Release Notes for the Cisco ASA Series, 9.10(x)

Release Notes for the Cisco ASA Series, 9.10(x)

This document contains release information for Cisco ASA software Version 9.10(x).

Important Notes

- Upgrade ROMMON for ASA 5506-X, 5508-X, and 5516-X to Version 1.1.15—There is a new ROMMON version for these ASA models (May 15, 2019); we highly recommend that you upgrade to the latest version. To upgrade, see the instructions in the ASA configuration guide.

  Caution The ROMMON upgrade for 1.1.15 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

- No support in 9.10(1) and later for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X—The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1) or later, the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.
- These ciphers are currently unsupported for DTLS 1.2 in FIPS mode for the Firepower 2100 (KP) platforms:
  - DHE-RSA-AES256-SHA
  - AES256-SHA
  - DHE-RSA-AES128-SHA
  - AES128-SHA
- If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.10(1), the defaulted SAML behavior is the embedded browser, which is not supported on AnyConnect 4.4 and 4.5. Therefore, you must enable the **saml external-browser** command in tunnel group configuration in order for AnyConnect 4.4 and 4.5 clients to authenticate with SAML using the external (native) browser.

Note The **saml external-browser** command is for migration purposes for those upgrading to AnyConnect 4.6 or later. Because of security limitations, use this solution only as part of a temporary migration while upgrading AnyConnect software. The command itself will be depreciated in the future.

- New ROMMON Version 1.1.12 for the ASA 5506-X, 5508-X, and 5516-X—We recommend that you upgrade your ROMMON for several crucial fixes. See https://www.cisco.com/go/asa-firepower-sw, choose your *model* > ASA Rommon Software > 1.1.12. Refer to the release notes on the software download page for more information. To upgrade the ROMMON, see Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X). Note that the ASA running Firepower Threat Defense does not yet support upgrading to this ROMMON version; you can, however, successfully upgrade it in ASA and then reimage to Firepower Threat Defense.
- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

  For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

System Requirements

This section lists the system requirements to run this release.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see Cisco ASA Compatibility.

VPN Compatibility

For VPN compatibility, see Supported VPN Platforms, Cisco ASA 5500 Series.

New Features

This section lists new features for each release.

Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.10(1)

Released: October 25, 2018

Feature	Description
Platform Features	
ASAv VHD custom images for Azure	You can now create your own custom ASAv images on Azure using a compressed VHD image available from Cisco. To deploy using a VHD image, you upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.
ASAv for Azure	The ASAv is available in the Azure China Marketplace.
ASAv support for DPDK	DPDK (Dataplane Development Kit) is integrated into the dataplane of the ASAv using poll-mode drivers.
ISA 3000 support for FirePOWER module Version 6.3	The previous supported version was FirePOWER 5.4.
Firewall Features	
Cisco Umbrella support	You can configure the device to redirect DNS requests to Cisco Umbrella, so that your Enterprise Security policy defined in Cisco Umbrella can be applied to user connections. You can allow or block connections based on FQDN, or for suspicious FQDNs, you can redirect the user to the Cisco Umbrella intelligent proxy, which can perform URL filtering. The Umbrella configuration is part of the DNS inspection policy. New/Modified commands: **umbrella**, **umbrella-global**, **token**, **public-key**, **timeout edns**, **dnscrypt**, **show service-policy inspect dns detail**
GTP inspection enhancements for MSISDN and Selection Mode filtering, anti-replay, and user spoofing protection	You can now configure GTP inspection to drop Create PDP Context messages based on Mobile Station International Subscriber Directory Number (MSISDN) or Selection Mode. You can also implement anti-replay and user spoofing protection. New/Modified commands: **anti-replay**, **gtp-u-header-check**, **match msisdn**, **match selection-mode**
Default idle timeout for TCP state bypass	The default idle timeout for TCP state bypass connections is now 2 minutes instead of 1 hour.
Support for removing the logout button from the cut-through proxy login page	If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address. New/Modified commands: **aaa authentication listener no-logout-button** *Also in 9.8(3).*

