Release Notes for the Cisco ASA Series, 9.13(x)

Release Notes for the Cisco ASA Series, 9.13(x)

This document contains release information for Cisco ASA software Version 9.13(x).

Important Notes

- **No support in ASA 9.13(1) and later for the ASA 5512-X, ASA 5515-X, ASA 5585-X, and the ASASM**—ASA 9.12(x) is the last supported version. For the ASA 5515-X and ASA 5585-X FirePOWER module, the last supported version is 6.4.

  Note: ASDM 7.13(1) and ASDM 7.14(1) also did not support these models; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

- **ASAv requires 2GB memory in 9.13(1) and later**—Beginning with 9.13(1), the minimum memory requirement for the ASAv is 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version. You must adjust the memory size before upgrading. See the ASAv Getting Started Guide for information about the resource allocations (vCPU and memory) supported in version 9.13(1).

- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 that you converted to Platform mode: If you downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13, or you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. (CSCvr19755)

- **Cluster control link MTU change in 9.13(1)**—Starting in 9.13(1), many cluster control packets are larger than they were in previous releases. The recommended MTU for the cluster control link has always been 1600 or greater, and this value is appropriate. However, if you set the MTU to 1600 but then failed to match the MTU on connecting switches (for example, you left the MTU as 1500 on the switch), then you will start seeing the effects of this mismatch with dropped cluster control packets. Be sure to set all devices on the cluster control link to the same MTU, specifically 1600 or higher.

- **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.

- **No support in 9.10(1) and later for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X**—The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1) or later, the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.
- **Beginning with 9.13(1), the ASA establishes an LDAP/SSL connection only if one of the following certification criteria is satisfied**:
  - The LDAP server certificate is trusted (exists in a trustpoint or the ASA trustpool) and is valid.
  - A CA certificate from servers issuing chain is trusted (exists in a trustpoint or the ASA trustpool) and all subordinate CA certificates in the chain are complete and valid.
- **Local CA server is removed in 9.13(1)**—When the ASA is configured as local CA server, it can issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the **crypto ca server** command is removed.
- **Removal of CRL Distribution Point commands**—The static CDP URL configuration commands, namely **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. The CDP URL was moved to match certificate command.

  Note The CDP URL configuration was enhanced to allow multiple instances of the CDP override for a single map (refer CSCvu05216).
- **Removal of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.

  The following subcommands are removed:
  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  Thus, after an upgrade, any revocation-check command that is no longer supported will transition to the new behavior by ignoring the trailing none.

  Note These commands were restored later (refer CSCtb41710).

- **Low-Security Cipher Deprecation**— Several encryption ciphers used by the ASA IKE, IPsec, and SSH modules are considered insecure and have been deprecated. They will be removed in a later release.

  IKEv1: The following subcommands are deprecated:

  - **crypto ikev1 policy** *priority*:
    - **hash md5**
    - **encryption 3des**
    - **encryption des**
    - **group 2**
    - **group 5**

  IKEv2: The following subcommands are deprecated:

  - **crypto ikev2 policy** *priority*
    - **integrity md5**
    - **prf md5**
    - **group 2**
    - **group 5**
    - **group 24**
    - **encryption 3des**
    - **encryption des** (this command is still available when you have the DES encryption license only)
    - **encryption null**

  IPsec: The following commands are deprecated:

  - **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 group5 group24**

  SSH: The following commands are deprecated:

  - **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
  - **ssh key-exchange group dh-group1-sha1**

  SSL: The following commands are deprecated:

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

Crypto Map: The following commands are deprecated:

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **In 9.13(1), Diffie-Hellman Group 14 is now the default** for the **group** command under **crypto ikev1 policy**, **ssl dh-group**, and **crypto ikev2 policy**for IPsec PFS using **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs**, and **crypto map set ikev1 phase1-mode**. The former default Diffie-Hellman group was Group 2.

  When you upgrade from a pre-9.13(1) release, if you need to use the old default (Diffie-Hellman Group 2), then you must *manually* configure the DH group as **group 2** or else your tunnels will default to Group 14. Because group 2 will be removed in a future release, you should move your tunnels to group 14 as soon as possible.

