Release Notes for the Cisco ASA Series, 9.9(x)

Release Notes for the Cisco ASA Series, 9.9(x)

This document contains release information for Cisco ASA software Version 9.9(x).

Important Notes

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

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

- 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 depreciated in the future.

- ASA 5506-X memory issues with large configurations on 9.9(2)—If you upgrade to 9.9(2), parts of a very large configuration might be rejected due to insufficient memory with the following message: "ERROR: Insufficient memory to install the rules". One option is to enter the **object-group-search access-control** command to improve memory usage for ACLs; your performance might be impacted, however. Alternatively, you can downgrade to 9.9(1).

- New ROMMON Version 1.1.12 for the ASA 5506-X, 5508-X, and 5516-X—We recommend that you upgrade your ROMMON for several crucial fixes. See https://www.cisco.com/go/asa-firepower-sw, choose your *model* > ASA Rommon Software > 1.1.12. Refer to the release notes on the software download page for more information. To upgrade the ROMMON, see Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X). Note that the ASA running Firepower Threat Defense does not yet support upgrading to this ROMMON version; you can, however, successfully upgrade it in ASA and then reimage to Firepower Threat Defense.

- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

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

System Requirements

This section lists the system requirements to run this release.

ASA and ASDM Compatibility

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

VPN Compatibility

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

New Features

This section lists new features for each release.

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

New Features in ASA 9.9(2)

Released: March 26, 2018

Feature	Description
Platform Features	
ASAv support for VMware ESXi 6.5	The ASAv virtual platform supports hosts running on VMware ESXi 6.5. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASAv on ESXi 6.5. We did not modify any commands.
ASAv support for VMXNET3 interfaces	The ASAv virtual platform supports VMXNET3 interfaces on VMware hypervisors. We did not modify any commands.

Feature	Description
ASAv support for virtual serial console on first boot	You can now configure the ASAv to use the virtual serial console on first boot, instead of the virtual VGA console, to access and configure the ASAv. New or Modified commands: **console serial**
ASAv support to update user-defined routes in more than one Azure subscription for High Availability on Microsoft Azure	You can now configure the ASAv in an Azure High Availability configuration to update user-defined routes in more than one Azure subscription. New or Modified commands: **failover cloud route-table**
VPN Features	
Remote Access VPN multi-context support extended to IKEv2 protocol	Support for configuring ASA to allow Anyconnect and third party Standards-based IPSec IKEv2 VPN clients to establish Remote Access VPN sessions to ASA operating in multi-context mode.
IPv6 connectivity to Radius Servers	ASA 9.9.2 now supports IPv6 connectivity to external AAA Radius Servers.
Easy VPN Enhancements for BVI Support	Easy VPN has been enhanced to support a Bridged Virtual Interface (BVI) as its internal secure interface, and you can now directly configure which interface to use as the internal secure interface. Otherwise, the ASA chooses its internal secure interface using security levels. Also, management services, such as **telnet**, **http**, and **ssh**, can now be configured on a BVI if VPN **management-access** has been enabled on that BVI. For non-VPN management access, you should continue to configure these services on the bridge group member interfaces. New or Modified commands: **vpnclient secure interface** [*interface-name*], **https**, **telnet**, **ssh**, **management-access**
Distributed VPN Session Improvements	• The Active Session Redistribution logic, which balances Distributed S2S VPN active and backup sessions, has been improved. Also, the balancing process may be repeated up to eight times in the background for a single **cluster redistribute vpn-sessiondb** command entered by the administrator. • The handling of dynamic Reverse Route Injections (RRI) across the cluster has been improved.
High Availability and Scalability Features	
Automatically rejoin the cluster after an internal failure	Formerly, many error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals by default: 5 minutes, 10 minutes, and then 20 minutes. These values are configurable. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New or Modified commands: **health-check system auto-rejoin, show cluster info auto-join**