Feature	Description
Trustsec SXP connection configurable delete hold down timer	The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds. New/Modified commands: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** *Also in 9.8(3).*
Support for offloading NAT'ed flows in transparent mode.	If you are using flow offload (the **flow-offload enable** and **set connection advanced-options flow-offload** commands), offloaded flows can now include flows that require NAT in transparent mode.
Support for transparent mode deployment for a Firepower 4100/9300 ASA logical device	You can now specify transparent or routed mode when you deploy the ASA on a Firepower 4100/9300. New/Modified FXOS commands: **enter bootstrap-key FIREWALL_MODE**, **set value routed**, **set value transparent**
VPN Features	
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6 (or later). This option will be deprecated in the near future. New/Modified commands: **saml external-browser** *Also in 9.8(3).*
DTLS 1.2 support for AnyConnect VPN remote access connections.	DTLS 1.2, as defined in RFC- 6347, is now supported for AnyConnect remote access in addition to the currently supported DTLS 1.0 (1.1 version number is not used for DTLS.) This applies to all ASA models except the 5506-X, 5508-X, and 5516-X; and applies when the ASA is acting as a server only, not a client. DTLS 1.2 supports additional ciphers, as well as all current TLS/DTLS cyphers, and a larger cookie size. New/Modified commands: **show run ssl**, **show vpn-sessiondb detail anyconnectssl cipher**, **ssl server-version**
High Availability and Scalability Features	
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/Modified FXOS commands: **set cluster-control-link network**

Feature	Description
Parallel joining of cluster units per Firepower 9300 chassis	For the Firepower 9300, this feature ensures that the security modules in a chassis join the cluster simultaneously, so that traffic is evenly distributed between the modules. If a module joins very much in advance of other modules, it can receive more traffic than desired, because the other modules cannot yet share the load. New/Modified commands: **unit parallel-join**
Cluster interface debounce time now applies to interfaces changing from a down state to an up state	When an interface status update occurs, the ASA waits the number of milliseconds specified in the **health-check monitor-interface debounce-time** command or the ASDM **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** screen before marking the interface as failed and the unit is removed from the cluster. This feature now applies to interfaces changing from a down state to an up state. For example, in the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster unit just because another cluster unit was faster at bundling the ports. We did not modify any commands.
Active/Backup High Availability for ASAv on Microsoft Azure Government Cloud	The stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv in the Microsoft Azure public cloud is now available in the Azure Government Cloud. New or modified command: **failover cloud** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History**
Interface Features	
show interface ip brief and **show ipv6 interface** output enhancement to show the supervisor association for the Firepower 2100/4100/9300	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces. New/Modified commands: **show interface ip brief**, **show ipv6 interface**
The **set lacp-mode** command was changed to **set port-channel-mode** on the Firepower 2100	The **set lacp-mode** command was changed to **set port-channel-mode** to match the command usage in the Firepower 4100/9300. New/Modified FXOS commands: **set port-channel-mode**
Administrative, Monitoring, and Troubleshooting Features	
Support for NTP Authentication on the Firepower 2100	You can now configure SHA1 NTP server authentication in FXOS. New/Modified FXOS commands: **enable ntp-authentication, set ntp-sha1-key-id, set ntp-sha1-key-string** New/Modified Firepower Chassis Manager screens: **Platform Settings** > **NTP** New/Modified options: **NTP Server Authentication: Enable** check box, **Authentication Key** field, **Authentication Value** field

