

# Release Notes for the Cisco ASA Series, 9.8(x)

## Release Notes for the Cisco ASA Series, 9.8(x)

This document contains release information for Cisco ASA software Version 9.8(x).

### Important Notes

- **ASDM signed-image support in 9.8(4.45)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message “%ERROR: Signature not valid for file disk0:/<filename>” will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. ([CSCwb05291](#), [CSCwb05264](#))
- 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.

---

- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.7.1.24, 9.8.2.28, or 9.9.2.1 (Release Date: 18-APR-2018), 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 deprecated in the future.

---

- Do not upgrade to 9.8(1) for ASAv on Amazon Web Services--Due to [CSCve56153](#), you should not upgrade to 9.8(1). After upgrading, the ASAv becomes unreachable. Upgrade to 9.8(1.5) or later instead.

- ASAv5 memory issues—Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. The following bugs were fixed in 9.8(1.5) to transparently improve memory function and to optionally allow you to assign more memory to the ASAv5 if necessary: [CSCvd90079](#) and [CSCvd90071](#).
- 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 9.8(4)

**Released: April 24, 2019**

Feature	Description
<b>VPN Features</b>	
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers.  New/Modified commands: <b>hostname(config-webvpn) includesubdomains</b>  <i>Also in 9.12(1).</i>
<b>Administrative Features</b>	

Feature	Description
Allow non-browser-based HTTPS clients to access the ASA	<p>You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients.</p> <p>New/Modified commands: <b>http server basic-auth-client</b></p> <p><i>Also in 9.12(1).</i></p>
<b>show tech-support</b> includes additional output	<p>The output of the <b>show tech-support</b> is enhanced to display the output of the following:</p> <ul style="list-style-type: none"> <li>• <b>show ipv6 interface</b></li> <li>• <b>show aaa-server</b></li> <li>• <b>show fragment</b></li> </ul> <p>New/Modified commands: <b>show tech-support</b></p> <p><i>Also in 9.12(1).</i></p>
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	<p>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.</p> <p>New/Modified command: <b>snmp-server enable oid</b></p> <p><i>Also in 9.10(1).</i></p>

## New Features in ASA 9.8(3)

Released: July 2, 2018

Feature	Description
<b>Platform Features</b>	
Firepower 2100 Active LED now lights amber when in standby mode	Formerly, the Active LED was unlit in standby mode.
<b>Firewall Features</b>	
Support for removing the logout button from the cut-through proxy login page.	<p>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.</p> <p>New/Modified commands: <b>aaa authentication listener no-logout-button.</b></p>
Trustsec SXP connection configurable delete hold down timer	<p>The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds.</p> <p>New/Modified commands: <b>cts sxp delete-hold-down period, show cts sxp connection brief, show cts sxp connections</b></p>

Feature	Description
<b>VPN Features</b>	
Support for legacy SAML authentication	<p>If you deploy an ASA with the fix for <a href="#">CSCvg65072</a>, 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. This option will be deprecated in the near future.</p> <p>New/Modified commands: <b>saml external-browser</b></p>
<b>Interface Features</b>	
Unique MAC address generation for single context mode	<p>You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses.</p> <p>New or modified command: <b>mac-address auto</b></p> <p><i>Also in 9.9(2) and later.</i></p>

## New Features in ASA 9.8(2)

Released: August 28, 2017

Feature	Description
<b>Platform Features</b>	
ASA for the Firepower 2100 series	<p>We introduced the ASA for the Firepower 2110, 2120, 2130, and 2140. Similar to the Firepower 4100 and 9300, the Firepower 2100 runs the base FXOS operating system and then the ASA operating system as an application. The Firepower 2100 implementation couples FXOS more closely with the ASA than the Firepower 4100 and 9300 do (pared down FXOS functions, single device image bundle, easy management access for both ASA and FXOS).</p> <p>FXOS owns configuring hardware settings for interfaces, including creating EtherChannels, as well as NTP services, hardware monitoring, and other basic functions. You can use the Firepower Chassis Manager or the FXOS CLI for this configuration. The ASA owns all other functionality, including Smart Licensing (unlike the Firepower 4100 and 9300). The ASA and FXOS each have their own IP address on the Management 1/1 interface, and you can configure management of both the ASA and FXOS instances from any data interface.</p> <p>We introduced the following commands: <b>connect fxos, fxos https, fxos snmp, fxos ssh, ip-client</b></p>
Department of Defense Unified Capabilities Approved Products List	<p>The ASA was updated to comply with the Unified Capabilities Approved Products List (UC APL) requirements. In this release, when you enter the <b>fips enable</b> command, the ASA will reload. Both failover peers must be in the same FIPS mode before you enable failover.</p> <p>We modified the following command: <b>fips enable</b></p>

Feature	Description
ASAv for Amazon Web Services M4 instance support	You can now deploy the ASAv as an M4 instance. We did not modify any commands.
ASAv5 1.5 GB RAM capability	Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. You can now assign 1.5 GB (up from 1 GB) of RAM to the ASAv5. We did not modify any commands.
<b>VPN Features</b>	
HTTP Strict Transport Security (HSTS) header support	HSTS protects websites against protocol downgrade attacks and cookie hijacking on clientless SSL VPN. It lets web servers declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in <a href="#">RFC 6797</a> . We introduced the following commands: <b>hsts enable</b> , <b>hsts max-age</b> <i>age_in_seconds</i>
<b>Interface Features</b>	
VLAN support for the ASAv50	The ASAv50 now supports VLANs on the ixgbe-vf vNIC for SR-IOV interfaces. We did not modify any commands.

## New Features in ASA 9.8(1.200)

Released: July 30, 2017



**Note** This release is only supported on the ASAv for Microsoft Azure. These features are not supported in Version 9.8(2).

Feature	Description
<b>High Availability and Scalability Features</b>	
Active/Backup High Availability for ASAv on Microsoft Azure	A 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. We introduced the following commands: <b>failover cloud</b> No ASDM support.

## New Features in ASA 9.8(1)

Released: May 15, 2017

Feature	Description
<b>Platform Features</b>	

Feature	Description
ASAv50 platform	The ASAv platform has added a high-end performance ASAv50 platform that provides 10 Gbps Firewall throughput levels. The ASAv50 requires ixgbe-vf vNICs, which are supported on VMware and KVM only.
SR-IOV on the ASAv platform	The ASAv platform supports Single Root I/O Virtualization (SR-IOV) interfaces, which allows multiple VMs to share a single PCIe network adapter inside a host. ASAv SR-IOV support is available on VMware, KVM, and AWS only.
Automatic ASP load balancing now supported for the ASAv	Formerly, you could only manually enable and disable ASP load balancing. We modified the following command: <b>asp load-balance per-packet auto</b>
<b>Firewall Features</b>	
Support for setting the TLS proxy server SSL cipher suite	You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the <b>ssl cipher</b> command. We introduced the following command: <b>server cipher-suite</b>
Global timeout for ICMP errors	You can now set the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet. When this timeout is disabled (the default), and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors. We added the following command: <b>timeout icmp-error</b>
<b>High Availability and Scalability Features</b>	
Improved cluster unit health-check failure detection	You can now configure a lower holdtime for the unit health check: .3 seconds minimum. The previous minimum was .8 seconds. This feature changes the unit health check messaging scheme to <i>heartbeats</i> in the data plane from <i>keepalives</i> in the control plane. Using heartbeats improves the reliability and the responsiveness of clustering by not being susceptible to control plane CPU hogging and scheduling delays. Note that configuring a lower holdtime increases cluster control link messaging activity. We suggest that you analyze your network before you configure a low holdtime; for example, make sure a ping from one unit to another over the cluster control link returns within the <i>holdtime</i> /3, because there will be three heartbeat messages during one holdtime interval. If you downgrade your ASA software after setting the hold time to .3 - .7, this setting will revert to the default of 3 seconds because the new setting is unsupported. We modified the following commands: <b>health-check holdtime, show asp drop cluster counter, show cluster info health details</b>
Configurable debounce time to mark an interface as failed for the Firepower 4100/9300 chassis	You can now configure the debounce time before the ASA considers an interface to be failed, and the unit is removed from the cluster. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. New or modified command: <b>health-check monitor-interface debounce-time</b>
<b>VPN Features</b>	

Feature	Description
Support for IKEv2, certificate based authentication, and ACL in VTI	<p>Virtual Tunnel Interface (VTI) now supports BGP (static VTI). You can now use IKEv2 in standalone and high availability modes. You can use certificate based authentication by setting up a trustpoint in the IPsec profile. You can also apply access lists on VTI using access-group commands to filter ingress traffic.</p> <p>We introduced the following command in the IPsec profile configuration mode: <b>set trustpoint</b>.</p>
Mobile IKEv2 (MobIKE) is enabled by default	<p>Mobile devices operating as remote access clients require transparent IP address changes while moving. Supporting MobIKE on ASA allows a current IKE security association (SA) to be updated without deleting the current SA. MobIKE is “always on.”</p> <p>We introduced the following command: <b>ikev2 mobike-rrc</b>. Used to enable/disable return routability checking.</p>
SAML 2.0 SSO Updates	<p>The default signing method for a signature in a SAML request changed from SHA1 to SHA2, and you can configure which signing method you prefer: <code>rsa-sha1</code>, <code>rsa-sha256</code>, <code>rsa-sha384</code>, or <code>rsa-sha512</code>.</p> <p>We changed the following command in webvpn mode: <b>saml idp signature</b> can be configured with a <i>value</i>. Disabled is still the default.</p>
Change for <b>tunnelgroup webvpn-attributes</b>	<p>We changed the <b>pre-fill-username</b> and <b>secondary-pre-fill-username</b> value from <b>ssl-client</b> to <b>client</b>.</p> <p>We changed the following commands in webvpn mode: <b>pre-fill-username</b> and <b>secondary-pre-fill-username</b> can be configured with a <b>client</b> value.</p>
<b>AAA Features</b>	
Login history	<p>By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days. This feature only applies to usernames in the local database when you enable local AAA authentication for one or more of the management methods (SSH, ASDM, Telnet, and so on).</p> <p>We introduced the following commands: <b>aaa authentication login-history</b>, <b>show aaa login-history</b></p>
Password policy enforcement to prohibit the reuse of passwords, and prohibit use of a password matching a username	<p>You can now prohibit the reuse of previous passwords for up to 7 generations, and you can also prohibit the use of a password that matches a username.</p> <p>We introduced the following commands: <b>password-history</b>, <b>password-policy reuse-interval</b>, <b>password-policy username-check</b></p>

Feature	Description
Separate authentication for users with SSH public key authentication and users with passwords	<p>In releases prior to 9.6(2), you could enable SSH public key authentication (<b>ssh authentication</b>) without also explicitly enabling AAA SSH authentication with the Local user database (<b>aaa authentication ssh console LOCAL</b>). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the <b>ssh authentication</b> command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with <i>passwords</i>, and you can use any AAA server type (<b>aaa authentication ssh console radius_1</b>, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS.</p> <p>We did not modify any commands.</p> <p><i>Also in Version 9.6(3).</i></p>
<b>Monitoring and Troubleshooting Features</b>	
Saving currently-running packet captures when the ASA crashes	<p>Formerly, active packet captures were lost if the ASA crashed. Now, packet captures are saved to disk 0 at the time of the crash with the filename [<i>context_name.</i>]capture_name.<b>pcap</b>.</p> <p>We did not modify any commands.</p>

## 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:

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

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.