Feature	Description
Configurable debounce time to mark an interface as failed for the ASA 5000-X series	You can now configure the debounce time before the ASA considers an interface to be failed and the unit is removed from the cluster on the ASA 5500-X series. 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. This feature was previously available for the Firepower 4100/9300. New or modified command: **health-check monitor-interface debounce-time**
Show transport related statistics for cluster reliable transport protocol messages	You can now view per-unit cluster reliable transport buffer usage so you can identify packet drop issues when the buffer is full in the control plane. New or modified command: **show cluster info transport cp detail**
Show failover history from peer unit	You can now view failover history from the peer unit, using the **details** keyword . This includes failover state changes and reason for the state change. New or modified command: **show failover**
Interface Features	
Unique MAC address generation for single context mode	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. New or modified command: **mac-address auto** *Also in 9.8(3) and 9.8(4).*
Administrative Features	
RSA key pair supports 3072-bit keys	You can now set the modulus size to 3072. New or modified command: **crypto key generate rsa modulus**
The FXOS bootstrap configuration now sets the enable password	When you deploy the ASA on the Firepower 4100/9300, the password setting in the bootstrap configuration now sets the enable password as well as the admin user password. Requires FXOS Version 2.3.1.
Monitoring and Troubleshooting Features	

Feature	Description
SNMP IPv6 support	The ASA now supports SNMP over IPv6, including communicating with SNMP servers over IPv6, allowing the execution of queries and traps over IPv6, and supporting IPv6 addresses for existing MIBs. We added the following new SNMP IPv6 MIB objects as described in RFC 8096. • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30)—Contains per-interface IPv6-specific information. • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32)—Includes all the prefixes learned by this entity. • ipAddressTable (OID: 1.3.6.1.2.1.4.34)—Contains addressing information relevant to the entity's interfaces. • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35)—Contains the mapping from IP addresses to physical addresses. New or modified command: **snmp-server host** **Note** The **snmp-server host-group** command does not support IPv6.
Conditional Debugging to troubleshoot a single user session	Conditional debugging feature now assists you to verify the logs of specific ASA VPN sessions based on the filter conditions that are set. Support for "any, any" for IPv4 and IPv6 subnets is provided.

New Features in ASA 9.9(1)

Released: December 4, 2017

Feature	Description
Firewall Features	
Ethertype access control list changes	EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access contol entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes. New or modified command: **access-list ethertype** added the new keywords **eii-ipx** and **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}; **capture ethernet-type** no longer supports the **ipx** keyword.
VPN Features	

Feature	Description
Distributed Site-to-Site VPN with clustering on the Firepower 9300	An ASA cluster on the Firepower 9300 supports Site-to-Site VPN in distributed mode. Distributed mode provides the ability to have many Site-to-Site IPsec IKEv2 VPN connections distributed across members of an ASA cluster, not just on the control unit (as in centralized mode). This significantly scales VPN support beyond Centralized VPN capabilities and provides high availability. Distributed S2S VPN runs on a cluster of up to two chassis, each containing up to three modules (six total cluster members), each module supporting up to 6K active sessions (12K total), for a maximum of approximately 36K active sessions (72K total). New or modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **vpn mode** , **show cluster resource usage**, **show vpn-sessiondb** , **show connection detail**, **show crypto ikev2**
High Availability and Scalability Features	
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. New or modified command: **failover cloud** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History** *Also in 9.8(1.200).*
Improved chassis health check failure detection for the Firepower chassis	You can now configure a lower holdtime for the chassis health check: 100 ms. The previous minimum was 300 ms. New or modified command: **app-agent heartbeat interval**
Inter-site redundancy for clustering	Inter-site redundancy ensures that a backup owner for a traffic flow will always be at the other site from the owner. This feature guards against site failure. New or modified commands: **site-redundancy, show asp cluster counter change, show asp table cluster chash-table, show conn flag**
cluster remove unit command behavior matches **no enable** behavior	The **cluster remove unit** command now removes a unit from the cluster until you manually reenable clustering or reload, similar to the **no enable** command. Previously, if you redeployed the bootstrap configuration from FXOS, clustering would be reenabled. Now, the disabled status persists even in the case of a bootstrap configuration redeployment. Reloading the ASA, however, will reenable clustering. New/Modified command: **cluster remove unit**
Administrative, Monitoring, and Troubleshooting Features	
SSH version 1 has been deprecated	SSH version 1 has been deprecated, and will be removed in a future release. The default setting has changed from both SSH v1 and v2 to just SSH v2. New/Modified commands: **ssh version**

Feature	Description
Enhanced packet tracer and packet capture capabilities	The packet tracer has been enhanced with the following features: • Trace a packet when it passes between cluster units. • Allow simulated packets to egress the ASA. • Bypass security checks for a similated packet. • Treat a simulated packet as an IPsec/SSL decrypted packet. The packet capture has been enhanced with the following features: • Capture packets after they are decrypted. • Capture traces and retain them in the persistent list. New or modified commands: **cluster exec capture test trace include-decrypted, cluster exec capture test trace persist, cluster exec clear packet-tracer, cluster exec show packet-tracer id, cluster exec show packet-tracer origin, packet-tracer persist, packet-tracer transmit, packet-tracer decrypted, packet-tracer bypass-checks**

