Release Notes for the Cisco ASA Series, 9.15(x)

Release Notes for the Cisco ASA Series, 9.15(x)

This document contains release information for Cisco ASA software Version 9.15(x).

Important Notes

- **No support in ASA 9.15(1) and later for the ASA 5525-X, ASA 5545-X, and ASA 5555-X**—ASA 9.14(x) is the last supported version. For the ASA FirePOWER module, the last supported version is 6.6.
- **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**—Limited support will continue on releases prior to 9.17(1).
- **For the Firepower 1010, invalid VLAN IDs can cause problems**—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See CSCvw33057 for more information.
- **Upgrade ROMMON for ASA 5506-X, 5508-X, and 5516-X to Version 1.1.15 or later**—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.
- **Upgrade ROMMON for the ISA 3000 to Version 1.0.5 or later**——There is a new ROMMON version for the ISA 3000 (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 1.0.5 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.
- **SAMLv1 feature deprecation**—Support for SAMLv1 is deprecated.
- **Low-Security Cipher Removal in ASA 9.15(1)**—Support for the following less secure ciphers used by IKE and IPsec have been removed:
  - Diffie-Hellman groups: 2 and 24
  - Encryption algorithms: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
  - Hash algorithms: MD5

Note Low-security SSH and SSL ciphers have not yet been removed.

Before you upgrade from an earlier version of ASA to Version 9.15(1), you must update your VPN configuration to use the ciphers supported in 9.15(1), or else the old configuration will be rejected. When the configuration is rejected, one of the following actions will occur, depending on the command:

- The command will use the default cipher.
- The command will be removed.

Fixing your configuration before upgrading is especially important for clustering or failover deployments. For example, if the secondary unit is upgraded to 9.15(1), and the removed ciphers are synced to this unit from the primary, then the secondary unit will reject the configuration. This rejection might cause unexpected behavior, like failure to join the cluster.

IKEv1: The following subcommands are removed:

- **crypto ikev1 policy** *priority*:
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2: The following subcommands are removed:

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec: The following subcommands are removed:

- **crypto ipsec ikev1 transform-set** ***name*** **esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal** ***name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile** ***name***

- **set pfs group2 group24**

Crypto Map: The following subcommands are removed:

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**

- **Re-introduction of CRL Distribution Point configuration**—The static CDP URL configuration option, that was removed in 9.13(1), was re-introduced in the **match-certificate** command.
- **Restoration of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was restored.

  The following subcommands were restored:

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

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 9.15(1)

Released: November 2, 2020

Feature	Description
Platform Features	
ASAv for the Public Cloud	We introduced the ASAv for the following Public Cloud offerings: • Oracle Cloud Infrastrucure (OCI) • Google Cloud Platform (GCP) No modified commands.
ASAv support for Autoscale	The ASAv now supports Autoscale for the following Public Could offerings: • Amazon Web Services (AWS) • Miscrosoft Azure Autoscaling increases or decreases the number of ASAv application instances based on capacity requirements. No modified commands.
ASAv for Microsoft Azure support for Accelerated Networking (SR-IOV).	The ASAv on the Microsoft Azure Public Cloud now supports Azure's Accelerated Networking (AN), which enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. No modified commands.
Firewall Features	