**Note** Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.



**Note** For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the [ASA Security Advisories](#).





**Note** ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.  
 ASA 9.2(x) was the final version for the ASA 5505.  
 ASA 9.1(x) was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

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

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 9.8(x) → 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 9.8(x)

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

Caveat ID Number	Description
<a href="#">CSCvj28716</a>	ASA VPN with multiple peers drops incoming packets after failover
<a href="#">CSCvk69317</a>	Configuration Generation in the crypto portion changes without configuration change
<a href="#">CSCvn03552</a>	ASA Traceback with Thread Name: Cluster CFG CLI Rep after removing captures and saving configuration
<a href="#">CSCvn15387</a>	Active unit Tracebacks in 'Thread Name: IKE Daemon'
<a href="#">CSCvn65598</a>	ASDM load fails with the error message: The flash device is in use by another task.
<a href="#">CSCvn82441</a>	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
<a href="#">CSCvo08881</a>	ASA may log negative values for conn-max exceeded syslog and drop permitted traffic
<a href="#">CSCvo14961</a>	ASA may traceback and reload while waiting for "dns_cache_timer" process to finish.
<a href="#">CSCvo30697</a>	Throughput drop when LINA capture is applied on various platforms
<a href="#">CSCvo33216</a>	FasterXML jackson-databind axis2-jaxws Class Server-Side Request Forge
<a href="#">CSCvo33218</a>	FasterXML jackson-databind openjpa Class Blocking Vulnerability
<a href="#">CSCvo33220</a>	FasterXML jackson-databind jboss-common-core Class Blocking Vulnerabil
<a href="#">CSCvo33222</a>	FasterXML jackson-databind axis2-transport-jms Class Blocking Vulnerab
<a href="#">CSCvo33223</a>	FasterXML jackson-databind slf4j-ext Class Arbitrary Code Execution Vu
<a href="#">CSCvo33224</a>	FasterXML jackson-databind Blaze-ds-Opt and Blaze-ds-Core Classes Arbi
<a href="#">CSCvo33226</a>	FasterXML jackson-databind Polymorphic Deserialization External XML En
<a href="#">CSCvo45738</a>	ASA L2TP clients fail to receive IP address from local pool
<a href="#">CSCvo45755</a>	ASA SCP transfer to box stall mid-transfer
<a href="#">CSCvo74631</a>	IKEv2: VTI tunnel doesn't work as expected when both sides are configured as initiator
<a href="#">CSCvo79255</a>	BGP redistribution to OSPF is getting wrong behavior if monitor-interface is enabled
<a href="#">CSCvo85588</a>	Secondary/active FTD does not block connections while TCP syslog server is not reachable.
<a href="#">CSCvp14697</a>	ASA traceback DATAPATH: Thread Name: SXP CORE
<a href="#">CSCvp18878</a>	ASA: Watchdog traceback in Datapath
<a href="#">CSCvp22166</a>	ASA may traceback and reload because the CPU is not yielded for "dns_cache_timer" thread.

Caveat ID Number	Description
<a href="#">CSCvp23530</a>	OSPF neighbor command not replicated to standby after write standby or reload

## Resolved Bugs

This section lists resolved bugs per release.

### Resolved Bugs in Version 9.8(4)

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

Caveat ID Number	Description
<a href="#">CSCux69220</a>	WebVPN 'enable intf' with DHCP , CLI missing when ASA boot
<a href="#">CSCuz70352</a>	Unable to SSH over remote access VPN (telnet, asdm working)
<a href="#">CSCvd28906</a>	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
<a href="#">CSCvd76939</a>	ASA policy-map configuration is not replicated to cluster slave
<a href="#">CSCve53415</a>	ASA traceback in DATAPATH thread while running captures
<a href="#">CSCve85565</a>	Traceback when syslog sent over VPN tunnel
<a href="#">CSCve95403</a>	ASA boot loop caused by logs sent after FIPS boot test
<a href="#">CSCvf83160</a>	Traceback on Thread Name: DATAPATH-2-1785
<a href="#">CSCvf85831</a>	asdm displays error uploading image
<a href="#">CSCvg36254</a>	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
<a href="#">CSCvg40735</a>	GTP inspection may spike cpu usage
<a href="#">CSCvg65072</a>	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
<a href="#">CSCvg76652</a>	Default DLY value of port-channel sub interface mismatch
<a href="#">CSCvh01213</a>	An ASA may Traceback and reload when processing traffic
<a href="#">CSCvh14743</a>	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
<a href="#">CSCvh16252</a>	ASA may traceback and reload in Thread Name: fover_rep during conn replication
<a href="#">CSCvh26447</a>	Firepower 2100 Series might report failure due to MIO-blade heartbeat failure
<a href="#">CSCvh55035</a>	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
<a href="#">CSCvh55340</a>	ASA Running config through REST-API Full Backup does not contain the specified context configuration
<a href="#">CSCvh83849</a>	DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvh95302</a>	ASDM/Webvpn stops working after reload if IPv6 address configured on the interface
<a href="#">CSCvh98781</a>	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
<a href="#">CSCvi03103</a>	BGP ASN cause policy deployment failures.
<a href="#">CSCvi07974</a>	FTD: Layer 2 packets (ex: BPDUs) are dropped during snort restarts (Inline/Passive Interfaces Only)
<a href="#">CSCvi19125</a>	Multicast ip-proto-50 (ESP) dropped by ASP citing 'np-sp-invalid-spi'
<a href="#">CSCvi19220</a>	ASA fails to encrypt after performing IPv6 to IPv4 NAT translation
<a href="#">CSCvi34164</a>	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
<a href="#">CSCvi37644</a>	PKI:- ASA fails to process CRL's with error "Add CA req to pool failed. Pool full."
<a href="#">CSCvi38151</a>	ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs.
<a href="#">CSCvi42008</a>	Stuck uauth entry rejects AnyConnect user connections
<a href="#">CSCvi46759</a>	Allow ASA to process packet with hop limit of 0 (Follow RFC 8200)
<a href="#">CSCvi51515</a>	REST-API:500 Internal Server Error
<a href="#">CSCvi53708</a>	ASA NAT position discrepancy between CLI and REST-API causing REST to delete wrong config
<a href="#">CSCvi54162</a>	"ha-replace" action not working when peer not present
<a href="#">CSCvi55464</a>	ASA5585 device power supply Serial Number not in the snmp response
<a href="#">CSCvi71622</a>	Traceback in DATAPATH on standby FTD
<a href="#">CSCvi77643</a>	Hanging downloads and slow downloads on a FPR4120 due to http inspect
<a href="#">CSCvi79691</a>	LDAP over SSL crypto engine error
<a href="#">CSCvi79999</a>	256 Byte block leak observed due to ARP traffic when using VTI
<a href="#">CSCvi85382</a>	ASA5515 Low DMA memory when ASA-IC-6GE-SFP-A module is installed
<a href="#">CSCvi87214</a>	Neighbour Solicitation messages are observed for IPv6 traffic
<a href="#">CSCvi89194</a>	pki handles: increase and fail to decrement
<a href="#">CSCvi90633</a>	Edit GUI language on ASDM AC downloads but ignores the change FPR-21XX
<a href="#">CSCvi96442</a>	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
<a href="#">CSCvi97729</a>	To-the-box traffic being routing out a data interface when failover is transitioning on a New Active

Caveat ID Number	Description
CSCvj99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj06993	ASA HA with NSF: NSF is not triggered properly when there is an Interface failure in ASA HA
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
CSCvj28643	reload command does not work properly on ASAv
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
CSCvj43591	Firepower 2110 with ASA DHCP does not work properly
CSCvj44262	portal-access-rule changing from "deny" to "permit"
CSCvj46777	Firepower Threat Defense 2100 asa traceback for unknown reason
CSCvj47119	"clear capture /all" might crash Firepower 9300 MI Firepower Threat Defense
CSCvj47256	ASA SIP and Skinny sessions drop, when two subsequent failovers take place
CSCvj48340	ASA memory Leak - snp_svc_insert_dtls_session
CSCvj48542	Trustsec SXP delete hold down timer value needs to be configurable
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
CSCvj56909	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvj58342	Multicast dropped after deleting a security context
CSCvj59347	Remove/Increase the maximum 255 characters error limit in result of a cli command!
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvj67740</a>	Static IPv6 route prefix will be removed from the ASA configuration
<a href="#">CSCvj67776</a>	clear crypto ipsec ikev2 commands not replicated to standby
<a href="#">CSCvj72309</a>	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
<a href="#">CSCvj73581</a>	Traceback in cli_xml_server Thread
<a href="#">CSCvj74210</a>	Traceback at "ssh" when executing 'show service-policy inspect gtp pdp-context detail'
<a href="#">CSCvj75220</a>	Usage of 'virtual http' or 'virtual telnet' incorrectly needs 'same-security permit intra-interface'
<a href="#">CSCvj75793</a>	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
<a href="#">CSCvj79765</a>	Netflow configuration on Active ASA is replicated in upside down order on Standby unit
<a href="#">CSCvj88461</a>	Withdrawal advertisements for specific prefixes are flooded before flooding aggregate prefix
<a href="#">CSCvj88514</a>	IP Local pools configured with the same name.
<a href="#">CSCvj89470</a>	Cisco Adaptive Security Appliance Direct Memory Access Denial of Service Vulnerability
<a href="#">CSCvj91449</a>	ASA traceback when logging host command is enable for IPv6 after each reboot
<a href="#">CSCvj91619</a>	1550 Block Depletion Causes ASA to reload 6.2.3.3.
<a href="#">CSCvj91815</a>	Invalid Http response (IO error during SSL communication) when trying to copy a file from CSM to ASA
<a href="#">CSCvj91858</a>	Cisco Adaptive Security Appliance Access Control List Bypass Vulnerability
<a href="#">CSCvj92048</a>	Large Config and ACL May Cause Data Interface Health Check Fail on Slave Join
<a href="#">CSCvj92444</a>	ASA keeps Type 7 NSSA after losing neighbor
<a href="#">CSCvj95451</a>	webvpn-17-rewriter: Bookmark logout fails on IE
<a href="#">CSCvj97157</a>	WebPage is not loading due to client rewriter issue on JS files
<a href="#">CSCvj97213</a>	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
<a href="#">CSCvj97514</a>	ASA Smart Licensing messaging fails with 'nonce failed to match'
<a href="#">CSCvj98964</a>	ASA may traceback due to SCTP traffic
<a href="#">CSCvk00985</a>	ASA: 9.6.4, 9.8.2 - Failover logging message appears in user context
<a href="#">CSCvk02250</a>	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvk04592</a>	Flows get stuck in lina conn table in half-closed state
<a href="#">CSCvk08377</a>	ASA 5525 running 9.8.2.20 memory exhaustion.
<a href="#">CSCvk08535</a>	ASA generates warning messages regarding IKEv1 L2L tunnel-groups
<a href="#">CSCvk11898</a>	GTP soft traceback seen while processing v2 handoff
<a href="#">CSCvk13703</a>	ASA5585 doesn't use priority RX ring when FlowControl is enabled
<a href="#">CSCvk14537</a>	SSH/Telnet Management sessions may get stuck in pc ftpc_suspend
<a href="#">CSCvk14768</a>	ASA traceback with Thread Name: DATAPATH-1-2325
<a href="#">CSCvk18330</a>	Active FTP Data transfers fail with FTP inspection and NAT
<a href="#">CSCvk18378</a>	ASA Traceback and reload when executing show process (rip: inet_ntop6)
<a href="#">CSCvk18578</a>	Enabling compression necessary to load ASA SSLVPN login page customization
<a href="#">CSCvk19435</a>	Unwanted IE present error when parsing GTP APN Restriction
<a href="#">CSCvk20381</a>	Traceback loop seen on fresh ASAv Azure, KVM and VMWare deployments
<a href="#">CSCvk26887</a>	Certificate import from Local CA fails due to invalid Content-Encoding
<a href="#">CSCvk27686</a>	ASA may traceback and reload when accessing qos metrics via ASDM/Telnet/SSH
<a href="#">CSCvk29263</a>	SSH session stuck after committing changes within a Configure Session.
<a href="#">CSCvk30665</a>	ASA "snmp-server enable traps memory-threshold" hogs CPU resulting in "no buffer" drops
<a href="#">CSCvk30739</a>	ASA CP core pinning leads to exhaustion of core-local blocks
<a href="#">CSCvk31035</a>	KVM (FTD): Mapping web server through outside not working consistent with other platforms
<a href="#">CSCvk34648</a>	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
<a href="#">CSCvk36087</a>	When logging into the ASA via ASDM, syslog 611101 shows IP as 0.0.0.0 as remote IP
<a href="#">CSCvk36733</a>	mac address is flapping on huasan switch when asa etherchannel is configured with active mode
<a href="#">CSCvk38176</a>	Traceback and reload due to GTP inspection and Failover
<a href="#">CSCvk43865</a>	Traceback: ASA 9.8.2.28 while doing mutex lock
<a href="#">CSCvk45443</a>	ASA cluster: Traffic loop on CCL with NAT and high traffic
<a href="#">CSCvk47583</a>	ASA WebVPN - incorrect rewriting for SAP Netweaver