Feature	Description
Packet capture support for matching IPv6 traffic without using an ACL	If you use the **match** keyword for the **capture** command, the **any** keyword only matches IPv4 traffic. You can now specify **any4** and **any6** keywords to capture either IPv4 or IPv6 traffic. The **any** keyword continues to match only IPv4 traffic. New/Modified commands: **capture match**
Support for public key authentication for SSH to FXOS on the Firepower 2100	You can set the SSH key so you can use public key authentication instead of/as well as password authentication. New/Modified FXOS commands: **set sshkey**
Support for GRE and IPinIP encapsulation	When you do a packet capture on interface inside, the output of the command is enhanced to display the GRE and IPinIP encapsulation on ICMP, UDP, TCP, and others. New/Modified commands: **show capture**
Support to enable memory threshold that restricts application cache allocations	You can restrict application cache allocations on reaching certain memory threshold so that there is a reservation of memory to maintain stability and manageability of the device. New/Modified commands: **memory threshold enable, show run memory threshold,clear conf memory threshold**
Support for RFC 5424 logging timestamp	You can enable the logging timestamp as per RFC 5424 format. New/Modified command: **logging timestamp**
Support to display memory usage of TCB-IPS	Shows application level memory cache for TCB-IPS New/Modified command: **show memory app-cache**
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New/Modified command: **snmp-server enable oid**

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- CLI—Use the **show version** command.
- ASDM—Choose **Home** > **Device Dashboard** > **Device Information**.

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Current Version	Interim Upgrade Version	Target Version
9.9(x)	—	Any of the following: → **9.10(x)** → **9.9(x)**
9.8(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)**
9.7(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x)
9.6(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x)
9.5(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x)

Current Version	Interim Upgrade Version	Target Version
9.4(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x)
9.3(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x)

Current Version	Interim Upgrade Version	Target Version
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(5+)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.3(x)	→ 8.4(6)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account. If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs in Version 9.10(x)

The following table lists select open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCuz92333	ASA must not set RS-bit longer than RouterDeadInterval sec - NSF Cisco
CSCva36446	ASA Stops Accepting Anyconnect Sessions/Terminates Connections Right After Successful SSL handshake
CSCvb37736	Formatting the blade results in "Format Failure"
CSCvd64182	Management Interface shows up even when connected switchport is shutdown
CSCvg40735	GTP inspection may spike cpu usage
CSCvg69028	ASA traceback in Thread name: idfw_proc on running "show access-list"
CSCvg74549	Traceback when trying to save/view access-list with object groups (display_hole_og)
CSCvg91150	ASA Traceback in Assert "0" failed: file "timer_services.c"
CSCvh13868	Priority Queueing does not work correctory on ASA5516 platform
CSCvh13869	ASA IKEv2 unable to open aaa session: session limit [2048] reached
CSCvi12735	Traceback and reload when removing access-list configuration
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvj00363	ASA may traceback and reload with combination of packet-tracer and captures
CSCvj40282	Traceback in thread icmp_thread during syslog notify
CSCvj84062	QoS Police not limiting traffic as expected
CSCvj88461	Withdrawal advertisements for specific prefixes are flooded before flooding aggregate prefix
CSCvk12607	FPR4110: ASA drops VPN traffic during rekeying on enabling "crypto engine accelerator-bias ipsec"
CSCvk13703	ASA5585 doesn't use priority RX ring when FlowControl is enabled
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT

Caveat ID Number	Description
CSCvk22322	ASA Traceback (watchdog timeout) when syncing config from active unit (inc. cachefs_umount)
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvk34142	Watchdog on 2100 FTD when logging to flash wraps
CSCvk47577	ASA may traceback in Checkheap due to issue with malloc buffer
CSCvk51181	FTD IPV6 traffic outage after interface edit and deployment part 1/2
CSCvk64990	ASA: Cisco Secure Desktop Host Scanner Bypass
CSCvk65105	Stuck IP from IP Local pool even when user disconnects from Anyconnect
CSCvk69317	Configuration Generation in the crypto portion changes without configuration change
CSCvk69762	Lina traceback at Thread Name: appAgent_monitor_nd_thread
CSCvk70301	VTI IKEv1: Responder-only breaks tunnel during rekey
CSCvk72958	Qos applied on interfaces doesn't work.
CSCvm00066	ASA is stuck on "reading from flash" for several hours
CSCvm00480	CPU spikes on cores in ASA5585-SSP-10
CSCvm08769	Standby unit sending BFD packets with active unit IP, causing BGP neighborship to fail.
CSCvm10086	ASA traceback and reload when issuing "sw-module module ips reload"
CSCvm11643	Inconsistency in the hash value generated in the ASA logs
CSCvm25582	ASA stops encrypting traffic for long sessions
CSCvm36320	match incorrect ACL
CSCvm36461	ASA traceback Thread Name: CMGR Server Processand after upgrade FiePOWER module
CSCvm40288	Port-Channel issues on HA link
CSCvm49260	ASA sending syslog traffic using the wrong interface.
CSCvm50421	ASA traceback on cluster slave node during cluster join due to OSPF and IPv6 used together in ACE
CSCvm53545	ASA may traceback and reload without generating a crashinfo file.
CSCvm63062	ASA stops listening Direct Authentication port for HTTP
CSCvm67174	REST-API on ASA fails with SERVER ERROR when pushing extensive group-policy configuration.