Upgrade the Software

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

ASA Upgrade Path

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

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

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

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
9.8(x)	—	Any of the following: → 9.9(x) → **9.8(x)**
9.3(x)	—	Any of the following: → 9.9(x)
9.2(x)	—	Any of the following: → 9.9(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: → 9.9(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.9(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.9(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.9(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.9(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.9(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.9(x) → 9.1(7.4) → 9.0(4)

Current Version	Interim Upgrade Version	Target Version
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.9(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.9(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 9.9(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 9.9(x)

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

Caveat ID Number	Description
CSCvg72879	9.9.1/SecGW: QP-HA w/ subsecond failover will occasionally have 10-20% packet loss for few mins
CSCvi36891	SecGW - During ASR a window of no vpn-context/rule exists on the cluster
CSCvp16482	ASA reloads when establishing simultaneous ASDM sessions

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.9(2)

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

Caveat ID Number	Description
CSCtk36754	Many HTTP GET for webvpn login page cause high CPU in UnicornProxyThread
CSCvb99424	ASA IKEv2 RA VPN does not clearly communicate "No License" status to AnyConnect user
CSCvc91266	ASA BFD echo function fails if RPF is enabled first.
CSCvd08983	ASA using TACACS authentication and configured 'password-policy lifetime' will deny access
CSCvd97780	ASA/FTD giving incorrect results for "trace" output in packet capture
CSCve02467	ENH: Lower timeout for igp stale-route should be reduced to a value lower than 10 seconds
CSCve76799	ENH: ASAv cannot boot up when installed in KVM AHV Nutanix.
CSCve79555	ASA/FTD traceback when clearing capture - assertion "0" failed: file "mps_hash_table_debug.c"
CSCvf26463	ASA 9.8.1 BVI in routed mode is not doing route lookup for traffic generated from ASA
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf68666	FP2100 IFT customer cannot use ASDM to download image to pc
CSCvf75628	ASAv on Hyper-V shows incorrect 'show interface' outputs: Half-Duplex, 10 Mbps
CSCvf92262	ASA Webvpn HTTP Strict-Transport-Security Header missing despite fix of CSCvc82150
CSCvg01119	IPV4: Implementing buffered reliability mechanism for routing updates
CSCvg01827	Permanent License Reservation license not installed on ASAv
CSCvg06695	Firepower 2100 Threat Defense pair reporting failed status due to "Detect service module failure"
CSCvg29442	When IPSec is enabled HA goes in Active-Failed state with 6.2.3 FMC and 6.2.1 KP
CSCvg58629	HTTP server and Anyconnect SSL VPN cannot coexists on the same interface/port on FTD
CSCvg90061	CSM failed to parse the tcp-state-bypass logs
CSCvh56214	ASA and putty: Incoming packet was garbled on decryption
CSCvh99159	RADIUS authentication/authorization fails for ASDM

Resolved Bugs in Version 9.9(1)

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

Caveat ID Number	Description
CSCth11758	aggregate-auth debugs should mask passwords
CSCuj98977	ASA Traceback in thread SSH when ran "show service set conn detail"
CSCvb53233	ASA 9.1(7)9 Traceback with %ASA-1-199010 and %ASA-1-716528 syslog messages
CSCvb97470	asa Rest-api - component monitoring - empty value/blank value
CSCvd67907	ASA SSL client does not respond to renegotiation request
CSCve02467	ENH: Lower timeout for igp stale-route should be reduced to a value lower than 10 seconds
CSCve72964	Traceback in DATAPATH-1-2084 ASA 9.(8)1
CSCve73025	All 1700 "4 byte blocks" were depleted after a weekend VPN load test.
CSCve94886	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
CSCve97874	ASA: Low free DMA Memory on versions 9.6 and later
CSCvf10327	ENH: Unique IPv6 link-local addresses assigned when sub-interface is being created
CSCvf16310	IPv6 Addresses intermittently assigned to AnyConnect clients
CSCvf16808	Unable to SSH to Active Unit//TCP connection Limit Exceeded
CSCvf17214	ASA Exports ECDSA as corrupted PKCS12
CSCvf25666	An ASA with low free memory fails to join existing cluster and could traceback and reload
CSCvf26463	ASA 9.8.1 BVI in routed mode is not doing route lookup for traffic generated from ASA
CSCvf28292	DAP config restored but inactive after backup restore
CSCvf28749	ASA not sending register stop when mroute is configured
CSCvf31539	ASA Connections stuck in idle state with DCD enabled
CSCvf34791	Install 6.2.2-1290 sfr on a ASA with firepower - asa cores
CSCvf37947	ASA creates a BVi0 interface on a custom routed context
CSCvf38655	ASA traceback in fover_parse after version up
CSCvf39679	Unable to add new networks to existing EIGRP configuration