<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvk50815</a>	GTP inspection should not process TCP packets
<a href="#">CSCvk51181</a>	FTD IPV6 traffic outage after interface edit and deployment part 1/2
<a href="#">CSCvk54779</a>	Async queue issues with fragmented packets leading to block depletion 9344
<a href="#">CSCvk57516</a>	Low DMA memory leading to VPN failures due to incorrect crypto maps
<a href="#">CSCvk66771</a>	The CPU profiler stops running without having hit the threshold and without collecting any samples.
<a href="#">CSCvk66963</a>	ASA 9.8.3 Smart Licensing Default Config Incorrect
<a href="#">CSCvk67239</a>	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
<a href="#">CSCvk67569</a>	ASA unable to handle Chunked Transfer-encoding returned in HTTP response pages in Clientless WebVPN
<a href="#">CSCvk70676</a>	Clientless webvpn fails when ASA sends HTTP as a message-body
<a href="#">CSCvk72192</a>	"Free memory" in "show memory" output is wrong as it includes memory utilisation due to overhead
<a href="#">CSCvk72958</a>	Qos applied on interfaces doesn't work.
<a href="#">CSCvm00066</a>	ASA is stuck on "reading from flash" for several hours
<a href="#">CSCvm01053</a>	ASA 9.8(2)24 traceback on FPR9K-SM-44
<a href="#">CSCvm07458</a>	Using EEM to track VPN connection events may cause traceback and reload
<a href="#">CSCvm08769</a>	Standby unit sending BFD packets with active unit IP, causing BGP neighborship to fail.
<a href="#">CSCvm17985</a>	Initiating write net command with management access for BVI interfaces does not succeed
<a href="#">CSCvm19791</a>	"capture stop" command doesn't work for asp-drop type capture
<a href="#">CSCvm23370</a>	ASA: Memory leak due to PC cssls_get_crypto_ctxt
<a href="#">CSCvm24706</a>	GTP delete bearer request is being dropped
<a href="#">CSCvm25972</a>	ASA Traceback: Thread Name NIC Status Poll.
<a href="#">CSCvm34983</a>	IPSEC RAVPN on Spyker fails due to IKEv2 Xuauth install failure
<a href="#">CSCvm36138</a>	With v1 host configured, a v2c walk from that host succeeds
<a href="#">CSCvm36362</a>	Route tracking failure
<a href="#">CSCvm43975</a>	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability

Caveat ID Number	Description
<a href="#">CSCvm49283</a>	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
<a href="#">CSCvm50421</a>	ASA traceback on slave/standby during sync config due to OSPF/EIGRP and IPv6 used together in ACE
<a href="#">CSCvm53531</a>	Cisco Adaptive Security Appliance Software Privilege Escalation Vulnerability
<a href="#">CSCvm54827</a>	Firepower 2100 ASA Smart Licensing Hostname Change Not Reflected in Smart Account
<a href="#">CSCvm55091</a>	HA failed primary unit shows active while "No Switchover" status on FP platforms
<a href="#">CSCvm56019</a>	Cisco Adaptive Security Appliance WebVPN - VPN not connecting through Browser
<a href="#">CSCvm56371</a>	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
<a href="#">CSCvm56719</a>	Traceback high availability standby unit Thread Name: vpnfol_thread_msg
<a href="#">CSCvm65725</a>	ASA kerberos auth fails switch to TCP if server has response too big (ERR_RESPONSE_TOO_BIG)
<a href="#">CSCvm67273</a>	ASA: Memory leak due to PC alloc_fo_ipsec_info_buffer_ver_1+136
<a href="#">CSCvm72378</a>	ASA: CLI: User should not be allowed to create network object "ANY"
<a href="#">CSCvm78449</a>	Unable to modify access control license entry with log default command
<a href="#">CSCvm80779</a>	ASA not inspecting H323 H225
<a href="#">CSCvm80874</a>	ASAv/FP2100 Smart Licensing - Unable to register/renew license
<a href="#">CSCvm82290</a>	ASA core blocks depleted when host unreachable in IRB configuration
<a href="#">CSCvm82930</a>	FTD: SSH to ASA Data interface fails if overlapping NAT statement is configured
<a href="#">CSCvm85257</a>	Spin lock traceback when changing vpn-mode with traffic
<a href="#">CSCvm86443</a>	Only first line of traceroute is captured in event manager output
<a href="#">CSCvm87970</a>	Webvpn Clientless- password management issue
<a href="#">CSCvm91014</a>	NTP synchronization don't work when setting BVI IF as NTP source interface
<a href="#">CSCvm95669</a>	ASA 5506 %Error copying http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img(No space left on device)
<a href="#">CSCvn03966</a>	FTD - When "object-group-search" is pushed through flexconfig, all ACLs get deleted causing outage.
<a href="#">CSCvn09322</a>	FTD device rebooted after taking Active State for less than 5 minutes
<a href="#">CSCvn09367</a>	Prevent administrators from installing CXSC module on ASA 5500-X

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvn09583</a>	show memory has negative values for used memory when low memory condition hit
<a href="#">CSCvn09640</a>	FTD: Need ability to trust ethertype ACLs from the parser. Need to allow BPDU to pass through
<a href="#">CSCvn13556</a>	port-channel IF's Interface number is displayed un-assigned when running at transparent mode
<a href="#">CSCvn15757</a>	ASA may traceback due to SCTP traffic inspection without NULL check
<a href="#">CSCvn17347</a>	Traceback and reload when displaying CPU profiling results
<a href="#">CSCvn19823</a>	ASA : Failed SSL connection not getting deleted and depleting DMA memory
<a href="#">CSCvn22833</a>	ADI process fails to start on ASA on Firepower 4100
<a href="#">CSCvn23254</a>	SNMPv2 pulls empty ifHCInOctets value if Nameif is configured on the interface
<a href="#">CSCvn29446</a>	Keepout configuration on the active ASA can not be synchronized to the standby ASA
<a href="#">CSCvn30108</a>	The 'show memory' CLI output is incorrect on ASAv
<a href="#">CSCvn30393</a>	ASA Traceback in emweb/https during Anyconnect Auth/DAP assessment
<a href="#">CSCvn31347</a>	ACL Unable to configure an ACL after access-group configuration error
<a href="#">CSCvn32620</a>	IKEv2 Failed to obtain an Other VPN license
<a href="#">CSCvn32657</a>	ASA traceback when removing interface configuration used in call-home
<a href="#">CSCvn33943</a>	Standby node traceback in wccp_int_statechange() with HA configuration sync
<a href="#">CSCvn35014</a>	ASA routes change during OS upgrade
<a href="#">CSCvn37829</a>	ASA should allow GCM(SSL) connections to use DMA_ALT1 when primary DMA pool is exhausted
<a href="#">CSCvn38453</a>	ASA: Not able to load Quovadis Root Certificate as trustpoint when FIPS is enabled
<a href="#">CSCvn40592</a>	'No certificate ' command under certificate chain removes wrong certificate
<a href="#">CSCvn44201</a>	ASA discards OSPF hello packets with LLS TLVs sent from a neighbor running on IOS XE 16.5.1 or later
<a href="#">CSCvn44748</a>	Specified virtual mac address could not display when executing "show interface"
<a href="#">CSCvn46425</a>	AnyConnect Cert Auth w/ periodic cert auth fails if failover enabled but other device unreachable
<a href="#">CSCvn47599</a>	RA VPN + SAML authentication causes 2 authorization requests against the RADIUS server
<a href="#">CSCvn47800</a>	ASA stops authenticating new AnyConnect connections due to fiber exhaustion

Caveat ID Number	Description
<a href="#">CSCvn49180</a>	ASA/FTD:MAC address not refreshing after changing member-interface of CCL link
<a href="#">CSCvn55007</a>	DTLS fails after rekey
<a href="#">CSCvn61662</a>	ASA 5500-X may reload without crashinfo written due to CXSC module continuously reloading
<a href="#">CSCvn62787</a>	To support multiple retry on devcmd failure to CRUZ during flow table configuration update.
<a href="#">CSCvn64163</a>	ASA's fail to reboot after power cycle if disk is FSCK'd
<a href="#">CSCvn64418</a>	ISA3000 interoperability issue with Nokia 7705 router
<a href="#">CSCvn67222</a>	DPD doesn't work following a failover, which can (in rare cases) cause an outage if things fail back
<a href="#">CSCvn68527</a>	KP:AnyConnect used IP from pool shows as available
<a href="#">CSCvn69213</a>	ASA traceback and reload due to multiple threads waiting for the same lock - watchdog
<a href="#">CSCvn73962</a>	ASA 5585 9.8.3.14 traceback in Datapath with ipsec
<a href="#">CSCvn76829</a>	ASA as an SSL Client Memory Leak in Handshake Error path
<a href="#">CSCvn78174</a>	traceback on inspect_process
<a href="#">CSCvn78870</a>	ASA Multicontext traceback and reload due to allocate-interface out of range command
<a href="#">CSCvn80394</a>	ASA SNMP CPU Hogs
<a href="#">CSCvn94100</a>	"Process Name: lina"   ASA traceback caused by Netflow
<a href="#">CSCvn96898</a>	Memory Leak in DMA_Pool in binsize 1024 with SCP download
<a href="#">CSCvn97591</a>	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", with circular asp drop captures
<a href="#">CSCvn97733</a>	Syslog ID 111005 generated incorrectly
<a href="#">CSCvo02097</a>	Upgrading ASA cluster to 9.10.1.7 cause traceback
<a href="#">CSCvo03808</a>	Deploy from FMC fails due to OOM with no indication of why
<a href="#">CSCvo06216</a>	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
<a href="#">CSCvo11077</a>	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
<a href="#">CSCvo12057</a>	DHCPRelay does not consume DHCP Offer packet with Unicast flag
<a href="#">CSCvo12504</a>	Failover fsm gets stuck in a multicontext active/active in case of module difference.
<a href="#">CSCvo13497</a>	Unable to remove access-list with 'log default' keyword

Caveat ID Number	Description
<a href="#">CSCvo15497</a>	Tunnel Group: 'no ikev2 local-authentication pre-shared-key' removes local cert authen
<a href="#">CSCvo17775</a>	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
<a href="#">CSCvo23222</a>	AnyConnect session rejected due to resource issue in multi context deployments
<a href="#">CSCvo27109</a>	Standby may enter reboot loop upon upgrading to 9.6(4)20 from 9.6(4)6
<a href="#">CSCvo42174</a>	ASA IPsec VPN EAP Fails to Load Valid Certificate in PKI
<a href="#">CSCvo43795</a>	OSPF Process ID doesnot change even after clearing OSPF process
<a href="#">CSCvo45230</a>	ASA5506 - IBR - not able to ping with hostname if the interface is in BVI in IBR mode
<a href="#">CSCvo47562</a>	VPN sessions failing due to PKI handles not freed during rekeys
<a href="#">CSCvo51265</a>	SCP large file transfer to the box result in a traceback
<a href="#">CSCvo55151</a>	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
<a href="#">CSCvo56675</a>	ASA traceback and reload when trying to switch from ACTIVE to STANDBY. Thread Name: fover_FSM_thread
<a href="#">CSCvo58030</a>	Failover mac address configured on interface does not allow to delete subinterface
<a href="#">CSCvo62031</a>	ASA Traceback and reload while running IKE Debug
<a href="#">CSCvo63240</a>	Smart Tunnel bookmarks don't work after upgrade giving certificate error
<a href="#">CSCvo64516</a>	ASA fails command authorization if tcp syslog is down.
<a href="#">CSCvo66534</a>	Traceback and reload citing Datapath as affected thread
<a href="#">CSCvo74350</a>	ASA may traceback and reload. Potentially related to WebVPN traffic
<a href="#">CSCvo93872</a>	Memory leak while inspecting GTP traffic

### Resolved Bugs in Version 9.8(3)

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

Caveat ID Number	Description
<a href="#">CSCsj42456</a>	ASA 8.0: CSCOPF.CAB has expired Code Signing cert .
<a href="#">CSCth11758</a>	aggregate-auth debugs should mask passwords
<a href="#">CSCuj98977</a>	ASA Traceback in thread SSH when ran "show service set conn detail"
<a href="#">CSCuu67159</a>	ASA: traceback in DATAPATH-2-1157
<a href="#">CSCuv68725</a>	ASA unable to remove ACE with 'log disable' option