Caveat ID Number	Description
CSCvm67783	BGP tears down in 180 second when used with the VTI.
CSCvm70296	Caveat traceback on FTD 6.2.3.5 Lina process causing HA lost and outage
CSCvm70848	ASA: IPSec SA installation failure due to 'Failed to create session mgmt entry for SPI <>'
CSCvm71014	Access-lists missing / expansion problem, causing outage
CSCvm72541	Connected routes not distributing after new Master election in cluster
CSCvm80779	ASA not inspecting H323 H225
CSCvm82290	ASA core blocks depleted when host unreachable in IRB configuration
CSCvm82993	Upgrade failed on the blade while upgrading ASA from 9.10.0.6 to .8 build
CSCvm86163	ASA Round Robin Pat Ip stickiness not working
CSCvm86443	Only first line of traceroute is captured in event manager output
CSCvm88306	DATAPATH traceback on ASA5585 involving 10GE interface driver (ixgbe)
CSCvm91014	NTP synchronization don't work when setting BVI IF as NTP source interface
CSCvm93860	REST-API Large Data transfer is failing to/from device
CSCvm93972	traceback on ASA5515 with CP Processing thread (accompanied by long CPU hog on the thread)
CSCvm95669	ASA 5506 %Error copying http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img(No space left on device)
CSCvm96400	ASA/IKEv2-L2L: Do not allow two IPsec tunnels with identical proxy IDs
CSCvm96779	FTD HA with encrypted failover link see block depletion of 1550 block
CSCvm97185	FTD crashed with thread name DATAPATH-19-14446 causing failover
CSCvm98344	after failover occurs ASA closes existing management connections with new IP but old MAC

Resolved Bugs in Version 9.10(1)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCuv68725	ASA unable to remove ACE with 'log disable' option
CSCux69220	WebVPN 'enable intf' with DHCP , CLI missing when ASA boot

Caveat ID Number	Description
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416
CSCvc62565	Failover crypto IPsec IKEv2 config does not match when sync with standby
CSCvd13180	AVT : Missing Content-Security-Policy Header in ASA 9.5.2
CSCvd13182	AVT : Missing X-Content-Type-Options in ASA 9.5.2
CSCvd28906	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
CSCvd44525	ASA "show tech" some commands twice, show running-config/ak47 detailed/startup-config errors
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCve53415	ASA traceback in DATAPATH thread while running captures
CSCve85565	Traceback when syslog sent over VPN tunnel
CSCve94917	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
CSCve95403	ASA boot loop caused by logs sent after FIPS boot test
CSCvf18160	ASA traceback on failover sync with WebVPN and shared storage-url config
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf40179	ERROR: Unable to create crypto map: limit reached, when adding entry
CSCvf82832	ASA : ICMPv6 syslog messages after upgrade to 962.
CSCvf85831	asdm displays error uploading image
CSCvf96773	Standby ASA has high CPU usage due to extremely large PAT pool range
CSCvg05442	ASA traceback due to deadlock between DATAPATH and webvpn processes
CSCvg36254	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCvg43389	ASA traceback due to 1550 block exhaustion.
CSCvg58133	Smart licensing doesn't work if ASA hostname is "ASAv"
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg76652	Default DLY value of port-channel sub interface mismatch
CSCvg90365	icmp/telnet traffic fail by ipv6 address on transparent ASA
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module