Feature	Description
Changes to PAT address allocation in clustering. The PAT pool **flat** option is now enabled by default and it is not configurable.	The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the master instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally included the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address. As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1023 - 65535. Previously, you could optionally use a flat range by including the **flat** keyword in a PAT pool rule. The **flat** keyword is no longer supported: the PAT pool is now always flat. The **include-reserve** keyword, which was previously a sub-keyword to **flat**, is now an independent keyword within the PAT pool configuration. With this option, you can include the 1 - 1023 port range within the PAT pool. Note that if you configure port block allocation (the **block-allocation** PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster. New/Modified commands: **nat**, **show nat pool**
XDMCP inspection disabled by default in new installations.	Previously, XDMCP inspection was enabled by default for all traffic. Now, on new installations, which includes new systems and reimaged systems, XDMCP is off by default. If you need this inspection, please enable it. Note that on upgrades, your current settings for XDMCP inspection are retained, even if you simply had it enabled by way of the default inspection settings.
High Availability and Scalability Features	
Disable failover delay	When you use bridge groups or IPv6 DAD, when a failover occurs the new active unit waits up to 3000 ms for the standby unit to finish networking tasks and transition to the standby state. Then the active unit can start passing traffic. To avoid this delay, you can disable the waiting time, and the active unit will start passing traffic before the standby unit transitions. New/Modified commands: **failover wait-disable**
Routing Features	
Multicast IGMP interface state limit raised from 500 to 5000	The multicast IGMP state limit per interface was raised from 500 to 5000. New/Modified commands: **igmp limit** *Also in 9.12(4).*
Interface Features	
DDNS support for the web update method	You can now configure an interface to use DDNS with the web update method. New/Modified commands: **show ddns update interface**, **show ddns update method**, **web update-url**, **web update-type**

Feature	Description
Certificate Features	
Modifications to Match Certificate commands to support static CRL Distribution Point URL	The static CDP URL configuration commands allowed CDPs to be mapped uniquely to each certificate in a chain that is being validated. However, only one such mapping was supported for each certificate. This modification allows statically configured CDPs to be mapped to a chain of certificates for authentication. New/Modified commands: **match certificate override cdp**,
Administrative and Troubleshooting Features	
Manual import of node secret file from the RSA Authentication Manager for SDI AAA server groups.	You can import the node secret file that you export from the RSA Authentication Manager for use with SDI AAA server groups. We added the following commands: **aaa sdi import-node-secret**, **clear aaa sdi node-secret**, **show aaa sdi node-secrets**.
show fragment command output enhanced	The output for **show fragment** command was enhanced to include IP fragment related drops and error counters. No modified commands.
show tech-support command output enhanced	The output for **show tech-support** command was enhanced to include the bias that is configured for the crypto accelerator. The bias value can be ssl, ipsec, or balanced. No modified commands.
Monitoring Features	
Support to configure cplane keepalive holdtime values	Due to communication delays caused by high CPU usage, the response to the keepalive event fails to reach ASA, resulting in trigerring failover due to card failure. You can now configure the keepalive timeout period and the maximum keepalive counter value to ensure sufficient time and retries are given. New/Modified commands: **service-module**
VPN Features	
Support for configuring the maximum in-negotiation SAs as an absolute value	You can now configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity; formerly, only a percentage was allowed. New/Modified commands: **crypto ikev2 limit max-in-negotiation-sa value** *Also in 9.12(4).*
Cross-Site Request Forgery (CSRF) Vulnerabilities Prevention for WebVPN Handlers	ASA provides protection against CSRF attacks for WebVPN handlers. If a CSRF attack is detected, a user is notified by warning messages. This feature is enabled by default.
Kerberos server validation for Kerberos Constrained Delegation (KCD).	When configured for KCD, the ASA initiates an AD domain join with the configured server in order to acquire Kerberos keys. These keys are required for the ASA to request service tickets on behalf of clientless SSL VPN users. You can optionally configure the ASA to validate the identity of the server during domain join. We modified the **kcd-server** command to add the **validate-server-certificate** keyword.

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 9.14(x) was the final version for the ASA 5525-X, 5545-X, and 5555-X.

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
9.14(x)	—	Any of the following: → 9.15(x)
9.13(x)	—	Any of the following: → 9.15(x) → 9.14(x)
9.12(x)	—	Any of the following: → 9.15(x) → 9.14(x)

Current Version	Interim Upgrade Version	Target Version
9.10(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.6(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.4(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	Any of the following: → 9.15(x) → 9.14(x) → 9.12(x) → 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: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 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 9.15(x)

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

Caveat ID Number	Description
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvp69936	ASA : Traceback on tcp_intercept Thread name : Threat detection
CSCvq29993	6.4.0-102 2140 w/ SSL policy runs out of 1550 and 9472 blocks. doesn't recover
CSCvq33761	ASA traceback when running "no threat-detection statistics tcp-intercept" command
CSCvq36879	ASA/Lina traceback in DATAPATH
CSCvr29769	Using EEM on ASA may cause HA pair to reload when resources are depleted.