Caveat ID Number	Description
<a href="#">CSCuy57310</a>	Cisco Adaptive Security Appliance Traffic Flow Confidentiality Denial of Service Vulnerability
<a href="#">CSCuy60200</a>	ASA traceback in Unicorn Proxy Thread
<a href="#">CSCva92997</a>	9.7.1 traceback in snp_fp_qos
<a href="#">CSCvb53233</a>	ASA 9.1(7)9 Traceback with %ASA-1-199010 and %ASA-1-716528 syslog messages
<a href="#">CSCvb97470</a>	asa Rest-api - component monitoring - empty value/blank value
<a href="#">CSCvd20408</a>	Threat Defense: Interface capture on ASA CLI causes all traffic to be dropped on data-plane
<a href="#">CSCvd33004</a>	_lina_assert in createFoverInterface when configuring failover
<a href="#">CSCvd44525</a>	ASA "show tech" some commands twice, show running-config/ak47 detailed/startup-config errors
<a href="#">CSCvd53381</a>	ASA Traceback when saving/viewing the configuration due to time-range ACLs
<a href="#">CSCvd67907</a>	ASA SSL client does not respond to renegotiation request
<a href="#">CSCvd86411</a>	ASA 9.6.2.11 - Intermittent authentication with CTP uauth in cluster
<a href="#">CSCve02467</a>	ENH: Lower timeout for igp stale-route should be reduced to a value lower than 10 seconds
<a href="#">CSCve18902</a>	Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability
<a href="#">CSCve20395</a>	ASA Portal Java plug-ins fail with the latest Java updates
<a href="#">CSCve34335</a>	Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability
<a href="#">CSCve61540</a>	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
<a href="#">CSCve72964</a>	Traceback in DATAPATH-1-2084 ASA 9.(8)1
<a href="#">CSCve73025</a>	All 1700 "4 byte blocks" were depleted after a weekend VPN load test.
<a href="#">CSCve77049</a>	ASA Memory depletion due to scansafe inspection
<a href="#">CSCve78652</a>	ASA Traceback on Kenton in Thread Name: CTM message handler
<a href="#">CSCve84791</a>	Capturing asp-drop causes unexpected ASA failure
<a href="#">CSCve93327</a>	Snort IAB on FTD requires PDTS to provide perfstat
<a href="#">CSCve94349</a>	SNMP::User is not added to a user-list or host ,after reconfigure it.
<a href="#">CSCve94917</a>	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
<a href="#">CSCve97874</a>	ASA: Low free DMA Memory on Versions 9.6 and later (Applies to ASA 5515 ONLY)

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvf04004</a>	AnyConnect multi-cert auth fails with IPsec and tunnel group URL
<a href="#">CSCvf10327</a>	ENH: Unique IPv6 link-local addresses assigned when sub-interface is being created
<a href="#">CSCvf16310</a>	IPv6 Addresses intermittently assigned to AnyConnect clients
<a href="#">CSCvf17214</a>	ASA Exports ECDSA as corrupted PKCS12
<a href="#">CSCvf18160</a>	ASA traceback on failover sync with WebVPN and shared storage-url config
<a href="#">CSCvf22930</a>	FTD on 2100/4100/9300 Traceback in DATAPATH due to flow offload
<a href="#">CSCvf25666</a>	An ASA with low free memory fails to join existing cluster and could traceback and reload
<a href="#">CSCvf26463</a>	ASA 9.8.1 BVI in routed mode is not doing route lookup for traffic generated from ASA
<a href="#">CSCvf28292</a>	DAP config restored but inactive after backup restore
<a href="#">CSCvf28749</a>	ASA not sending register stop when mroute is configured
<a href="#">CSCvf30738</a>	ASA crashes on DATAPATH due to SIP traffic hitting dynamic NAT rule
<a href="#">CSCvf37947</a>	ASA creates a BVi0 interface on a custom routed context
<a href="#">CSCvf39539</a>	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
<a href="#">CSCvf39679</a>	Unable to add new networks to existing EIGRP configuration
<a href="#">CSCvf40179</a>	ERROR: Unable to create crypto map: limit reached, when adding entry
<a href="#">CSCvf40650</a>	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
<a href="#">CSCvf43019</a>	Webvpn rewriter failing for internal URL
<a href="#">CSCvf43150</a>	ASA// 9.6 // FTP inspection does not allocate new NAT entrie for DATA traffic on Active FTP with PAT
<a href="#">CSCvf43650</a>	OSPF route not getting installed on peer devices when an ASA failover happens with NSF enabled
<a href="#">CSCvf46168</a>	"no capture <name> stop" doesn't change capture status from Stopped
<a href="#">CSCvf49899</a>	ENH: GOID allocation and sync cleanup
<a href="#">CSCvf51066</a>	ASA on FXOS is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
<a href="#">CSCvf54981</a>	ASA - 80 Byte memory block depletion
<a href="#">CSCvf56506</a>	ASA 9.6(2), 9.6(3) traceback in DataPath

Caveat ID Number	Description
<a href="#">CSCvf56774</a>	KP: CPU hogs on standby ASA in fover_parse when performing "write mem all" on active ASA
<a href="#">CSCvf56917</a>	ASA doesn't send LACP PDU during port flap in port-channel
<a href="#">CSCvf57908</a>	Transparent Firewall: Ethertype ACLs installed with incorrect DSAP value
<a href="#">CSCvf59524</a>	Optimization: Allow multiple DATAPATH threads to read compiling tmatch structure in parallel
<a href="#">CSCvf61419</a>	Traceback in thread DATAPATH due to NAT
<a href="#">CSCvf62365</a>	ASA: entConfigChange is unexpectedly sent when secondary ASA is reloaded
<a href="#">CSCvf63108</a>	ASA drops the IGMP Report packet which has Source IP address 0.0.0.0
<a href="#">CSCvf63718</a>	Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability
<a href="#">CSCvf64643</a>	ERROR on Firepower Threat Defense device: Captive-portal port not available. Try again
<a href="#">CSCvf68666</a>	FP2100 IFT customer cannot use ASDM to download image to pc
<a href="#">CSCvf72068</a>	FXOS - ASA/FTD standby unit in transparent mode may still traffic for offloaded flows
<a href="#">CSCvf72930</a>	Firepower Threat Defense may traceback in Thread Name appAgent_monitor_nd_thread during registration
<a href="#">CSCvf74218</a>	ASAv image in AWS GovCloud not working in Hourly Billing Mode
<a href="#">CSCvf76013</a>	ASA crash with snp_egress_capture_sgt()
<a href="#">CSCvf76281</a>	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
<a href="#">CSCvf77377</a>	Hostscan: Errors in cscan.log downloading Microsoft and Panda .dll files
<a href="#">CSCvf79262</a>	OpenSSL CVE-2017-3735 "incorrect text display of the certificate"
<a href="#">CSCvf80539</a>	management-only comes back after reboot
<a href="#">CSCvf81222</a>	Memory leak in 112 byte bin when packet hits PBR and connection is built
<a href="#">CSCvf81672</a>	ASA Routes flushed after failover when etherchannel fails
<a href="#">CSCvf81932</a>	'Incomplete command' error with some inspects due to K7 license
<a href="#">CSCvf82832</a>	ASA : ICMPv6 syslog messages after upgrade to 962.
<a href="#">CSCvf83537</a>	Traceback with traffic in 3 node Intra Chassis Cluster
<a href="#">CSCvf83709</a>	Slave kicked out due to CCL link failure and rejoins, but loses v3 user in multiple context mode



<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvf85065</a>	ASA: Traceback by Thread Name idfw_proc
<a href="#">CSCvf87899</a>	ASA - rare scheduler corruption causes console lock
<a href="#">CSCvf89504</a>	ASA cluster intermittently drop IP fragments when NAT is involved
<a href="#">CSCvf90278</a>	ASA/Firepower Threat Defense traceback when enabling or clearing the packet capture buffer
<a href="#">CSCvf91098</a>	Cisco Firepower 2100 Series Security Appliances IP Fragmentation Denial of Service Vulnerability
<a href="#">CSCvf92262</a>	ASA Webvpn HTTP Strict-Transport-Security Header missing despite fix of CSCvc82150
<a href="#">CSCvf94973</a>	ASA on FP 2100 traceback when uploading AnyConnect image via ASDM or show file system
<a href="#">CSCvf96773</a>	Standby ASA has high CPU usage due to extremely large PAT pool range
<a href="#">CSCvg00265</a>	ASA fails to rejoin the failover HA Or a cluster with insufficient memory error, OGS enabled
<a href="#">CSCvg00565</a>	ASA crashes in glib/g_slice when do "debug menu" self testing
<a href="#">CSCvg01016</a>	ASA does not create pinholes for DCERPC inspection, debug dcerpc shows "MEOW not found".
<a href="#">CSCvg01132</a>	ASA : After upgrading from 9.2(4) to 9.2(4)18 serial connection hangs
<a href="#">CSCvg01827</a>	Permanent License Reservation license not installed on ASA v
<a href="#">CSCvg05250</a>	"clear local-host <IP>" deletes all stub flows present in the entire ASA cluster for all hosts/conns
<a href="#">CSCvg05368</a>	Upon joining cluster slave unit generates ASA-3-202010: NAT/PAT pool exhausted for all PAT'd conns
<a href="#">CSCvg05442</a>	ASA traceback due to deadlock between DATAPATH and webvpn processes
<a href="#">CSCvg06695</a>	Firepower 2100 Threat Defense pair reporting failed status due to "Detect service module failure"
<a href="#">CSCvg07197</a>	ASA : High memory utilization when inspection enabled
<a href="#">CSCvg08891</a>	iPhone IKEv2 PKI leaks over Wi-Fi using local certificate authentication on ASA 5555 9.6.3
<a href="#">CSCvg09778</a>	ASA-SSP HA reload in CP Processing due to DNS inspect
<a href="#">CSCvg12376</a>	Chunk memory not released back to the system after stopping traffic
<a href="#">CSCvg17478</a>	Traceback with Show OSPF Database Commands

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvg20796</a>	ASA local DNS resolution fails when DNS server is reachable over a site to site sec VPN tunnel
<a href="#">CSCvg21077</a>	One node rejoined and traffic restarted will cause the unit 100% CPU due to snpi_untranslate
<a href="#">CSCvg23028</a>	REST-API residues on Firepower Threat Defense (2100, 4100, 9300 Series)
<a href="#">CSCvg23945</a>	ASA panic/crash spin_lock_fair_mode_enqueue: Lock (mps_shash_bucket_t) is held for a long time
<a href="#">CSCvg25175</a>	ASA getting stuck in hung state because of STATIC NAT configuration for SNMP ports
<a href="#">CSCvg25538</a>	FORWARD PORT: 1550/2048/9344 byte memory block depletion due to identity UDP traffic
<a href="#">CSCvg25694</a>	Crash on Standby Firepower 4140 module after Policy deployment.
<a href="#">CSCvg25983</a>	ASA Inter-Site Clustering - Extra ARP not generated when ASA receives unicast ARP request
<a href="#">CSCvg26548</a>	High CPU observed with SFR monitoring mode
<a href="#">CSCvg28370</a>	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
<a href="#">CSCvg29442</a>	When IPsec is enabled, high availability goes in Active-Failed state
<a href="#">CSCvg29692</a>	ASA, when acting as an HTTP client (file copy, etc) sometimes fail to close the connection
<a href="#">CSCvg30391</a>	ASA SNMP OID for ifInDiscards always 0
<a href="#">CSCvg32179</a>	Javascript elements rewriter issue
<a href="#">CSCvg32530</a>	ASA broadcasting packets sent to subnet address as destination IP
<a href="#">CSCvg33669</a>	"OCTEON:DROQ[8] idx: 494 len:0" message appearing on console access of the device
<a href="#">CSCvg33985</a>	Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability
<a href="#">CSCvg35618</a>	Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability
<a href="#">CSCvg38437</a>	ASA AC client PKI username from cert longer than 64 characters - radius username is cut short to 64
<a href="#">CSCvg39447</a>	SNMP deployment failure causes policy rollback
<a href="#">CSCvg39694</a>	FP4120 / ASA 9.6(3)230 "established tcp" not working anymore after SW upgrade
<a href="#">CSCvg43389</a>	ASA traceback due to 1550 block exhaustion.