Caveat ID Number	Description
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh30261	ASA watchdog traceback during context modification/configuration sync
CSCvh46202	Slow 2048 byte block leak due to fragmented traffic over VPN
CSCvh47057	ASA - ICMP flow drops with "no-adjacency" on interface configured in zone when inspection enabled
CSCvh53276	IPv6 protocol 112 packets passing through L2FW are dropping with Invalid IP length message
CSCvh53616	ASA on Firepower Threat Defense devices traceback due to SSL
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh55340	ASA Running config through REST-API Full Backup does not contain the specified context configuration
CSCvh62705	Firepower 2110 ASA : Shared management across context unable to reach to GW
CSCvh70603	change failover standby unit license status "invalid" to "not applicable in standby state"
CSCvh71738	FQDN object are getting resolved after removing access-group configuration
CSCvh75060	Rest-API gives empty response for certain queries
CSCvh77671	ASAv - Traceback in DATAPATH thread due to panic in spin_lock
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh83849	DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping
CSCvh91053	ASA sending DHCP decline | not assiging address to AC clients via DHCP
CSCvh91399	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)
CSCvh92381	ASA Traceback and goes to boot loop on 9.6.3.1
CSCvh95302	ASDM/Webvpn stops working after reload if IPv6 address configured on the interface
CSCvh95960	Using the "match" keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvh97782	KP traceback illegal memory access inside a vendor Modular Exponentiation implementation

Caveat ID Number	Description
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi01376	Upon reboot, non-default SSL commands are removed from the Firepower 4100
CSCvi03103	BGP ASN cause policy deployment failures.
CSCvi07636	ASA: Traceback in Thread Name UserFromCert
CSCvi07974	FTD: Layer 2 protocol packets (ex: BPDUs) are dropped during snort process restarts
CSCvi08450	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition
CSCvi16264	ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure
CSCvi19125	Multicast ip-proto-50 (ESP) dropped by ASP citing 'np-sp-invalid-spi'
CSCvi19220	ASA fails to encrypt after performing IPv6 to IPv4 NAT translation
CSCvi19263	ASA - Traceback while releasing a vpn context spin lock
CSCvi22507	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
CSCvi31540	Traceback and reload with 'show tech' on ASA with No Payload Encryption (NPE)
CSCvi33962	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
CSCvi34164	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
CSCvi35805	ASA Cut-Through Proxy allowing user to access website, but displaying "authentication failed"
CSCvi37644	PKI:- ASA fails to process CRL's with error "Add CA req to pool failed. Pool full."
CSCvi38151	ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs.
CSCvi42008	Stuck uauth entry rejects AnyConnect user connections
CSCvi42965	ASA does not report accurate free memory under "show memory" output
CSCvi44246	Port-channel's subinterfaces share same MAC address on both unit of Threat Defense pair
CSCvi44713	"show memory binsize" and "show memory top-usage" do not show correct information, all show PC 0x0
CSCvi45567	Not able to do snmpwalk when snmpv1&2c host group configured.
CSCvi45807	ASA: DNS expire-entry-timer configuration disappears after reboot