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 9.13(1)

Released: September 25, 2019

Feature	Description
Platform Features	
ASA for the Firepower 1010	We introduced the ASA for the Firepower 1010. This desktop model includes a built-in hardware switch and Power-Over-Ethernet+ (PoE+) support. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **forward interface**, **interface vlan**, **power inline**, **show counters**, **show environment**, **show interface**, **show inventory**, **show power inline**, **show switch mac-address-table**, **show switch vlan**, **switchport**, **switchport access vlan**, **switchport mode**, **switchport trunk allowed vlan**
ASA for the Firepower 1120, 1140, and 1150	We introduced the ASA for the Firepower 1120, 1140, and 1150. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **show counters**, **show environment**, **show interface**, **show inventory**
Firepower 2100 Appliance mode	The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). You can run the Firepower 2100 in the following modes: • Appliance mode (now the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI. • Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firepower Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI. If you are upgrading to 9.13(1), the mode will remain in Platform mode. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **fxos mode appliance**, **show counters**, **show environment**, **show fxos mode**, **show interface**, **show inventory**
DHCP reservation	The ASA DHCP server now supports DHCP reservation. You can assign a static IP address from the defined address pool to a DHCP client based on the client's MAC address. New/Modified commands: **dhcpd reserve-address**
ASAv minimum memory requirement	The minimum memory requirement for the ASAv is now 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version without increasing the memory of your ASAv VM. You can also redeploy a new ASAv VM with version 9.13(1). No modified commands.

Feature	Description
ASAv MSLA Support	The ASAv supports Cisco's Managed Service License Agreement (MSLA) program, which is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA is a new form of Smart Licensing where the licensing Smart Agent keeps track of the usage of licensing entitlements in units of time. New/Modified commands: **license smart**, **mode**, **utility**, **custom-id**, **custom-info**, **privacy**, **transport type**, **transport url**, **transport proxy**
ASAv Flexible Licensing	Flexible Licensing is a new form of Smart Licensing where any ASAv license now can be used on any supported ASAv vCPU/memory configuration. Session limits for AnyConnect and TLS proxy will be determined by the ASAv platform entitlement installed rather than a platform limit tied to a model type. New/Modified commands: **show version**, **show vm**, **show cpu**, **show license features**
ASAv for AWS support for the C5 instance; expanded support for C4, C3, and M4 instances	The ASAv on the AWS Public Cloud now supports the C5 instance (c5.large, c5.xlarge, and c5.2xlarge). In addition, support has been expanded for the C4 instance (c4.2xlarge and c4.4xlarge); C3 instance (c3.2xlarge, c3.4xlarge, and c3.8xlarge); and M4 instance (m4.2xlarge and m4.4xlarge). No modified commands.
ASAv for Microsoft Azure support for more Azure virtual machine sizes	The ASAv on the Microsoft Azure Public Cloud now supports more Linux virtual machine sizes: • Standard_D4, Standard_D4_v2 • Standard_D8_v3 • Standard_DS3, Standard_DS3_v2 • Standard_DS4, Standard_DS4_v2 • Standard_F4, Standard_F4s • Standard_F8, Standard_F8s Earlier releases only supported the Standard_D3 and Standard_D3_v2 sizes. No modified commands.
ASAv enhanced support for DPDK	The ASAv supports enhancements to the Data Plane Development Kit (DPDK) to enable support for multiple NIC queues, which allow multi-core CPUs to concurrently and efficiently service network interfaces. This applies to all ASAv hypervisors except Microsoft Azure and Hyper-V. **Note** DPDK support was introduced in release ASA 9.10(1). No modified commands.

Feature	Description
ASAv support for VMware ESXi 6.7	The ASAv virtual platform supports hosts running on VMware ESXi 6.7. 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 6.7. No modified commands.
Increased VLANs for the ISA 3000	The maximum VLANs for the ISA 3000 with the Security Plus license increased from 25 to 100.
Firewall Features	
Location logging for mobile stations (GTP inspection).	You can configure GTP inspection to log the initial location of a mobile station and subsequent changes to the location. Tracking location changes can help you identify possibly fraudulent roaming charges. New/Modified commands: **location-logging**.
GTPv2 and GTPv1 release 15 support.	The system now supports GTPv2 3GPP 29.274 V15.5.0. For GTPv1, support is up to 3GPP 29.060 V15.2.0. The new support includes recognition of 2 additional messages and 53 information elements. No modified commands.
Mapping Address and Port-Translation (MAP-T)	Mapping Address and Port (MAP) is primarily a feature for use in service provider (SP) networks. The service provider can operate an IPv6-only network, the MAP domain, while supporting IPv4-only subscribers and their need to communicate with IPv4-only sites on the public Internet. MAP is defined in RFC7597, RFC7598, and RFC7599. New/Modified commands: **basic-mapping-rule**, **default-mapping-rule**, **ipv4-prefix**, **ipv6-prefix**, **map-domain**, **share-ratio**, **show map-domain**, **start-port**.
Increased limits for AAA server groups and servers per group.	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the following commands to accept these new limits: **aaa-server**, **aaa-server host**.
TLS proxy deprecated for SCCP (Skinny) inspection.	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was deprecated. The keyword will be removed from the **inspect skinny** command in a future release.
VPN Features	