Caveat ID Number	Description
<a href="#">CSCvg44785</a>	Offloaded flows fail to update their idle timer resulting in connections being incorrectly timed out
<a href="#">CSCvg45952</a>	ASA traceback: thread name scansafe
<a href="#">CSCvg51984</a>	High CPU in IKE Daemon causing slow convergence of VPN tunnels in a scaled environment
<a href="#">CSCvg52545</a>	9300 pair NGFWs in inlineIPS mode do not trigger SNAP packet updates with proper VLAN tags
<a href="#">CSCvg52995</a>	Unable to save configuration in system context after enabling password encryption in ASA
<a href="#">CSCvg53981</a>	"dir /recursive cache:/stc" and "dir cache:stc/2/" list AnyConnect.xsd differently on ASA9.8.2
<a href="#">CSCvg54185</a>	ASA 5506 running on 9.8.2.8 version, memory block of size 80 is getting depleted
<a href="#">CSCvg55617</a>	ASA 9.8.1+ IKEv2 vpn load-balancing sends DELETE following IKE_AUTH
<a href="#">CSCvg56122</a>	SSL handshake fails with large certificate chain size
<a href="#">CSCvg56493</a>	ASA L2TP/IPSEC SMB upload of big files fails - tcp-buffer-timeout drops
<a href="#">CSCvg57954</a>	Modifying service object-groups (add and remove objects) removes ACE
<a href="#">CSCvg58385</a>	ASA reports incorrectly double input packets traffic on PPPoe/VPDN interface
<a href="#">CSCvg58941</a>	Elevated CPU Using Flow-Offload & High Rate of Flow Table Collisions
<a href="#">CSCvg61799</a>	Sysopt permit-vpn behavior change to prevent unintended clear-text traffic
<a href="#">CSCvg61829</a>	SSH/Telnet Traffic, 3-WHS, ACK packets with data is getting dropped - reason (intercept-unexpected)
<a href="#">CSCvg62916</a>	ASA: Software traceback in Thread Name: Dynamic Filter updater
<a href="#">CSCvg65072</a>	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
<a href="#">CSCvg66606</a>	GTP echo response is dropped in ASA cluster
<a href="#">CSCvg67135</a>	ASA backs out of connection when it receives Server Key exchange with named curve as x25519
<a href="#">CSCvg68914</a>	segfault while processing TCP traffic (StreamQueue).
<a href="#">CSCvg72276</a>	Direct Authentication is not working in ASA cluster.
<a href="#">CSCvg73231</a>	ASA/FTD: OSPFv3 stops redistributing routes due to missing LSA after failover
<a href="#">CSCvg81583</a>	Split brain after recovery from interface failure when fover and then data ifc goes down in order.

Caveat ID Number	Description
CSCvg82650	RDP session does not establish after changing SSL certificate on ASA.
CSCvg82932	Memory Leaking on ASA with vpnfol_memory_allocate and vpnfol_data_dyn_string_allocator
CSCvg83623	FTD: IPv6 traffic is not being load-balanced as per 5-tuple algorithm
CSCvg85765	Kenton: ASA5506 traceback on policy deploy
CSCvg85982	ERSPAN not working on Firepower Threat Defense running 6.2.2
CSCvg89102	ASA:multi-session command being configured after write erase
CSCvg89215	ASA crashed with Thread name DATAPATH-1-27929 in 3 node Firepower 9300 Distributed Cluster
CSCvg90061	CSM failed to parse the tcp-state-bypass logs
CSCvg90365	icmp/telnet traffic fail by ipv6 address on transparent ASA
CSCvg90403	Blocks of size 80 leak observed when IRB is used in conjunction with multicast traffic
CSCvg90820	SSPs with ASA in multiple context moves in active-active situation while failover is occurring
CSCvg91038	NAT'd traffic with flow offload is not working in transparent mode.
CSCvg97541	Firepower Threat Defense prefilter policy only fast-paths single direction of bidirectional flow
CSCvg98106	ASA ping to IPv6 address selects egress interface source IP instead of specified source IP
CSCvh03889	Failover Master Passphrase Crash via ASDM
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvh05193	ARP traffic should not be hardcoded to be sent to Snort for inspection
CSCvh13415	ASA:OpenSSL Vulnerabilities CVE-2017-3737 and CVE-2017-3738
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh15344	snmp: After upgradet to 9.6(3)1, the snmpwalk results are different
CSCvh20742	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvh23085	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvh23089	ACLs with source objects that are ranges incorrectly track hit counts

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvh23776</a>	Both ASA traceback in high availability pair on 4140 chassis
<a href="#">CSCvh27703</a>	ASA - Traceback in thread name SSH while applying BGP show commands
<a href="#">CSCvh28309</a>	ASDM stops working with hostscan enabled. ASDM works with hostscan disabled.
<a href="#">CSCvh28763</a>	ASA takes significant time to send ICMPv6 echo when pinging.
<a href="#">CSCvh30261</a>	ASA watchdog traceback during context modification/configuration sync
<a href="#">CSCvh32323</a>	Memory leak in idfw component on ASA
<a href="#">CSCvh32673</a>	Freed memory not released back to the system quick enough on ASA 5506-x platforms
<a href="#">CSCvh44149</a>	ASAv5: Low free DMA memory on 9.8(2) and later
<a href="#">CSCvh46202</a>	Slow 2048 byte block leak due to fragmented traffic over VPN
<a href="#">CSCvh47057</a>	ASA - ICMP flow drops with "no-adjacency" on interface configured in zone when inspection enabled
<a href="#">CSCvh48662</a>	'no snmp-server host <interface> <ip-address>' does not work
<a href="#">CSCvh50032</a>	Unable to completely disable scansafe application health checking
<a href="#">CSCvh53276</a>	IPv6 protocol 112 packets passing through L2FW are dropping with Invalid IP length message
<a href="#">CSCvh53616</a>	ASA on Firepower Threat Defense devices traceback due to SSL
<a href="#">CSCvh54940</a>	ASA traceback with thread name "idfw_proc "
<a href="#">CSCvh55035</a>	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
<a href="#">CSCvh56214</a>	ASA and putty: Incoming packet was garbled on decryption
<a href="#">CSCvh56378</a>	ASA backup command fails to backup identity certificate
<a href="#">CSCvh62164</a>	Firepower 9300 standby stuck in Bulk-Sync state with high CPS traffics on active
<a href="#">CSCvh63896</a>	ASA traceback in threadname CP Processing
<a href="#">CSCvh67981</a>	ASA 9.8.2 Cluster Slave unit traceback when joining cluster and SNMPv3 sync
<a href="#">CSCvh69967</a>	5506 traceback when ASA module and RestAPI both enabled
<a href="#">CSCvh71738</a>	FQDN object are getting resolved after removing access-group configuration
<a href="#">CSCvh72007</a>	Username and privilege display are incorrect when x-auth-token is used for REST API
<a href="#">CSCvh73582</a>	traceback related to SIP inspection processing
<a href="#">CSCvh75025</a>	ASA traceback when failing over to standby unit
<a href="#">CSCvh75060</a>	Rest-API gives empty response for certain queries

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvh77942</a>	new Certificate configuration of primary unit does not sync to standby unit in a Active/Active setup
<a href="#">CSCvh79732</a>	Cisco Adaptive Security Appliance Denial of Service Vulnerability
<a href="#">CSCvh81737</a>	Cisco Adaptive Security Appliance Denial of Service Vulnerability
<a href="#">CSCvh81870</a>	Cisco Adaptive Security Appliance Denial of Service Vulnerability
<a href="#">CSCvh83026</a>	ASA tracebacks intermittently with Thread Name: CTM message handler
<a href="#">CSCvh83145</a>	ASA interface IP and subnet mask changes to 0.0.0.0 0.0.0.0 causing outage of services on interface
<a href="#">CSCvh85514</a>	ASA Traceback in Thread Name: Unicorn Proxy Thread
<a href="#">CSCvh89431</a>	Skinny inspection in Routed ASA with BVIs not letting SCCP phones to register or denying SCCP calls
<a href="#">CSCvh90944</a>	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server
<a href="#">CSCvh90947</a>	ASA traceback with Thread Name: fover_parse
<a href="#">CSCvh91053</a>	ASA sending DHCP decline   not assigning address to AC clients via DHCP
<a href="#">CSCvh91399</a>	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)
<a href="#">CSCvh92381</a>	ASA Traceback and goes to boot loop on 9.6.3.1
<a href="#">CSCvh95325</a>	Standby ASA traceback during replication from mate 9.2(4)27
<a href="#">CSCvh95456</a>	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
<a href="#">CSCvh97782</a>	KP traceback illegal memory access inside a vendor Modular Exponentiation implementation
<a href="#">CSCvh99159</a>	RADIUS authentication/authorization fails for ASDM
<a href="#">CSCvh99896</a>	[ASA]-Master agent is missing user on standby device in multi-context mode
<a href="#">CSCvi01312</a>	webvpn: multiple rendering issues on Confluence and Jira applications
<a href="#">CSCvi01376</a>	Upon reboot, non-default SSL commands are removed from the Firepower 4100
<a href="#">CSCvi06120</a>	vpn-idle-timeout is not triggered after switching to rebooted failover pair
<a href="#">CSCvi07636</a>	ASA: Traceback in Thread Name UserFromCert
<a href="#">CSCvi08450</a>	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition

Caveat ID Number	Description
<a href="#">CSCvi16029</a>	Cisco Adaptive Security Appliance WebVPN Denial of Service Vulnerability
<a href="#">CSCvi16264</a>	ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure
<a href="#">CSCvi19263</a>	ASA 9.7.1.15 Traceback while releasing a vpn context spin lock
<a href="#">CSCvi22507</a>	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
<a href="#">CSCvi23766</a>	IKEv2 stuck Tunnel Manager Entries
<a href="#">CSCvi33962</a>	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
<a href="#">CSCvi35805</a>	ASA Cut-Through Proxy allowing user to access website, but displaying "authentication failed"
<a href="#">CSCvi37889</a>	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", even after removing captures
<a href="#">CSCvi42965</a>	ASA does not report accurate free memory under "show memory" output
<a href="#">CSCvi45567</a>	Not able to do snmpwalk when snmpv1&2c host group configured.
<a href="#">CSCvi45807</a>	ASA: dns expire-entry-timer configuration disappears after reboot
<a href="#">CSCvi46573</a>	ASA: IKEv2 S2S VPN with a dynamic crypto map - ASP table not programmed correctly
<a href="#">CSCvi55070</a>	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
<a href="#">CSCvi58045</a>	interface shutdown command not replicating in HA.
<a href="#">CSCvi58089</a>	Memory leak on webvpn
<a href="#">CSCvi64007</a>	Zeroize RSA key after Failover causes REST API to fail to changeto System context
<a href="#">CSCvi66291</a>	ASA far exceeds 100% rate in TCP Intercept output
<a href="#">CSCvi66905</a>	PIM Auto-RP packets are dropped after cluster master switchover
<a href="#">CSCvi68495</a>	Standby ASA not sending NTP packets to NTP server
<a href="#">CSCvi70606</a>	ASA 9.6(4): WebVPN page not loading correctly
<a href="#">CSCvi76577</a>	ASA:netsnmp:Snmpwalk is failed on some group of IPs of a host-group.
<a href="#">CSCvi77352</a>	Illegal update occurs when device removes itself from the cluster
<a href="#">CSCvi80849</a>	Cisco Firepower 2100 Series POODLE TLS security scanner alerts
<a href="#">CSCvi81436</a>	ASA Lots of 'PPPoE daemon not configured' messages are outputted in console
<a href="#">CSCvi82779</a>	ASA generate traceback in DATAPATH thread

Caveat ID Number	Description
<a href="#">CSCvi86799</a>	ASA traceback during output of "show service-policy" with a high number of interfaces and qos
<a href="#">CSCvi87921</a>	ASA self-signed RSA certificate is not allowed for TLS in FIPS mode
<a href="#">CSCvi89194</a>	pki handles: increase and fail to decrement
<a href="#">CSCvi95544</a>	ASA not matching IPv6 traffic correctly in ACL with "any" keyword configured
<a href="#">CSCvi97776</a>	show environment output incompletely from show tech
<a href="#">CSCvj22929</a>	Reapplying Certificate Chain Configuration Renders LOCAL CA TP Status "Not Authenticated"
<a href="#">CSCvj25817</a>	ASA responds to MOBIKE but clears SA due to DPD.
<a href="#">CSCvj26450</a>	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
<a href="#">CSCvj39858</a>	Traceback: Thread Name: IPsec message handler
<a href="#">CSCvj43591</a>	Firepower 2110 with ASA DHCP does not work properly
<a href="#">CSCvj46777</a>	FPR 2100 asa traceback for unknown reason
<a href="#">CSCvj48542</a>	Trustsec SXP delete hold down timer value needs to be configurable
<a href="#">CSCvj56008</a>	Scansafe feature doesn't work at all for HTTPS traffic

