Release Notes for the Cisco ASA Series, Version 9.2(x)

First Published: April 24, 2014
Last Updated: March 30, 2017

This document contains release information for Cisco ASA software Version 9.2(x). This document includes the following sections:

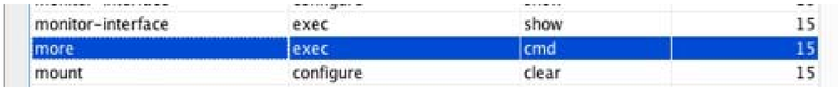
Important Notes

- Potential Traffic Outage (9.2(4.15) through 9.2(4.19))--Due to bug CSCvd78303, the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reload the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice FN-64291 for affected versions and more information.
- ASA 5505 with 256 MB DRAM—Starting in Version 8.3, the DRAM requirements for the ASA 5505 were increased to 512 MB. If you did not use the Unlimited Hosts license or the Security Plus license with failover enabled, then the ASA could continue to operate with 256 MB. As of Version 9.2 and later, all ASA 5505 licenses require 512 MB. If you only have 256 MB, the ASA image may not load into memory. See Cisco ASA Compatibility for memory requirements and upgrade information.
- Upgrade impact for ASDM login when upgrading from a pre-9.2(2.4) release to 9.2(2.4) or later—If you upgrade from a pre-9.2(2.4) release to ASA Version 9.2(2.4) or later and you use command authorization and ASDM-defined user roles, users with Read Only access will not be able to log in to ASDM. You must change the **more** command either before or after you upgrade to be at privilege level 5; only Admin level users can make this change. Note that ASDM version 7.3(2) and later includes the **more** command at level 5 for defined user roles, but preexisting configurations need to be fixed manually.

  ASDM:

  a. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authorization**, and click **Configure Command Privileges**.

  b. Select **more**, and click **Edit**.



monitor-interface	exec	show	15
more	exec	cmd	15
mount	configure	clear	15

c. Change the **Privilege Level** to 5, and click **OK**.

d. Click **OK**, and then **Apply**.

CLI:

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

- Windows NT AAA server to be deprecated—In ASA Version 9.3, the Windows NT AAA server will no longer be supported. If you use WinNT, you should start planning alternative server types.
- ASA CX module upgrade requirements—For ASA Version 9.2(3) and later, only ASA CX Version 9.3.2.1 and later is supported. When upgrading your ASA, first upgrade the ASA CX software; otherwise the ASA CX module will become unresponsive.
- Downgrade from 9.2(1) or later to 9.1 or earlier with clustering—Zero Downtime Downgrade is not supported.

System Requirements

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

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

New Features

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

New Features in Version 9.2(4)

Released: July 16, 2015

The following table lists the new features for ASA Version 9.2(4).

Table 1 New Features for ASA Version 9.2(4)

Feature	Description
Platform Features	
Show invalid usernames in syslog messages	You can now show invalid usernames in syslog messages for unsuccessful login attempts. The default setting is to hide usernames when the username is invalid or if the validity is unknown. If a user accidentally types a password instead of a username, for example, then it is more secure to hide the "username" in the resultant syslog message. You might want to show invalid usernames to help with troubleshooting login issues. We introduced the following command: **no logging hide username**
DHCP features	
DHCP Relay server validates the DHCP Server Identifier for replies	If the ASA DHCP relay server receives a reply from an incorrect DHCP server, it now verifies that the reply is from the correct server before acting on the reply.
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. *Also available in 8.4(5) and 9.1(5).*

New Features in Version 9.2(3)

Released: December 15, 2014

Table 2 lists the new features for ASA Version 9.2(3).

Table 2 New Features for ASA Version 9.2(3)

Feature	Description
Remote Access Features	
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript. Note Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office applications) • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications We introduced the following command: **http-only-cookie**

New Features in Version 9.2(2.4)

Released: August 12, 2014

Table 3 lists the new features for ASA Version 9.2(2.4).

Note: Version 9.2(2) was removed from Cisco.com due to build issues; please upgrade to Version 9.2(2.4) or later.