Caveat ID Number	Description
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvu50049	ASA:Not replicating specific configuration to standby ASA when copying config file to the active ASA
CSCvu71568	2100: incoming packets dropped due to "no buffer" and outgoing packets leading to block depletion
CSCvu73496	Internal1/1 data interface goes down without any reason or logs.
CSCvu76937	snort-busy counter incrementing while snort cpu less than 40%
CSCvv17509	ASA: Unexpected traceback and reload due to DRBG health check failure
CSCvv19521	FTD with RAVPN and sysopt connection permit-vpn, stops working when adding a monitor rule
CSCvv30172	Intermittently after reboot, ADI can't join KCD
CSCvv30476	Clear crypto ipsec sa inactive command not deleting outbound SAs
CSCvv32160	Failover: standby unit crashed during modifying access-lists, with high CPU utilization
CSCvv34851	6.7.0-1992: SSL info is not populated in the FMC connection events page
CSCvv38481	Improper ordering of context between primary and secondary ASA units in multi-context mode
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvv50265	DAP - No Client Certificate information is passed to DAP
CSCvv51232	SNMP traps not generated on FP 2100 after changing from platform to appliance mode on 9.14.1.15
CSCvv65648	ISA-3000 hardware-bypass behavior is not changed after write erase
CSCvv69392	ASA/FTD may traceback and reload in Thread Name 'IKE Daemon'
CSCvv70984	ASA traceback while modifying the bookmark SSL Ciphers configuration
CSCvv71435	ASA 256 and 1550 block depletion causes DMA Memory unreleased allocation
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73786	ASA should use IPv4 for OCSP as a fallback method because IPv6 is not supported
CSCvv76249	ASA not closing connections associated with terminated S2S connection
CSCvv78039	Static routes not replicating to Standby Unit.
CSCvv82254	FPR-2110 traceback with crypto_pki traceback

Caveat ID Number	Description
CSCvv82389	SOF seen after EOF for a connection without any further packets
CSCvv85029	ASA5555 traceback and reload on Thread Name: ace_work
CSCvv86718	ASA traceback "Address not mapped" "periodic_handler_internal"
CSCvv87232	ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process
CSCvv88523	SSL VPN connection failed to establish when the counter of active session reaching a certain value
CSCvv94701	ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.
CSCvv95805	ASA5516 9.12.3 crash and reboot for the active unit (Octeon crash)
CSCvv97877	Secondary unit not able to join the cluster
CSCvv99256	Large object-group config with increased control point CPU usage can lead to config sync failure
CSCvw00161	ASA traceback and reload due to VPN thread on firepower 2140
CSCvw00516	Fragments in Q-in-Q frames are dropped by lina when using inline set
CSCvw03373	ASA is getting traceback and reload frequently due to memory corruption
CSCvw03628	ASA will not import CA certificate with name constraint of RFC822Name set as empty
CSCvw06298	Duplicate MAC Addresses in Shared Interfaces of Contexts
CSCvw07407	FTD/HA: "no shutdown" command disappear from running-config of standby
CSCvw07687	FTD Traceback On appAgent_hb_receiver_thread
CSCvw08643	Stale VPN Context seen for AnyConnect IKEv2 sessions
CSCvw08722	AnyConnect client-to-client communication (Cisco IP Phone Calls) blocked after upgrade to 9.12(4)
CSCvw09521	ASA traceback and reload on NTP thread triggered watch dog
CSCvw09790	ASAv traceback and reload in thread name Pthread on version 9.12(3)9
CSCvw12040	Heapcache Memory depleting rapidly due to certificate chain failed validation
CSCvw14711	IKEv1 Phase 2 incorrectly hits deny statement of crypto ACL
CSCvw16165	FPR1k ASA stops passing traffic when a member of the port-channel is down
CSCvw16619	Offloaded UDP traffic not failed over to secondary route in ECMP setup
CSCvw16723	Redirect failure for Chrome Popups when using bookmark for clientless VPN