Caveat ID Number	Description
CSCvi46759	Allow ASA to process packet with hop limit of 0 (Follow RFC 8200)
CSCvi48170	SNMP causing slow memory leak
CSCvi49383	Azure: ASAv running Cloud high availability gets in a watchdog crash loop
CSCvi51515	REST-API:500 Internal Server Error
CSCvi53708	ASA NAT position discrepancy between CLI and REST-API causing REST to delete wrong config
CSCvi55070	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
CSCvi55464	ASA5585 device power supply Serial Number not in the snmp response
CSCvi58089	Memory leak on webvpn
CSCvi59968	Firepower 2100 Incorrect reply for SNMP get request 1.3.6.1.2.1.1.2.0
CSCvi64007	Zeroize RSA key after Failover causes REST API to fail to changeto System context
CSCvi65512	FTD: AAB might force a snort restart with relatively low load on the system
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi70606	ASA 9.6(4): WebVPN page not loading correctly
CSCvi76577	ASA:netsnmp:Snmpwalk is failed on some group of IPs of a host-group.
CSCvi77352	Illegal update occurs when device removes itself from the cluster
CSCvi79691	LDAP over SSL crypto engine error
CSCvi79999	256 Byte block leak observed due to ARP traffic when using VTI
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts
CSCvi82779	ASA generate traceback in DATAPATH thread
CSCvi85382	ASA5515 Low DMA memory when ASA-IC-6GE-SFP-A module is installed
CSCvi86799	ASA traceback during output of "show service-policy" with a high number of interfaces and qos
CSCvi87214	Neighbour Solicitation messages are observed for IPv6 traffic
CSCvi87921	ASA self-signed RSA certificate is not allowed for TLS in FIPS mode
CSCvi89194	pki handles: increase and fail to decrement
CSCvi90633	Edit GUI language on ASDM AC downloads but ignores the change FPR-21XX
CSCvi95544	ASA not matching IPv6 traffic correctly in access control license with "any" keyword configured

Caveat ID Number	Description
CSCvi96442	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
CSCvi97729	To-the-box traffic being routing out a data interface when failover is transitioning on a New Active
CSCvi99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj05640	Traceback at snmp address not mapped when snmp-server not enabled
CSCvj15572	Flow-offload rewrite rules not updated when MAC address of interface changes
CSCvj17314	In version 9.7 and lower ASA does not honor "no signature" under saml configuration
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj26450	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvj32264	ASA - zonelabs-integrity : Traceback and High CPU due to Process 'Integrity FW task'
CSCvj37448	ASA : Device sends only ID certificate in SSL server certificate packet after reload
CSCvj37924	CWE-20: Improper Input Validation
CSCvj39858	Traceback: Thread Name: IPsec message handler
CSCvj41748	Bonita BPM app's web pages access fail via webvpn
CSCvj42269	ASA 9.8.2 Receiving syslog 321006 reporting System Memory as 101%
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj44262	portal-access-rule changing from "deny" to "permit"
CSCvj46777	Firepower Threat Defense 2100 asa traceback for unknown reason
CSCvj47256	ASA SIP and Skinny sessions drop, when two subsequent failovers take place
CSCvj48340	ASA memory Leak - snp_svc_insert_dtls_session
CSCvj49883	ASA traceback on Firepower Threat Defense 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby port not coming up after link failure
CSCvj54840	create/delete context stress test causes traceback in nameif_install_arp_punt_service
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic
CSCvj56909	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvj59347	Remove/Increase the maximum 255 characters error limit in result of a cli command!
CSCvj65581	Excessive logging from ftdrpcd process on 2100 series appliances

Caveat ID Number	Description
CSCvj67740	Static IPv6 route prefix will be removed from the ASA configuration
CSCvj67776	clear crypto ipsec ikev2 commands not replicated to standby
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvj73581	Traceback in cli_xml_server Thread
CSCvj74210	Traceback at "ssh" when executing 'show service-policy inspect gtp pdp-context detail'
CSCvj75220	Usage of 'virtual http' or 'virtual telnet' incorrectly needs 'same-security permit intra-interface'
CSCvj75793	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
CSCvj79765	Netflow configuration on Active ASA is replicated in upside down order on Standby unit
CSCvj85516	Packet capture fails for interface named "management" on Firepower Threat Defense
CSCvj88514	IP Local pools configured with the same name.
CSCvj90428	Clock sync issue on ASA with FXOS
CSCvj91449	ASA traceback when logging host command is enable for IPv6 after each reboot
CSCvj91619	1550 Block Depletion Causes ASA to reload 6.2.3.3.
CSCvj95451	webvpn-l7-rewriter: Bookmark logout fails on IE
CSCvj97157	WebPage is not loading due to client rewriter issue on JS files
CSCvj97514	ASA Smart Licensing messaging fails with 'nonce failed to match'
CSCvj98964	ASA may traceback due to SCTP traffic
CSCvk00985	ASA: 9.6.4, 9.8.2 - Failover logging message appears in user context
CSCvk02250	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk07522	webvpn: Bookmark fails to render on Firefox and Chrome. IE fine.
CSCvk08377	ASA 5525 running 9.8.2.20 memory exhaustion.
CSCvk08535	ASA generates warning messages regarding IKEv1 L2L tunnel-groups
CSCvk11898	GTP soft traceback seen while processing v2 handoff
CSCvk14768	ASA traceback with Thread Name: DATAPATH-1-2325