Table 3 New Features for ASA Version 9.2(2.4)

Feature	Description
Platform Features	
ASA 5585-X (all models) support for the matching ASA FirePOWER SSP hardware module. ASA 5512-X through ASA 5555-X support for the ASA FirePOWER software module.	The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).You can use the module in single or multiple context mode, and in routed or transparent mode. We introduced or modified the following commands: **capture interface asa_dataplane**, **debug sfr**, **hw-module module 1 reload**, **hw-module module 1 reset**, **hw-module module 1 shutdown**, **session do setup host ip, session do get-config, session do password-reset, session sfr, sfr, show asp table classify domain sfr**, **show capture**, **show conn**, **show module sfr**, **show service-policy, sw-module sfr**.
Remote Access Features	
Internet Explorer 11 browser support on Windows 8.1 and Windows 7 for clientless SSL VPN	We added support for Internet Explorer 11 with Windows 7 and Windows 8.1 for clientless SSL VPN.. We did not modify any commands.

New Features in Version 9.2(1)

Released: April 24, 2014

Table 4 lists the new features for ASA Version 9.2(1).

Note: The ASA 5510, ASA 5520, ASA 5540, ASA 5550, and ASA 5580 are not supported in this release or later. ASA Version 9.1 was the final release for these models.

Table 4 New Features for ASA Version 9.2(1)

Feature	Description
Platform Features	
The Cisco Adaptive Security Virtual Appliance (ASAv) has been added as a new platform to the ASA series.	The ASAv brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments. The ASAv runs on VMware vSphere. You can manage and monitor the ASAv using ASDM or the CLI.
Routing Features	

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
BGP Support	We now support the Border Gateway Protocol (BGP). BGP is an inter autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). We introduced the following commands**: router bgp, bgp maxas-limit, bgp log-neighbor-changes, bgp transport path-mtu-discovery, bgp fast-external-fallover, bgp enforce-first-as, bgp asnotation dot, timers bgp, bgp default local-preference, bgp always-compare-med, bgp bestpath compare-routerid, bgp deterministic-med, bgp bestpath med missing-as-worst, policy-list, match as-path, match community, match metric, match tag, as-path access-list, community-list, address-family ipv4, bgp router-id, distance bgp, table-map, bgp suppress-inactive, bgp redistribute-internal, bgp scan-time, bgp nexthop, aggregate-address, neighbor, bgp inject-map, show bgp, show bgp cidr-only, show bgp all community, show bgp all neighbors, show bgp community, show bgp community-list, show bgp filter-list, show bgp injected-paths, show bgp ipv4 unicast, show bgp neighbors, show bgp paths, show bgp pending-prefixes, show bgp prefix-list, show bgp regexp, show bgp replication, show bgp rib-failure, show bgp route-map, show bgp summary, show bgp system-config, show bgp update-group, clear route network, maximum-path, network.** We modified the following commands: **show route**, **show route summary**, **show running-config router**, **clear config router**, **clear route all**, **timers lsa arrival**, **timers pacing**, **timers throttle**, **redistribute bgp**.
Static route for Null0 interface	Sending traffic to a Null0 interface results in dropping the packets destined to the specified network. This feature is useful in configuring Remotely Triggered Black Hole (RTBH) for BGP. We modified the following command: **route**.
OSPF support for Fast Hellos	OSPF supports the Fast Hello Packets feature, resulting in a configuration that results in faster convergence in an OSPF network. We modified the following command: **ospf dead-interval**
New OSPF Timers	New OSPF timers were added; old ones were deprecated. We introduced the following commands: **timers lsa arrival**, **timers pacing**, **timers throttle.** We removed the following commands: **timers spf**, **timers lsa-grouping-pacing**
OSPF Route filtering using ACL	Route filtering using ACL is now supported. We introduced the following command: **distribute-list**