Feature	Description
HSTS Support for WebVPN as Client	A new CLI mode under WebVPN mode called http-headers was added so that WebVPN could transform HTTP references to HTTPS references for hosts that are HSTS. Configures whether the user agent should allow the embedding of resources when sending this header for WebVPN connections from the ASA to browsers. You can choose to configure the http-headers as: **x-content-type-options**, **x-xss-protection**, **hsts-client** (HSTS support for WebVPN as client), **hsts-server**, or **content-security-policy**. New/Modified commands: **webvpn**, **show webvpn hsts host (name <hostname&s{253}> | all)**and **clear webvpn hsts host (name <hostname&s{253}> | all)**.
Diffie-Hellman groups 15 and 16 added for key exchange	To add support for Diffie-Hellman groups 15 and 16, we modified few **crypto** commands to accept these new limits. **crypto ikev2 policy <index> group <number>** and **crypto map <map-name> <map-index> set pfs <group>.**
show asp table vpn-context enhancement to output	To enhance debug capability, these vpn context counters were added to the output: Lock Err, No SA, IP Ver Err, and Tun Down. New/Modified commands: **show asp table vpn-context** (output only).
Immediate session establishment when the maximum remote access VPN session limit is reached.	When a user reaches the maximum session (login) limit, the system deletes the user's oldest session and waits for the deletion to complete before establishing the new session. This can prevent the user from successfully connecting on the first attempt. You can remove this delay and have the system establish the new connection without waiting for the deletion to complete. New/Modified commands: **vpn-simultaneous-login-delete-no-delay**.
High Availability and Scalability Features	
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	If you enable Dead Connection Detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. New/Modified commands: **show conn** (output only).
Monitor the traffic load for a cluster	You can now monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default. New/Modified commands: **debug cluster load-monitor**, **load-monitor**, **show cluster info load-monitor**

Feature	Description
Accelerated cluster joining	When a data unit has the same configuration as the control unit, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each unit, and is not replicated from the control unit to the data unit. **Note** Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the unit, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** to view incompatible configuration. New/Modified commands: **unit join-acceleration**, **show cluster info unit-join-acceleration incompatible-config**
Routing Features	
SMTP configuration enhancement	You can optionally configure the SMTP server with primary and backup interface names to enable ASA for identifying the routing table to be used for logging—management routing table or data routing table. If no interface is provided, ASA would refer to management routing table lookup, and if no proper route entry is present, it would look at the data routing table. New/Modified commands: **smtp-server [primary-interface][backup-interface]**
Support to set NSF wait timer	OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known whether all neighbors are listed in the packet, and the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **timers nsf wait**
Support to set tftp blocksize	The typical blocksize fixed for tftp file transfer is 512-octets. A new command, **tftp blocksize**, is introduced to configure a larger blocksize and thereby enhance the tftp file transfer speed. You can set a blocksize varying from 513 to 8192 octets. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **tftp blocksize**
Certificate Features	
Support to view FIPS status	The **show running-configuration fips** command displayed the FIPS status only when fips was enabled. In order to know the operational state, the **show fips** command was introduced where, it displays the fips status when an user enables or disables fips that is in disabled or enabled state. This command also displays the status for rebooting the device after an enable or disable action. New/Modified commands: **show fips**