### Resolved Bugs in Version 9.8(2)

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

Caveat ID Number	Description
<a href="#">CSCse02836</a>	ASDM: doesn't show the source port, even when an ACE has one
<a href="#">CSCto19051</a>	Resolve any vulnerabilities in ASA/FTD lina Heimdal Kerberos code
<a href="#">CSCto19832</a>	OpenLDAP needs to be upgraded or patched in ASA/FTD lina process
<a href="#">CSCuj69650</a>	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
<a href="#">CSCuu90811</a>	TLS CTP does not work in TLSv1.2 when GCM ciphers are used
<a href="#">CSCuv63875</a>	ASA traceback in Thread Name:ci/console while running show ospf commands
<a href="#">CSCuw37752</a>	FTP data conn scaling fails with dynamic PAT
<a href="#">CSCuz22961</a>	Support for more than 255 characters for Split DNS value
<a href="#">CSCuz52474</a>	Evaluation of pix-asa for OpenSSL May 2016
<a href="#">CSCuz72137</a>	ASA dropping packets with "novalid adjacency" though valid ARP entry avail



<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCuz77293</a>	OSPF multicast filter rules missing in cluster slave
<a href="#">CSCva69652</a>	NGFW CLI 'show tech-support' missing SNORT data
<a href="#">CSCva92997</a>	9.7.1 traceback in snp_fp_qos
<a href="#">CSCvb40875</a>	Default inspect statements are missing on ASA 5500-x and 2100 device running Threat Defense
<a href="#">CSCvb75685</a>	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
<a href="#">CSCvb91810</a>	ASA - Incorrect interface-based route-lookup if more specific route exist out different interface
<a href="#">CSCvb93926</a>	ENH: Remove DES and 3DES from ASDM AnyConnect IKEv2 Wizard
<a href="#">CSCvc07112</a>	Implement detection and auto-fix capability for scheduler corruption problems
<a href="#">CSCvc27704</a>	Logs lost when TCP is used as transport protocol for Syslogs
<a href="#">CSCvc56526</a>	CEP records edit page take minutes to load
<a href="#">CSCvc72860</a>	Implement debugs to troubleshoot issue where flash becomes read only after ASA is up a long time.
<a href="#">CSCvc76146</a>	981 VTI - Slow BGP neighbor formation after state change
<a href="#">CSCvc82150</a>	PSB Requirement SEC-HTP-HSTS.x4i : HTTP Strict-Transport-Security Header
<a href="#">CSCvc82270</a>	ASA 1550 block gradual depletion
<a href="#">CSCvc83462</a>	gzip compression not working via Webvpn
<a href="#">CSCvc85369</a>	ASA does not respond to IPv6 MLD Query.
<a href="#">CSCvc96614</a>	ASA: IKEv2 ipsec-proposal command removed if more than 9 proposals configured in single command
<a href="#">CSCvd00293</a>	VTI - Some sessions do not get cleared from vpn-sessiondb
<a href="#">CSCvd01101</a>	Syslog logging messages performance is low with tcp protocol
<a href="#">CSCvd01130</a>	ASA TCP SIP inspection translation not working when IP phone is behind VPN tunnel
<a href="#">CSCvd03718</a>	Error configuring the interface in multi-context mode
<a href="#">CSCvd05267</a>	Copy to running-config with a loop reloads the box with no indication as to why
<a href="#">CSCvd17581</a>	ASA IKEv1: Set non-zero SPI in INVALID_ID_INFO Notify
<a href="#">CSCvd20013</a>	Traceback in "Thread Name: IPsec message handler" on EZVPN client
<a href="#">CSCvd25094</a>	Traceback when modifying interfaces. Assert in interface_action.c

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvd26699</a>	ASA erroneously triggers syslog ID 201011
<a href="#">CSCvd28780</a>	Crash when clearing interface configuration and NAT
<a href="#">CSCvd35811</a>	Traceback in thread name DATAPATH
<a href="#">CSCvd36992</a>	Ether-channel: 5585-60 LACP state shows SYSTEM ID of old neighbor on interface which is in disabled
<a href="#">CSCvd37850</a>	9.6.2 DHCPR: Maximum relay bindings (500) exceeded
<a href="#">CSCvd43471</a>	Packets encrypted through virtual tunnel interface have source MAC of 0000.0000.0000
<a href="#">CSCvd46434</a>	ASA crashes after entering the command "debug menu ike-common 11"
<a href="#">CSCvd49262</a>	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
<a href="#">CSCvd49550</a>	ASA with 9.5.1 and above does not show SXP socket when managment0/0 is used as src-ip
<a href="#">CSCvd50107</a>	ASA traceback in Thread name: idfw_proc on running "show access-list", while displaying remark
<a href="#">CSCvd53381</a>	ASA Traceback when saving/viewing the configuration due to time-range ACLs
<a href="#">CSCvd55115</a>	ASA in cluster results in incorrect user group mappings between the Master and Slave
<a href="#">CSCvd58094</a>	ASA traceback in ARP thread, PBR configured
<a href="#">CSCvd58321</a>	Web folder filebrowser applet code signing certificate expired
<a href="#">CSCvd66303</a>	Error deploying ASAv on ESXi vCenter 6.5
<a href="#">CSCvd69551</a>	ASA fails to contact the secondary LDAP server with reactivation mode timed configured
<a href="#">CSCvd71473</a>	ASA: slow memory leak when using many DNS queries
<a href="#">CSCvd75631</a>	Threat Defense DHCP Client tries to request a DHCP address instead of declining
<a href="#">CSCvd76791</a>	Sub-Interfaces Not Supported on SRIOV/IXGBE-VF
<a href="#">CSCvd76821</a>	tcp-options md5 allow is pushed to slave units as tcp-options md5 clear
<a href="#">CSCvd76939</a>	ASA policy-map configuration is not replicated to cluster slave
<a href="#">CSCvd77893</a>	ASA may generate an assert traceback while modifying access-group
<a href="#">CSCvd78444</a>	Traceback due to webvpn process configuration
<a href="#">CSCvd79797</a>	ASA local dns resolution fails when dns server is reachable through a site to site ipsec tunnel

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvd79863</a>	FTD OSPF with ECMP, packets are sent to peer in down state for existing connections
<a href="#">CSCvd80721</a>	In security context, cannot generate the SNMP events trap.
<a href="#">CSCvd82064</a>	Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability
<a href="#">CSCvd82265</a>	Increase memory allocated to rest-agent on ASAv5
<a href="#">CSCvd87211</a>	ASA traceback when trying to remove configured capture
<a href="#">CSCvd87647</a>	ASA traceback in Thread Name: fover_parse performing upgrade from 9.1.5 to 9.4.3
<a href="#">CSCvd89003</a>	ASA traceback observed in Datapath due to SIP inspection
<a href="#">CSCvd89925</a>	Unable to switch standby unit of the failover pair to active
<a href="#">CSCvd90071</a>	Allow ASAv5 to operate using > 1GB memory
<a href="#">CSCvd90079</a>	ASAv5: Reduce DMA packet memory to 64MB
<a href="#">CSCvd90096</a>	WebVPN forces IE to use IE8 mode
<a href="#">CSCvd92196</a>	ASA981 Beta: asp load-balance output inconsistent with show run vs. show run all
<a href="#">CSCvd92423</a>	ASA Traceback in Unicorn Proxy Thread
<a href="#">CSCvd92489</a>	L2TP/IPsec fails when transform-set with mode transport is 11th in dynamic-map
<a href="#">CSCvd96108</a>	Traceback in thread name DATAPATH due to lan to lan VPN
<a href="#">CSCvd97249</a>	FTD: block depletion with continuous SSL traffic and decrypt resign enabled.
<a href="#">CSCvd97568</a>	FTD traceback observed during failover synchronization.
<a href="#">CSCvd97780</a>	ASA/FTD giving incorrect results for "trace" output in packet capture
<a href="#">CSCvd99476</a>	The interactive icons on internal bookmark site not showing properly (+CSCO+0undefined)
<a href="#">CSCvd99859</a>	ASA may drop DNS reply containing only additional RR of type TXT
<a href="#">CSCvd99945</a>	ASA traceback when customer was authenticating to AnyConnect
<a href="#">CSCve00395</a>	ISA 3000: show tech needs to include show inventory
<a href="#">CSCve02469</a>	ASA Issue with bgp route summarization(auto-summary)and route advertisement
<a href="#">CSCve02854</a>	SFR Backplane is pulling the public address for policy match instead of ASA inside address
<a href="#">CSCve03387</a>	Proxy ARP information for SSH NLP NAT is not updating on the FTD upon failover
<a href="#">CSCve03974</a>	ASA with FirePOWER services module generates traceback and reload

Caveat ID Number	Description
<a href="#">CSCve04326</a>	Slave should have use CCL to forward traffic instead of blackholing when egress interface is down
<a href="#">CSCve04443</a>	ASAv Azure: Allow 750 VPN sessions on ASAv30
<a href="#">CSCve05841</a>	ASA reloaded while joining cluster and active as slave
<a href="#">CSCve06436</a>	Routes do not sync properly between different minor versions during hitless upgrade
<a href="#">CSCve07856</a>	CRL verification fails due to incorrect KU after CSCvd41423
<a href="#">CSCve08898</a>	Memory leak with capture with trace and clear capture
<a href="#">CSCve08947</a>	In multi-context ASA drops traffic sourced from certain ports when interface PAT is used
<a href="#">CSCve09249</a>	ASA: Active FTP not working with extended keyword in NAT.
<a href="#">CSCve12654</a>	ASA clustering to support rollback feature with CSM
<a href="#">CSCve13410</a>	Upgrading the ASA results in No Valid adjacency due to track configure on the route
<a href="#">CSCve15873</a>	ASA: Multicast packets getting dropped starting code 9.6.3
<a href="#">CSCve18293</a>	ASA traceback observed in datapath
<a href="#">CSCve18880</a>	Username is not fetched from certificate when certificate map is used in clientless portal
<a href="#">CSCve19179</a>	Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability
<a href="#">CSCve20346</a>	ASA SNI connection fails after upgrade - no shared cipher
<a href="#">CSCve20438</a>	"activate-tunnel-group-scripts" not available in 9.6.3.1
<a href="#">CSCve20980</a>	CSCOGet_origin wrapper doesn't handle 'origin' property if it belongs to Location object
<a href="#">CSCve21824</a>	"hostscan data-limit" service-internal command must be exposed and documented
<a href="#">CSCve23033</a>	ICMP Unreachables (PMTU) dropped indicating "Routing failed to locate next hop"
<a href="#">CSCve23091</a>	Auto-RP packet is dropped due to no-route - No route to host
<a href="#">CSCve23155</a>	BTF not supported on ASA application on FXOS Chassis, but smart licensing show this feature enabled.
<a href="#">CSCve23784</a>	ASA may traceback on displaying access-list config or saving running config
<a href="#">CSCve24088</a>	Smart Licensing ID cert renewal failure should not deregister product instance
<a href="#">CSCve26349</a>	ASDM doesn't display Object Descriptions
<a href="#">CSCve28027</a>	Calls not working with CUCI Lync version 11.6.3 on ASA

Caveat ID Number	Description
<a href="#">CSCve28639</a>	AnyConnect Cert Auth w/ periodic cert auth fails if failover enabled but other device unreachable
<a href="#">CSCve29989</a>	ASA - Traceback in DATAPATH during PAT pool socket allocation
<a href="#">CSCve31809</a>	ASA corrupt dst mac address of return traffic from l2tp client
<a href="#">CSCve31880</a>	network_udpmod_get not releasing shr_lock in rare error case
<a href="#">CSCve34335</a>	SSL Record length verification missing in remove pad length function
<a href="#">CSCve34729</a>	ASA interfaces may stop passing traffic after ASA reload with FIPS mode enabled
<a href="#">CSCve35799</a>	CPU Hog CI_CONSOLE Traceback During Configuration
<a href="#">CSCve37948</a>	ASA does not install routes learned via OSPF over IPSec using UDP/4500
<a href="#">CSCve42460</a>	"NSF IETF/CISCO" commands getting removed on reload
<a href="#">CSCve42583</a>	ASA: IPv6 protocol X rule for passing through FW is dropping packets with Invalid IP length message
<a href="#">CSCve43146</a>	AnyConnect new customization creation fails on ASDM for all ASA versions above 9.5(3)
<a href="#">CSCve44561</a>	ASA sends the ICMP unreachable type 3 code 4 in the wrong direction when SFR redirection enabled
<a href="#">CSCve46883</a>	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
<a href="#">CSCve47393</a>	OSPF Rogue LSA with maximum sequence number vulnerability
<a href="#">CSCve48105</a>	Slave reports Master's interface status as "init" while it is up
<a href="#">CSCve49968</a>	Downloadable ACLs retrieved for Cut Through Proxy in a cluster are not marked dynamic on slaves
<a href="#">CSCve50118</a>	ASA Memory Leak - RSA toolkit
<a href="#">CSCve53582</a>	SSH Connections to ASA fail with SLA monitoring & nonzero floating-conn timeout
<a href="#">CSCve53783</a>	"service resetoutside" impacts to-the-device traffic on all interfaces, behaves different on Standby
<a href="#">CSCve55694</a>	ASDM sets service as "service tcp destination eq -1" when configuring range on service object
<a href="#">CSCve56153</a>	asav in aws: asav unreachable after binary upgrade to 9.8.1
<a href="#">CSCve57150</a>	vpn vlan mapping issue
<a href="#">CSCve57548</a>	ASA- Traceback in 'Thread Name : Datapath' on crypto_SSL functions
<a href="#">CSCve58709</a>	ASA 9.5.1 onwards, Traffic incorrectly routed instead of management interface