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
OSPF Monitoring enhancements	Additional OSPF monitoring information was added. We modified the following commands: **show ospf events**, **show ospf rib**, **show ospf statistics**, **show ospf border-routers [detail]**, **show ospf interface brief**
OSPF redistribute BGP	OSPF redistribution feature was added. We added the following command: **redistribute bgp**
EIGRP Auto- Summary	For EIGRP, the Auto-Summary field is now disabled by default.
High Availability Features	
Support for cluster members at different geographical locations (inter-site) for transparent mode	You can now place cluster members at different geographical locations when using Spanned EtherChannel mode in transparent firewall mode. Inter-site clustering with spanned EtherChannels in routed firewall mode is not supported. We did not modify any commands.
Static LACP port priority support for clustering	Some switches do not support dynamic port priority with LACP (active and standby links). You can now disable dynamic port priority to provide better compatibility with spanned EtherChannels. You should also follow these guidelines: - Network elements on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped. - Port-channel bundling downtime should not exceed the configured keepalive interval. We introduced the following command: **clacp static-port-priority**.

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
Support for 32 active links in a spanned EtherChannel for clustering	ASA EtherChannels now support up to 16 active links. With *spanned* EtherChannels, that functionality is extended to support up to 32 active links across the cluster when used with two switches in a vPC and when you disable dynamic port priority. The switches must support EtherChannels with 16 active links, for example, the Cisco Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module. For switches in a VSS or vPC that support 8 active links, you can now configure 16 active links in the spanned EtherChannel (8 connected to each switch). Previously, the spanned EtherChannel only supported 8 active links and 8 standby links, even for use with a VSS/vPC. Note If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links. We introduced the following command: **clacp static-port-priority**.
Support for 16 cluster members for the ASA 5585-X	The ASA 5585-X now supports 16-unit clusters. We did not modify any commands.
Support for clustering with the Cisco Nexus 9300	The ASA supports clustering when connected to the Cisco Nexus 9300.
Remote Access Features	
ISE Change of Authorization	The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA. When an end user requests a VPN connection the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA "policy push." This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates. We introduced the following commands: **dynamic-authorization, authorize-only**, **debug radius dynamic-authorization**. We modified the following commands: **without-csd** [**anyconnect**], **interim-accounting-update** [**periodic** [*interval*]]. We removed the following commands: **nac-policy**, **eou**, **nac-settings**.

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
Improved clientless rewriter HTTP 1.1 compression handling	The rewriter has been changed so that if the client supports compressed content and the content will not be rewritten, then it will accept compressed content from the server. If the content must be rewritten and it is identified as being compressed, it will be decompressed, rewritten, and if the client supports it, recompressed. We did not introduce or modify any commands.
OpenSSL upgrade	The version of OpenSSL on the ASA will be updated to version 1.0.1e. Note We disabled the heartbeat option, so the ASA is not vulnerable to the Heartbleed Bug. We did not introduce or modify any commands.
Interface Features	
Support for 16 active links in an EtherChannel	You can now configure up to 16 active links in an EtherChannel. Previously, you could have 8 active links and 8 standby links. Be sure your switch can support 16 active links (for example the Cisco Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module). Note If you upgrade from an earlier ASA version, the maximum active interfaces is set to 8 for compatibility purposes (the **lacp max-bundle** command). We modified the following commands: **lacp max-bundle** and **port-channel min-bundle**.
Maximum MTU is now 9198 bytes	The maximum MTU that the ASA can use is 9198 bytes (check for your model’s exact limit at the CLI help). This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems. If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value. We modified the following command: **mtu** *Also in Version 9.1(6).*
Monitoring Features	

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
Embedded Event Manager (EEM)	The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. The EEM responds to events in the EEM system by performing actions. There are two components: events that the EEM triggers, and event manager applets that define actions. You may add multiple events to each event manager applet, which triggers it to invoke the actions that have been configured on it. We introduced or modified the following commands: **event manager applet**, **description**, **event syslog id**, **event none**, **event timer**, **event crashinfo**, **action cli command**, **output**, **show running-config event manager**, **event manager run**, **show event manager**, **show counters protocol eem**, **clear configure event manager**, **debug event manager**, **debug menu eem**.
SNMP hosts, host groups, and user lists	You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We introduced or modified the following commands: **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
SNMP message size	The limit on the message size that SNMP sends has been increased to 1472 bytes.
SNMP OIDs and MIBs	The ASA now supports the cpmCPUTotal5minRev OID. The ASAv has been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID. The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASAv platform.