Feature	Description
CRL cache size increased	To prevent failure of large CRL downloads, the cache size was increased, and the limit on the number of entries in an individual CRL was removed. • Increased the total CRL cache size to 16 MB per context for multi-context mode. • Increased the total CRL cache size to 128 MB for single-context mode.
Modifications to the CRL Distribution Point commands	The static CDP URL configuration commands are removed and moved to the match certificate command. New/Modified commands: **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. **match-certificate override-cdp** was introduced. The static CDP URL was re-introduced in 9.13(1)12 to the match certificate command.
Administrative and Troubleshooting Features	
Management access when the Firepower 1000, Firepower 2100 Appliance mode is in licensing evaluation mode	The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager. **Note** If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature. No modified commands.
Additional NTP authentication algorithms	Formerly, only MD5 was supported for NTP authentication. The ASA now supports the following algorithms: • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC New/Modified commands: **ntp authentication-key**
ASA Security Service Exchange (SSE) Telemetry Support for the Firepower 4100/9300	With Cisco Success Network enabled in your network, device usage information and statistics are provided to Cisco which is used to optimize technical support. The telemetry data that is collected on your ASA devices includes CPU, memory, disk, or bandwidth usage, license usage, configured feature list, cluster/failover information and the like. New/Modified commands: **service telemetry**and **show telemetry**

Feature	Description
SSH encryption ciphers are now listed in order from highest to lowest security for pre-defined lists	SSH encryption ciphers are now listed in order from highest security to lowest security for pre-defined lists (such as medium or high). In earlier releases, they were listed from lowest to highest, which meant that a low security cipher would be proposed before a high security cipher. New/Modified commands: **ssh cipher encryption**
show tech-support includes additional output	The output of **show tech-support** is enhanced to display the output of the following: **show flow-offload info detail** **show flow-offload statistics** **show asp table socket** New/Modified commands: **show tech-support** (output only).
Enhancement to **show-capture asp_drop** output to include drop location information	While troubleshooting using ASP drop counters, the exact location of the drop is unknown, especially when the same ASP drop reason is used in many different places. This information is critical in finding root cause of the drop. With this enhancement, the ASP drop details such as the build target, ASA release number, hardware model, and ASLR memory text region (to facilitate the decode of drop location) are shown. New/Modified commands: **show-capture asp_drop**
Modifications to **debug crypto ca**	The **debug crypto ca transactions** and **debug crypto ca messages** options are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels are reduced to 14. New/Modified commands: **debug crypto ca**
FXOS Features for the Firepower 1000 and 2100	
Secure Erase	The secure erase feature erases all data on the SSDs so that data cannot be recovered even by using special tools on the SSD itself. You should perform a secure erase in FXOS when decomissioning the device. New/Modified FXOS commands: **erase secure** (local-mgmt) Supported models: Firepower 1000 and 2100
Configurable HTTPS protocol	You can set the SSL/TLS versions for FXOS HTTPS acccess. New/Modified FXOS commands: **set https access-protocols** Supported models: Firepower 2100 in Platform Mode

Feature	Description
FQDN enforcement for IPSec and Keyrings	For FXOS, you can configure FQDN enforcement so that the FDQN of the peer needs to match the DNS Name in the X.509 Certificate presented by the peer. For IPSec, enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections. For keyrings, all hostnames must be FQDNs, and cannot use wild cards. New/Modified FXOS commands: **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id** Removed commands: **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6** Supported models: Firepower 2100 in Platform Mode
New IPSec ciphers and algorithms	We added the following IKE and ESP ciphers and algorithms to configure an IPSec tunnel to encrypt FXOS management traffic: • Ciphers—aes192. Existing ciphers include: aes128, aes256, aes128gcm16. • Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include: prfsha1. • Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms incldue: sha1. • Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Existing groups include: modp2048. No modified FXOS commands. Supported models: Firepower 2100 in Platform Mode
SSH authentication enhancements	We added the following SSH server encryption algoritghms for FXOS: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com We added the following SSH server key exchange methods for FXOS: • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 New/Modified FXOS commands: **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm** Supported models: Firepower 2100 in Platform Mode

Feature	Description
EDCS keys for X.509 Certificates	You can now use EDCS keys for FXOS certificates. Formerly, only RSA keys were supported. New/Modified FXOS commands: **set elliptic-curve**, **set keypair-type** Supported models: Firepower 2100 in Platform Mode
User password improvements	We added FXOS password security improvements, including the following: • User passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. • Removed the **set change-during-interval** command, and added a **disabled** option for the **set change-interval**, **set no-change-interval**, and **set history-count** commands. New/Modified FXOS commands: **set change-during-interval**, **set expiration-grace-period**, **set expiration-warning-period**, **set history-count**, **set no-change-interval**, **set password**, **set password-expiration**, **set password-reuse-interval** Supported models: Firepower 2100 in Platform Mode