Caveat ID Number	Description
CSCve60829	ASA Cluster : Potential UDP loop on cluster link with PAT pool
CSCve61284	ASA Log message 414003 may be generated with bogus IP data when TCP Syslog Server down
CSCve62358	ASA 2048 block depletion when PBR next-hop is interface address
CSCve63762	ASASM: Interface vlans going to admin down after reload.
CSCve64342	'Dynamic Access Policies' page is freezed and unable to access after HS image uninstalled.
CSCve66939	Don't offer 9.8.1 as an upgrade option for ASAs in AWS
CSCve69985	ASDM does not allow more than one static MAC address table entry per interface in transparent mode.
CSCve71661	FTD - Multicast and BPDU traffic dropped due to dst-l2_lookup-fail
CSCve71712	webvpn-17-rewriter: Jira 7.3.0's login page through WebVPN portal does not render completely
CSCve72155	Memory leak at location "snp_fp_encrypt" when syslog server is reachable over the VPN tunnel
CSCve72201	ASA Webvpn Rewriter issue. Unable to browse tabs of WebSite over Clientless VPN
CSCve72227	IPsec SA fail to come up and flap with more than 1000 IPsec SA count in ASA5506/5508/5516
CSCve72433	ASDM error requesting to remove prefix-list used in route-maps for dynamic routing protocol
CSCve73556	ASA traceback on websns_rcv_tcp
CSCve75132	Start of Flow Block event has incorrect number of Initiator Bytes
CSCve76799	ENH: ASA cannot boot up when installed in KVM AHV Nutanix.
CSCve76967	ASDM Where Used option not displaying results
CSCve77440	Traceback in Unicorn Proxy Thread due to Webvpn
CSCve78986	ASA/ 9.6.3 // WebVPN Smart tunnel works but floods windows with event viewer
CSCve85698	ASA WebVPN Rewriter: WebVPN bookmark scholar.google.com not properly written
CSCve87984	Network connectivity is not enabled for more than 19 context
CSCve90305	Contexts are missing on ASA once Chassis reloads after becoming Master on 9.7 and later code
CSCve91223	Standby ASA rejects NAT rule when dest overlaps with interface IP, Active allows this

Caveat ID Number	Description
<a href="#">CSCve92587</a>	Unable to copy anyconnect image via SCP to the ASA flash post upgrade to 9.8(1)
<a href="#">CSCve93019</a>	ASDM Hangs when editing crypto map associated to Dynamic Site-to-Site tunnel
<a href="#">CSCve94828</a>	Cannot create\edit new document with MS Office apps in SP2013
<a href="#">CSCve94886</a>	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
<a href="#">CSCve95969</a>	Unable to scale the flash virtualisation feature up to 250 contexts
<a href="#">CSCve97831</a>	CDA agent stucks in 'Probing' when domain-lookup is enable
<a href="#">CSCve97844</a>	ASA OSPF interface gets stuck in State DOWN (waiting for NSF) after 3rd failover
<a href="#">CSCve99752</a>	Edit Second password on ASDM AC downloads but ignores the change ASA 9.8.1 higher
<a href="#">CSCvf01873</a>	Regex is not matching for HTTP argument field
<a href="#">CSCvf03676</a>	Ports not getting reserved on ASA after adding snmp configuration.
<a href="#">CSCvf07075</a>	ASA - Crypto accelerator traceback in a loop
<a href="#">CSCvf08411</a>	Display of Cipher Algorithms at ASDM is incorrect,when TLS1.2's Cipher Security Level is "medium"
<a href="#">CSCvf11695</a>	Traceback: Duplicate host entries in flow-export action cause crash after policy deployment
<a href="#">CSCvf14391</a>	multicast traffic sourced from anyconnect pool dropped due to reverse path checked.
<a href="#">CSCvf16142</a>	ASA-5-720012:(VPN-Secondary)Failed to update IPSec failover runtime data in ASA cluster environment
<a href="#">CSCvf16429</a>	Ikev2 Remote Access client sessions stuck in Delete state
<a href="#">CSCvf16808</a>	Unable to SSH to Active Unit//TCP connection Limit Exceeded
<a href="#">CSCvf17222</a>	SAML 2.0    (5525) 9.7.1 ASA : ASA compiler not taking the sign-in URL for SAML authentication.
<a href="#">CSCvf17850</a>	ssh/snmp not working in transparent mode after giving 'clear conf int'
<a href="#">CSCvf19938</a>	ASAv: Upgrade issues to the 9.7.1.4 and 9.8.1 when installed on Hyper-V Windows Server 2012-R2
<a href="#">CSCvf21556</a>	ASA: SNMP Host Group not working as required for multi context configuration.
<a href="#">CSCvf24063</a>	ASA5585 traceback in DATAPATH - snp_vpn_process_natt_pkt
<a href="#">CSCvf24387</a>	EC Certificates that are imported to the ASA in PKCS12s cannot be used for SSL
<a href="#">CSCvf31539</a>	ASA Connections stuck in idle state with DCD enabled

Caveat ID Number	Description
<a href="#">CSCvf35263</a>	Port Manager Debug File portmgr.out contains incomplete Timestamps
<a href="#">CSCvf38655</a>	ASA crash in fover_parse after version up
<a href="#">CSCvf39608</a>	Azure-HA: 'clear configure failover' doesn't clear the Peer IP address and sometimes crashes ASAv
<a href="#">CSCvf41547</a>	traceback in watchdog process
<a href="#">CSCvf44142</a>	ASA 9.x: DNS inspection appending "0" on PTR query
<a href="#">CSCvf44950</a>	iOS and OS X IKEv2 Native Clients unable to connect to ASA with EAP-TLS
<a href="#">CSCvf48785</a>	ASA crashes with '[no] nameif' command on cluster interface while running regression
<a href="#">CSCvf54081</a>	TLS version 1.1 connection failed no shared signature algorithms@t1_lib.c:3106

### Resolved Bugs in Version 9.8(1.200)

We did not resolve any bugs in this release.

### Resolved Bugs in Version 9.8(1)

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

Caveat ID Number	Description
<a href="#">CSCuj69650</a>	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
<a href="#">CSCum28756</a>	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
<a href="#">CSCuq80704</a>	ASA classifies TCP packets as PAWS failure incorrectly
<a href="#">CSCut07712</a>	ASA - TO the box traffic break due to int. missing in asp table routing
<a href="#">CSCuu50708</a>	ASA Traceback on 9.1.5.19
<a href="#">CSCuv61791</a>	CWS redirection on ASA may corrupt sequence numbers with https traffic
<a href="#">CSCuv86562</a>	Traceback: ASA crash in thread name fover_health_monitoring_thread
<a href="#">CSCuw71147</a>	Traceback in Unicorn Proxy Thread, in http_header_by_name
<a href="#">CSCuw88759</a>	ASA: Protocol and Status showing UP without connecting the interface
<a href="#">CSCuw95262</a>	After some time flash operations fail and configuration can not be saved
<a href="#">CSCuy22155</a>	ASA generates unexpected syslog messages with mcast routing disabled
<a href="#">CSCuy43438</a>	L2TP over IPSec can not be connected after disconnection from client.
<a href="#">CSCuy55468</a>	Unicorn Proxy Thread causing CP contention
<a href="#">CSCuy60793</a>	Duplicate link-local address observed after failover



<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCuy89288</a>	AnyConnect DTLS on-demand DPDs are not sent intermittently
<a href="#">CSCuz77293</a>	OSPF multicast filter rules missing in cluster slave
<a href="#">CSCva10054</a>	ASA ASSERT traceback in DATAPATH due to sctp inspection
<a href="#">CSCva22048</a>	ASA: SIP Call Drops with PAT when same media port used in multiple calls
<a href="#">CSCva32092</a>	OSPFv3/IPv6 flapping every 30 min between ASA cluster and 4500
<a href="#">CSCva35990</a>	Traceback on CP Process with H323 inspection, rip h323_service_early_msg
<a href="#">CSCva39094</a>	ASA traceback in CLI thread while making MPF changes
<a href="#">CSCva43992</a>	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
<a href="#">CSCva69346</a>	Unable to relay DHCP discover packet from ASA when NAT is matched
<a href="#">CSCva70095</a>	ASA negotiates TLS1.2 when server in tls-proxy
<a href="#">CSCva70979</a>	failover descriptor is not updated in Port Channel interfaces
<a href="#">CSCva71783</a>	ICMP error packets in response to reply packets are dropped
<a href="#">CSCva76568</a>	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
<a href="#">CSCva81412</a>	ASR9000 BGP Graceful Restart doesnt work as expected
<a href="#">CSCva88796</a>	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
<a href="#">CSCva92813</a>	ASA Cluster DHCP Relay doesn't forward the server replies to the client
<a href="#">CSCva92975</a>	ASA 5585-60 dropping out of cluster with traceback
<a href="#">CSCva94702</a>	Enqueue failures on DP-CP queue may stall inspected TCP connection
<a href="#">CSCva98240</a>	SIP: Address from Route: header not translated correctly
<a href="#">CSCvb05667</a>	H.323 inspection causes Traceback in Thread Name: CP Processing
<a href="#">CSCvb08776</a>	Internal ATA Compact Flash size is incorrectly shown in "show version"
<a href="#">CSCvb15265</a>	ASA Page fault traceback in Thread Name: DATAPATH
<a href="#">CSCvb22435</a>	ASA Traceback in thread name CP Processing due to DCERPC inspection
<a href="#">CSCvb22848</a>	ASA 9.1.7-9 crash in Thread Name: NIC status poll
<a href="#">CSCvb25139</a>	IPv6 DNS packets getting malformed when DNS inspection is enabled.
<a href="#">CSCvb26119</a>	Webvpn rewriter failing on matterport.com
<a href="#">CSCvb29688</a>	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416

Caveat ID Number	Description
<a href="#">CSCvb30445</a>	ASA may generate DATAPATH Traceback with policy-based routing enabled
<a href="#">CSCvb31055</a>	ASA Multiple Context SNMP PAT Interface Missing
<a href="#">CSCvb33009</a>	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
<a href="#">CSCvb33013</a>	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
<a href="#">CSCvb38522</a>	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
<a href="#">CSCvb39147</a>	Lower NFS throughput rate on Cisco ASA platform
<a href="#">CSCvb40818</a>	nlp information seen in ipv6 commands
<a href="#">CSCvb40847</a>	ASA not sending Authen Session End log if user logs out manually
<a href="#">CSCvb41097</a>	GTPv2 Dropping instance 1 handoffs
<a href="#">CSCvb43120</a>	ASA Traceback in Checkheaps Thread
<a href="#">CSCvb45039</a>	ASA traceback with Thread Name aaa_shim_thread
<a href="#">CSCvb46321</a>	Cisco ASA Software and Cisco FTD Software TCP Normalizer Denial of Service Vulnerability
<a href="#">CSCvb47006</a>	ASA traceback observed on auto-update thread.
<a href="#">CSCvb48640</a>	Evaluation of pix-asa for Openssl September 2016
<a href="#">CSCvb49264</a>	Delete Bearer Req fails to delete second default bearer after v2 Handoff callflow.
<a href="#">CSCvb49273</a>	Traceback triggered by CoA on ASA when sending/receiving to/from ISE
<a href="#">CSCvb49445</a>	IKEv2: It is NOT cleaning the sessions after disconnected from the client.
<a href="#">CSCvb50301</a>	ASA traceback at Thread Name: rtcli
<a href="#">CSCvb50609</a>	RADIUS authorization request does not send Called-Station-ID attribute
<a href="#">CSCvb50750</a>	Lina core during failover with sip traffic
<a href="#">CSCvb52157</a>	viewer_dart.js file not loading correctly
<a href="#">CSCvb52381</a>	OSPF continuously flaps after master change (L2 cluster, multi-ctx)
<a href="#">CSCvb52492</a>	VPN tunnels are lost after failover due to OSPF route issue
<a href="#">CSCvb52988</a>	ASA Traceback Thread Name: emweb/https
<a href="#">CSCvb53094</a>	ASA : Discrepancy in used memory calculation for Multiple context firewall
<a href="#">CSCvb55721</a>	GARP flood done by ASAs in multi-site cluster using the site-ip address
<a href="#">CSCvb57817</a>	EIGRP: Need to add large number error handling when getting scaled bandwidth