Caveat ID Number	Description
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf43150	ASA// 9.6 // FTP inspection does not allocate new NAT entrie for DATA traffic on Active FTP with PAT
CSCvf43650	OSPF route not getting installed on peer devices when an ASA failover happens with NSF enabled
CSCvf44142	ASA 9.x: DNS inspection appending "0" on PTR query
CSCvf44950	iOS and OS X IKEv2 Native Clients unable to connect to ASA with EAP-TLS
CSCvf51066	ASA on FXOS is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvf54081	TLS version 1.1 connection failed no shared signature algorithms@t1_lib.c:3106
CSCvf54981	ASA - 80 Byte memory block depletion
CSCvf56506	ASA 9.6(2), 9.6(3) traceback in DataPath
CSCvf56917	ASA doesn't send LACP PDU during port flap in port-channel
CSCvf57908	Transparent Firewall: Ethertype ACLs installed with incorrect DSAP value
CSCvf61419	Traceback in thread DATAPATH due to NAT
CSCvf63108	ASA drops the IGMP Report packet which has Source IP address 0.0.0.0
CSCvf64643	ERROR: Captive-portal port not available. Try again
CSCvf72930	FTD may traceback in Thread Name appAgent_monitor_nd_thread during device registration
CSCvf74218	ASAv image in AWS GovCloud not working in Hourly Billing Mode
CSCvf76281	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCvf79262	OpenSSL CVE-2017-3735 "incorrect text display of the certificate"
CSCvf80539	management-only comes back after reboot
CSCvf81222	Memory leak in 112 byte bin when packet hits PBR and connection is built
CSCvf81932	'Incomplete command' error with some inspects due to K7 license
CSCvf83709	Slave kicked out due to CCL link failure and rejoins, but loses v3 user in multiple context mode
CSCvf85065	ASA: Traceback by Thread Name idfw_proc
CSCvf87899	ASA - rare scheduler corruption causes console lock

Caveat ID Number	Description
CSCvf89504	ASA cluster intermittently drop IP fragments when NAT is involved
CSCvf92262	ASA Webvpn HTTP Strict-Transport-Security Header missing despite fix of CSCvc82150
CSCvf94973	ASA on FP 2100 traceback when uploading AnyConnect image via ASDM
CSCvg01016	ASA does not create pinholes for DCERPC inspection, debug dcerpc shows "MEOW not found".
CSCvg01132	ASA : After upgrading from 9.2(4) to 9.2(4)18 serial connection hangs
CSCvg01827	Permanent License Reservation license not installed on ASAv
CSCvg05250	"clear local-host <IP>" deletes all stub flows present in the entire ASA cluster for all hosts/conns
CSCvg06695	FP2100 Threat Defense pair reporting failed status due to "Detect service module failure"
CSCvg09778	ASA-SSP HA reload in CP Processing due to DNS inspect
CSCvg17478	traceback with Show OSPF Database Commands
CSCvg20796	ASA local DNS resolution fails when DNS server is reachable over a site to site sec VPN tunnel
CSCvg21077	One node rejoined and traffic restarted will cause the unit 100% CPU due to snpi_untranslate
CSCvg23028	REST-API residues on SSP
CSCvg25694	Assert Traceback, thread name : cli_xml_server
CSCvg25983	ASA Inter-Site Clustering - Extra ARP not generated when ASA receives unicast ARP request
CSCvg29442	When IPSec is enabled HA goes in Active-Failed state with 6.2.3 FMC and 6.2.1 KP
CSCvg33669	"OCTEON:DROQ[8] idx: 494 len:0" message appearing on console access of the device
CSCvg55617	ASA 9.8.1+ IKEv2 vpn load-balancing sends DELETE following IKE_AUTH

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.