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
9.12(x)	—	Any of the following: → 9.13(x)
9.10(x)	—	Any of the following: → 9.13(x) → **9.12(x)**
9.9(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x)
9.8(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x)
9.7(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

Current Version	Interim Upgrade Version	Target Version
9.6(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.5(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.3(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Current Version	Interim Upgrade Version	Target Version
9.2(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(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: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(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: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(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 9.13(x)

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

Caveat ID Number	Description
CSCvp95110	Platform and package versions are not getting updated after ASA upgrade in APP-Mode
CSCvq02977	KP Copy image performance is very low via HTTPS
CSCvq15125	SSP FXOS/ASA: ipsec connection not up b/w mio and ASA gateway
CSCvq54299	After restart of Active and standby units, only 4 context were created instead 40 configured
CSCvq61523	FP1000: AnyConnect-Parent SSL-Tunnel continuously reconnecting
CSCvq73464	ipv6 address of asa where ip-client is enabled is not showing in snmptrap logs

Caveat ID Number	Description
CSCvr02080	CPU Hogs observed in CERT API process while decoding the CRL with large number of entries in it
CSCvr19755	FP2100 ASA: Getting Timed out error while creating Portchannel and edit Interfaces
CSCvr19922	Cluster: BGP route may go in out of sync in some scenarios
CSCvr21119	Add power cycle msg when SSD Secure erase cmd is issued on FP1000 units
CSCvr22260	lina reload in IkeAddFailEntry at ike_mib.c:578 under general stress
CSCvr23986	Asserts being triggered in LINA in mh_magic_verify and in SrDoMgmt under load
CSCvr29769	segfault and reload in malloc_show_bin_info_pool running eem
CSCvr44123	Unable to login via chassis Manager or Rest api in FPR2100 if session timeout is non-deafult

Resolved Bugs in Version 9.13(1)

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

Caveat ID Number	Description
CSCvi07901	CISCO-REMOTE-ACCESS-MONITOR-MIB crasIPSecNumSessions is zero on ASA for IKEv2 AnyConnect
CSCvj99658	ASA/Lina HA failover interface testing rendering control channel unresponsive
CSCvn16864	ENH: Missing Content-Security-Policy Header in ASA HTTP WebVPN portal
CSCvo05052	Fluctuating delay for ICMP packets going through Snort engine inspection on vFTD
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvp09083	ASA does not respond to DHCP request packet on BVI interface
CSCvp23530	OSPF neighbor command not replicated to standy after write standby or reload
CSCvp38774	WebVPN rewriter not loading website correctly
CSCvp42484	IS-IS hello packet length not updated to correct mtu when mtu modified
CSCvp71766	Radius authentication fails when sourced from BVI across a VPN tunnel
CSCvp73394	Failover ASA IKEv2 VTI: Secondary ASA sends standby IP as the traffic selector
CSCvp75965	primary FPR2110 crash after customer configure syslog setting on FMC
CSCvp78171	ASA in cluster fail to synchronise IPv6 ND table with peer units.
CSCvp91905	ASA will add the newly configured IPv6 Address to the current link-local address

Caveat ID Number	Description
CSCvq00560	ASA silently drops packets which violate ESP Authentication data field size (ICV)
CSCvq10239	With SSL HW acceleration enabled, FTD TCP Proxy tears down the connection after 3 retransmissions
CSCvq10500	captures of both CLISH and LINA doesn't work with IPv6 address
CSCvq15976	ASA Memory Leak - snp_svc_insert_dtls_session
CSCvq17551	Syslog 711004 not consistently triggering event manager event
CSCvq22358	Disabling anti-replay for one context it disables it for other contexts as well
CSCvq24494	FP2100 - Flow oversubscribing ring/CPU core causing disruption to working flows on FP2100 platforms
CSCvq46737	Deployment fails to FTD device with L4 service port in NAT policy configuration
CSCvq57591	When only IP communication is disrupted on failover link LANTEST msg is not sent on data interfaces
CSCvq73595	ASA webvpn unable to extract username from cert UPN if username is longer than 32 chars
CSCvq76706	Ability to clear message logged statistics in output of "show logging"
CSCvq84444	Configuring static routes causes "Route Session" rerr counter to increment on standby ASA

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.

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.