege_level</i>	The user privilege level.
<i>protocol</i>	The protocol of the packet, for example, ICMP, TCP, or UDP.
<i>real_address</i>	The real IP address, before Network Address Translation (NAT).
<i>real_port</i>	The real port number, before NAT.
<i>reason</i>	A text string describing the reason for the syslog message.
<i>service</i>	The service specified by the packet, for example, SNMP or Telnet.
<i>severity_level</i>	The severity level of a syslog message.
<i>source_address</i>	The source address of a packet.
<i>source_port</i>	The source port number.
<i>string</i>	Text string (for example, a username).
<i>tcp_flags</i>	Flags in the TCP header such as: <ul style="list-style-type: none"> • ACK • FIN • PSH • RST • SYN • URG
<i>time</i>	Duration, in the format <i>hh:mm:ss</i> .
<i>url</i>	A URL.
<i>user</i>	A username.