Caveat ID Number	Description
CSCvw16858	ASA memory usage stays at 100%.
CSCvw16924	WebVPN: Not able to open the WebVPN portal
CSCvw18086	ASA long CPU hogs caused by "Crypto CA" process
CSCvw18614	ASA traceback in the LINA process
CSCvw19324	FP2100 traceback observed in IKE daemon
CSCvw19490	OSPF Database don't reflect RIB changes
CSCvw19686	Enabling Jumbo frames on the ASA 5508 causes low DMA memory issues
CSCvw21386	ASA Traceback and reload on SNMP functions
CSCvw23199	ASA/FTD Traceback and reload in Thread Name: Logger
CSCvw23246	vpn_putuauth: ERR: uxlate collision for ip x.x.x.x user xxxxx on interface outside.
CSCvw24556	FTP File transfer (Big File) not properly closed when Flow offload is enabled
CSCvw26171	ASA Traceback in thread name: DATAPATH
CSCvw26331	ASA traceback and reload on Thread Name: ci/console
CSCvw27301	IKEv2 with EAP, MOBIKE status fails to be processed.
CSCvw28296	H323 Inspection not natting the Media server IP embedded in FacilityOpenLocgicalChannel packet
CSCvw28995	Unable to access SAP portal hyperlinks over webvpn only from the Google Chrome
CSCvw33057	ASA WM 1010: FXOS_PARSER_ERROR: curl return with error code:401 invalid IDs

Resolved Bugs in Version 9.15(1)

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

Caveat ID Number	Description
CSCvq98396	ASA: crypto session handles leak on the standby unit
CSCvr77005	Traffic does not fallback to primary interface from crypto map when interface becomes available
CSCvt48260	Standby unit traceback at fover_parse and boot loop when detecting Active unit
CSCvt92077	Ping Failure on ASAv - 9.13 after CAT9k reboot
CSCvt97205	SNMPPOLL/SNMPTRAP to remote end (site-to-site vpn) ASA interface fails on ASA 9.14.1

Caveat ID Number	Description
CSCvu33992	traceback: ASA reloaded lina_sigcrash+1394
CSCvu89110	ASA: Block new conns even when the "logging permit-hostdown" is set & TCP syslog is down
CSCvv10778	Traceback in threadname DATAPATH (5585) or Lina (2100) after upgrade to 9.12.4
CSCvv25394	After upgrade ASA swapped names for disks, disk0 became disk1 and vice versa.
CSCvv31755	Interface status may be mismatched between application and chassis due to missed update
CSCvv32333	ASA still doesn't allow to poll internal-data0/0 counters via SNMP in multiple mode
CSCvv37629	Malformed SIP packets leads to 4k block hold-up till SIP conn timeout causing probable traffic issue
CSCvv41453	Removing static ipv6 route from management-only route table affects data traffic
CSCvv49698	ASA Anyconnect url-redirect not working for ipv6
CSCvv50338	Traceback Cluster unit on snpi_nat_xlate_destroy+2508
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvv53696	ASA/FTD traceback and reload during AAA or CoA task of Anyconnect user
CSCvv58332	ASA/FTD is reading BGP MP_REACH_NLRI attribute's next-hop bytes in reverse order
CSCvv62305	ASA traceback and reload in fover_parse when attempting to join the failover pair.
CSCvv63412	ASA dropping all traffic with reason "No route to host" when tmatch compilation is ongoing
CSCvv64068	After modify network/service object name. mis-match will occur on hash value of ACL in syslog.
CSCvv66920	Inner flow: U-turn GRE flows trigger incorrect connection flow creation
CSCvv69991	FTD stuck in Maintenance Mode after upgrade to 6.6.1
CSCvv87496	ASA cluster members 2048 block depletion due to "VPN packet redirect on peer"
CSCvv89355	DHCP-Proxy renewal timer is not started after failover

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.