Caveat ID Number	Description
CSCvk18378	ASA Traceback and reload when executing show process (rip: inet_ntop6)
CSCvk18578	Enabling compression necessary to load ASA SSLVPN login page customization
CSCvk19435	Unwanted IE present error when parsing GTP APN Restriction
CSCvk24297	IKEv2 RA with EAP fails due to Windows 10 version 1803 IKEv2 fragmentation feature enabled.
CSCvk25729	Large ACL taking long time to compile on boot causing outage
CSCvk26887	Certificate import from Local CA fails due to invalid Content-Encoding
CSCvk27686	ASA may traceback and reload when acessing qos metrics via ASDM/Telnet/SSH
CSCvk28023	WebVPN: Grammar Based Parser fails to handle META tags
CSCvk30228	ASAv and FTDv deployment fails in Microsoft Azure and/or slow console response
CSCvk30665	ASA "snmp-server enable traps memory-threshold" hogs CPU resulting in "no buffer" drops
CSCvk30739	ASA CP core pinning leads to exhaustion of core-local blocks
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk36087	When logging into the ASA via ASDM, syslog 611101 shows IP as 0.0.0.0 as remote IP
CSCvk36733	mac address is flapping on huasan switch when asa etherchannel is configued with active mode
CSCvk37890	Firepower 2110, Webvpn conditional debugging causes Threat Defense to traceback
CSCvk38176	Traceback and reload due to GTP inspection and Failover
CSCvk43865	Traceback: ASA 9.8.2.28 while doing mutex lock
CSCvk45443	ASA cluster: Traffic loop on CCL with NAT and high traffic
CSCvk47583	ASA WebVPN - incorrect rewriting for SAP Netweaver
CSCvk50732	AnyConnect 4.6 Web-deploy fails on MAC using Safari 11.1.x browsers
CSCvk50815	GTP inspection should not process TCP packets
CSCvk54779	Async queue issues with fragmented packets leading to block depletion 9344
CSCvk57516	Firepower Threat Defense: Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk62896	ASA IKEv2 crash while deleting SAs

Caveat ID Number	Description
CSCvk67239	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvk67569	ASA unable to handle Chunked Transfer-encoding returned in HTTP response pages in Clientless WebVPN
CSCvk70676	Clientless webvpn fails when ASA sends HTTP as a message-body
CSCvm06114	RDP bookmark plugin won't launch
CSCvm07458	Using EEM to track VPN connection events may cause traceback and reload
CSCvm19791	"capture stop" command doesn't work for asp-drop type capture
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm25972	ASA Traceback: Thread Name NIC Status Poll.
CSCvm26004	Incorrect calculation of AAB in ASA causes random AAB invocations.
CSCvm54827	Firepower 2100 ASA Smart Licensing Hostname Change Not Reflected in Smart Account
CSCvm56019	Cisco Adaptive Security Appliance WebVPN - VPN not connecting through Browser
CSCvm67316	ASA: Add additional IKEv2/IPSec debugging for CSCvm70848
CSCvm70848	ASA: IPSec SA installation failure due to 'Failed to create session mgmt entry for SPI <>'
CSCvm80874	ASAv/FP2100 Smart Licensing - Unable to register/renew license

End-User License Agreement

For information on the end-user license agreement, go to http://www.cisco.com/go/warranty.

Related Documentation

For additional information on the ASA, see Navigating the Cisco ASA Series Documentation.