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvb58087</a>	Object-group-search redundant service group objects are incorrectly removed
<a href="#">CSCvb61056</a>	9.6.2 TCP connection doesn't work through L2TP
<a href="#">CSCvb63503</a>	AAA session handle leak with IKEv2 when denied due to time range
<a href="#">CSCvb63819</a>	ASA-SM traceback with Thread : fover_parse during upgrade OS 9.1.6 to 9.4.3
<a href="#">CSCvb64161</a>	ASA fairly infrequently rewrites the dest MAC address of multicast packet for client
<a href="#">CSCvb66593</a>	webvpn_state cookie information disclosure in url
<a href="#">CSCvb68766</a>	ASA traceback at Thread Name: IKE Daemon.
<a href="#">CSCvb74084</a>	SCP fails in 962
<a href="#">CSCvb74249</a>	ASA dropping traffic with TCP syslog configured in multicontext mode
<a href="#">CSCvb75266</a>	ASA - ACL remark displayed incorrectly in the Packet Tracer tool's XML output
<a href="#">CSCvb75685</a>	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
<a href="#">CSCvb78614</a>	4GE-SSM RJ45 interface may drop traffic due to interface "rate limit drops"
<a href="#">CSCvb83446</a>	v1 PDP may get deleted on parse IE failure
<a href="#">CSCvb88126</a>	ASA: Stuck uauth entry rejects AnyConnect connection despite fix for CSCuu48197
<a href="#">CSCvb88358</a>	webvpn-17-rewriter: 5515 9.1.6 Content Rewrite Problem for ASA Web Bookmark
<a href="#">CSCvb89988</a>	WebVPN: Internal page login button not working through rewriter
<a href="#">CSCvb90108</a>	Inconsistent Upper Bounds for Failover Replication Rate Limiting
<a href="#">CSCvb92125</a>	ASA drops DNS PTR Reply with reason Label length exceeded during rewrite
<a href="#">CSCvb92417</a>	Cluster ASA drops to-the-box ICMP replies with reason "inspect-icmp-seq-num-not-matched"
<a href="#">CSCvb92548</a>	ASA matches incorrect ACL with object-group-search enabled
<a href="#">CSCvb92823</a>	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
<a href="#">CSCvb99424</a>	ASA IKEv2 RA VPN does not clearly communicate "No License" status to AnyConnect user
<a href="#">CSCvc00015</a>	Incorrect behaviour when SNMP polling is done on virtual IP of an ASA cluster.
<a href="#">CSCvc00689</a>	ASA : memory leak due to ikev2
<a href="#">CSCvc00760</a>	RDP Plugin Connection failed with error
<a href="#">CSCvc01685</a>	PLR: ASA generates invalid reservation code
<a href="#">CSCvc04741</a>	ASA DHCP relay is incompatible with intercept-dhcp feature

Caveat ID Number	Description
<a href="#">CSCvc05005</a>	ASA cluster TCP/SSL ports are not displayed on LISTEN state
<a href="#">CSCvc06150</a>	ASA unable to add multiple attribute entries in a certificate map
<a href="#">CSCvc07112</a>	Implement detection and auto-fix capability for scheduler corruption problems
<a href="#">CSCvc07330</a>	ASAv may crash when running webvpn
<a href="#">CSCvc11628</a>	Pre-fill feature extracts username from wrong cert (cert 1-machine) for double cert vs.(cert 2-user)
<a href="#">CSCvc14190</a>	ASA fails SSL VPN session establishment with EC under load
<a href="#">CSCvc14448</a>	9.6.2 - Traceback during AnyConnect IKEv2 Performance Test
<a href="#">CSCvc14502</a>	ASA multicontext disallowing new conns with TCP syslog unreachable and logging permit-hostdown set
<a href="#">CSCvc16330</a>	ASA-SM 9.5.2 inspect-sctp licensing breaks existing deployments
<a href="#">CSCvc19318</a>	ASA traceback at Thread Name: sch_syslog
<a href="#">CSCvc22193</a>	DSCP Markings Not Copied to Outer IP Header With IPsec Encapsulation
<a href="#">CSCvc23838</a>	Cisco ASA Heap Overflow in Webvpn CIFS
<a href="#">CSCvc24657</a>	MIB object cempMemPoolHCUsed disappeared
<a href="#">CSCvc24788</a>	ASA: OspfV3 routes are not getting installed
<a href="#">CSCvc25195</a>	ASA portal reveals that multiple context is configured when anyconnect is deployed.
<a href="#">CSCvc25281</a>	Error synchronizing the SNMPv3 user after rebooting a cluster unit
<a href="#">CSCvc25409</a>	ASA memory leak in CloneOctetString when using SNMP polling
<a href="#">CSCvc33796</a>	Implement speed improvements for ACL and NAT table compilation
<a href="#">CSCvc36805</a>	Firepower Threat Defense (FTD) IKEv2 NAT-T gets disabled after reboot
<a href="#">CSCvc37557</a>	SSL connection hangs between ASA and backend server in clientless WebVPN
<a href="#">CSCvc38425</a>	ASA with FirePOWER module generates traceback and reloads or causes process not running
<a href="#">CSCvc39121</a>	Anyconnect address assignment fails using external DHCP server when ASA is in Multi-context Mode
<a href="#">CSCvc44240</a>	ASA clustering: mac-address cmd is ignored on spanned port-channel interface in 9.6.2
<a href="#">CSCvc46502</a>	FTD Cluster 9K block depletion with fragmented Traffic
<a href="#">CSCvc48640</a>	ASA not update access-list dynamically when forward-reference enable is configured

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvc52072</a>	Webvpn portal not displayed correctly for connections landing on default webvpn group.
<a href="#">CSCvc52272</a>	ASA inspection-MPF ACL changes are not getting ordered correctly in the ASP Table
<a href="#">CSCvc52504</a>	ASA may traceback with Thread Name: Unicorn Admin Handler
<a href="#">CSCvc52879</a>	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
<a href="#">CSCvc55674</a>	ASA: IPSec SA failed to come up
<a href="#">CSCvc55974</a>	ikev2 handles get leaked in a L2L setup
<a href="#">CSCvc58272</a>	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue
<a href="#">CSCvc60254</a>	SIP: 200 OK messages with multiple seqments not reassembled correctly
<a href="#">CSCvc60964</a>	ASA L3 Cluster: DHCP relay drops DHCPOFFER in case of asymmetric routing
<a href="#">CSCvc61818</a>	CTP after failed attempt sends the domain along with the username
<a href="#">CSCvc61845</a>	RDP plugin activex Full Screen option is not available with ASA 9.6.2 version
<a href="#">CSCvc62252</a>	Tracking route is up while the reachability is down
<a href="#">CSCvc62556</a>	Traceback in ASA Cluster Thread Name: qos_metric_daemon
<a href="#">CSCvc65409</a>	Traceback observed on gtpv2_process_msg on cluster
<a href="#">CSCvc68229</a>	BGP's BFD support code opens tcp/udp 3784 and 3785 to bypass access-lists
<a href="#">CSCvc77123</a>	ASA may traceback in network_tcpmod_close_conn with AnyConnect IPv6 DTLS stress scenario
<a href="#">CSCvc79077</a>	ASA watchdog traceback during cluster config sync with rest-api enabled
<a href="#">CSCvc79371</a>	ASA nat pool not getting updated correctly.
<a href="#">CSCvc79454</a>	Unable to configure ssh public auth for script users
<a href="#">CSCvc79569</a>	mac-address auto command uses default prefix of 1 on ASA5585-X
<a href="#">CSCvc82146</a>	ASA traceback in threadname Datapath
<a href="#">CSCvc85369</a>	ASA does not respond to IPv6 MLD Query.
<a href="#">CSCvc86554</a>	Traceback: ASA 9.5(2)11 crash Active
<a href="#">CSCvc87914</a>	ASA traceback and Reload on Config Sync Failure
<a href="#">CSCvc88115</a>	ASA Clustering IDFW not updating user mappings
<a href="#">CSCvc88411</a>	1550-byte block depletion seen due to Radius Accounting packets

Caveat ID Number	Description
<a href="#">CSCvc91266</a>	ASA BFD echo function fails if RPF is enabled first.
<a href="#">CSCvc92982</a>	Unable to delete Configured Auto NAT from FMC
<a href="#">CSCvc93947</a>	ASA(9.1.7.12):Connection entries created for multicast streams through standby ASA.
<a href="#">CSCvc97734</a>	Deployment fails when management-only enabled on port-channel interface
<a href="#">CSCvd01736</a>	L2TP connects only sometimes when DHCP used
<a href="#">CSCvd03261</a>	ASAv Goes Unresponsive / VPN fails to function after restart
<a href="#">CSCvd03343</a>	Unable to configure SSH public key auth for non-system contexts
<a href="#">CSCvd06527</a>	SNMPv3 linkup/linkdown should be generated through admin context
<a href="#">CSCvd08200</a>	Slow Memory leak in ASA
<a href="#">CSCvd08479</a>	ACL last hit-cnt counter shows incorrect time
<a href="#">CSCvd08709</a>	asymetric path icmp traffic fails through distributed clustering
<a href="#">CSCvd08983</a>	ASA using TACACS authentication and configured 'password-policy lifetime' will deny access
<a href="#">CSCvd09066</a>	asav-aws: In AWS, excessive console output causes reload CLI to fail
<a href="#">CSCvd18126</a>	ASA traceback in thread name DATAPATH
<a href="#">CSCvd20818</a>	ASA IKEv1: Always accept NAT-T encapsulation mode in transform payload
<a href="#">CSCvd21154</a>	5585 does not unbundle its data intfs for 30 seconds after leaving cluste
<a href="#">CSCvd21541</a>	Cannot delete port-object once created under the Service object group in ASA 944
<a href="#">CSCvd21665</a>	ASA w/ RRI and OSPF : Fails to flush route from ASP routing table
<a href="#">CSCvd23016</a>	ASA may traceback when copying capture out using tftp
<a href="#">CSCvd23471</a>	ASA may traceback while loading a large context config during bootup
<a href="#">CSCvd24066</a>	ASA drops web traffic when IM inspection is enabled.
<a href="#">CSCvd26939</a>	SNMP lists same Hostname for all Firepower Threat Defense managed devices
<a href="#">CSCvd28859</a>	ASA: PBR Memory leak for ICMP traffic
<a href="#">CSCvd39113</a>	Cluster C-Hash table is updated with one more unit despite the new unit didn't join the setup
<a href="#">CSCvd41052</a>	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
<a href="#">CSCvd41423</a>	CRL must be signed by certificate containing cRLSign key usage

Caveat ID Number	Description
<a href="#">CSCvd47781</a>	ASA traceback while doing in-service upgrade
<a href="#">CSCvd49262</a>	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
<a href="#">CSCvd50389</a>	RT#687120: Bookmark Issue with clientless VPN - SAML
<a href="#">CSCvd53884</a>	ASA FirePOWER module data plane down after reload of module
<a href="#">CSCvd55983</a>	Traceback in Thread Name: dhcp_daemon
<a href="#">CSCvd56292</a>	Default "global_policy" service-policy removed after reboot
<a href="#">CSCvd58417</a>	DCERPC inspection drops packets and breaks communication
<a href="#">CSCvd62509</a>	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
<a href="#">CSCvd63718</a>	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER
<a href="#">CSCvd65797</a>	ASA May crash when changing a NAT related object to fqdn
<a href="#">CSCvd77893</a>	ASA may generate an assert traceback while modifying access-group
<a href="#">CSCvd78303</a>	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'

## 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](#).

---

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.