Table 4 New Features for ASA Version 9.2(1) (continued)

Feature	Description
Administrative Features	
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The **auto-enable** option was added to the **aaa authorization exec** command. We modified the following command: **aaa authorization exec**.
Auto Update Server certificate verification enabled by default	The Auto Update Server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning: `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` The configuration will be migrated to explicitly configure no verification: **auto-update server no-verification** We modified the following command: **auto-update server** [**verify-certificate** | **no-verification**].

Upgrading the Software

See the following table for the upgrade path for your version. Some versions require an interim upgrade before you can upgrade to the latest version.

Note: There are no special requirements for Zero Downtime Upgrades for failover and ASA clustering with the following exceptions:

- Upgrading ASA clustering from 9.0(1) or 9.1(1)—Due to CSCue72961, hitless upgrading is not supported.
- Upgrade issues with 8.4(6), 9.0(2), and 9.1(2) for failover—Due to CSCug88962, you cannot perform a Zero Downtime Upgrade to 8.4(6), 9.0(2), or 9.1(3). You should instead upgrade to 8.4(5) or 9.0(3) or later. To upgrade 9.1(1), you cannot upgrade directly to the 9.1(3) release due to CSCuh25271, so there is no workaround for a Zero Downtime Upgrade; you must upgrade to 9.1(2) before you upgrade to 9.1(3) or later.

Current ASA Version	First Upgrade to:	Then Upgrade to:
8.2(x) and earlier	8.4(5)	9.2(1) or later
8.3(x)	8.4(5)	9.2(1) or later
8.4(1) through 8.4(4)	8.4(5) or 9.0(4)	9.2(1) or later
8.4(5) and later	—	9.2(1) or later

Current ASA Version	First Upgrade to:	Then Upgrade to:
8.5(1)	9.0(4)	9.2(1) or later
8.6(1)	9.0(4)	9.2(1) or later
9.0(1)	9.0(4)	9.2(1) or later
9.0(2) or later	—	9.2(1) or later
9.1(1)	9.1(2)	9.2(1) or later
9.1(2) or later	—	9.2(1) or later

For detailed steps about upgrading, see the 9.2 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.

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

Open Bugs

All open bugs severity 3 and higher for Version 9.2 are included in the following search:

9.2 open bug search

Resolved Bugs

Resolved Bugs in Version 9.2(4)

All resolved bugs are included in the following search:

- 9.2(4) Fixed bug search.

Resolved Bugs in Version 9.2(3)

Table 5 contains resolved bugs in ASA Version 9.2(3).

If you are a registered Cisco.com user, view more information about each bug using Bug Search at the following website:

https://bst.cloudapps.cisco.com/bugsearch/

Table 5 Resolved Bugs in ASA Version 9.2(3)

Bug	Description
CSCtt88306	Syslog 106100 not generated on second context when cascading contexts.
CSCtu24956	ASDM: ASDM_Handler getting wrong data for ISAKMP_SA
CSCty17881	vpn-sessiondb detail missing Filter Name after IKEv1 rekey
CSCub53088	Arsenal:twice NAT with service type ftp not working.
CSCuf31654	Linux Kernel GUID Partition Tables Handling Arbitrary Code Execution V
CSCug51375	ASA SSL: Continues to accept SSLv3 during TLSv1 only mode
CSCui27525	Idle timer and half-closed idle timer reset by out of sequence SYN
CSCul04263	ASA Webvpn CIFS vnode_create: VNODE ALLOCATION LIMIT 100000 REACHED!
CSCum91201	SSH timeout on ASA
CSCun23552	JavaScript parser error: StoreFront 2.1 login fails; ActiveX broken;
CSCun64754	ASA may traceback when "write standby" command is entered twice
CSCun66613	ASA stops decrypting certain L2L traffic after working for some time
CSCuo09383	ASA WebVPN Memory leak leading to Blank Portal Page/AnyConnect failure
CSCuo11778	ENH: Add "speed nonegotiate" command for fiber interfaces on ASA5585
CSCuo45321	ASA allows IKEv1 clients to bypass address assignment, causing conflict
CSCuo68855	BGP:router bgp missing in system context if admin is in transparent mode
CSCup16419	Traceback in Thread Name: ssh_init
CSCup28968	When ACL optimization is enabled, wrong rules get deleted
CSCup35713	ASA tmatch_summary_alloc block leak in binsize 1024
CSCup36514	webvpn jscript post to wrong URL - ASA FQDN same as server FQDN
CSCup43257	ASA Traceback in Thread name: ci/console while modifying an object-group
CSCup46524	"no speed nonegotiate" command in ASA 5580 running 9.1.5 in show run
CSCup47195	ASA - Traceback in DATAPATH-0-1275
CSCup50857	ASA traceback in thread name idfw_adagent
CSCup54184	Cisco ASA SharePoint RAMFS Integrity and Lua Injection Vulnerability
CSCup55377	ASA: Traceback Page Fault in vpnfol_thread_msg on Standby ASA
CSCup59017	ASA with ACL optimization crashing in "fover_parse" thread
CSCup59499	ASA: BGP not performing outbound route-filtering
CSCup60837	Personal bookmarks get deleted with ASA in Active/Standby failover
CSCup66273	ASA SSLVPN Citrix Java client error - java.lang.ClassNotFoundException
CSCup70157	ASA configured with BGP drop packets with reason unexpected packet
CSCup70720	ASA crashes with Page Fault with multiple configuration sessions
CSCup74532	ASA failover standby device reboots due to delays in config replication
CSCup85529	ASA Smart Call does not hide IPv6 addresses for ND
CSCup86857	IPv4 ACLs not working after merging IPv4 and IPv6 ACLs by upgrading
CSCup86960	ASA : Failover descriptor does not change after reconfiguring VLAN
CSCup87430	accounting not per rfc in dual factor auth case
CSCup90173	SNMP: Power supply OIDs missing if no power input on 5500-X

Table 5 Resolved Bugs in ASA Version 9.2(3) (continued)

Bug	Description
CSCup92782	ASA providing inaccurate Tunnel count to ASDM
CSCuq03216	IPsecOverNatT tunnel disappears after ASA failovers
CSCuq04306	Smart Tunnels Spawn " UNKNOWN Publisher" Warning w/Java 7 Update 60
CSCuq05768	Using " ?" to list files in directory with thousands of files causing hog
CSCuq08854	Show memory app-cache command shows incorrect bytes if more than 2^32
CSCuq09352	vbscript getting caught in loop when passing thru ASA WebVPN Rewriter
CSCuq09709	Using ASA 9.2.1, Anyconnect weblaunch fails with URL-list in DAP
CSCuq20396	Traceback when executing " show crypto accelerator load-balance"
CSCuq21016	Local pool address not released -> Duplicate local pool address found
CSCuq24404	traceback in thread name: netfs_thread_init
CSCuq25488	WebVPN HTML Style " Overflow:Hidden" Breaks Custom Logon Pages
CSCuq26046	ASA - Traceback in thread name SSH while changing NAT configuration
CSCuq26812	ASDM Certificate validation failure
CSCuq28978	WebVPN: Rewriter issue with PATHIX Inspection Database
CSCuq33451	ASA: Increased processor temperature after upgrade
CSCuq34213	Double Free when processing DTLS packets
CSCuq34226	OpenSSL Zero-Length Fragments DTLS Memory Leak Denial of Service Vuln
CSCuq35090	Webvpn: Support for XFRAME in additional portal and CSD pages
CSCuq36615	Traceback caused by WCCP
CSCuq37448	Cisco ASA Failover IPSEC does not encrypt failover link
CSCuq37873	ASA : timeout floating-conn not working when PPPoE is configured
CSCuq38805	ASA 9.2 : Static Null route not redistributed over EIGRP to neighbors
CSCuq38807	ASA Radius Access-Request contains both User-Password and CHAP-Password
CSCuq39511	ASA: EIGRP neighbor relationship flapping
CSCuq42475	IPv6 tunneled route on link-local interfaces
CSCuq46931	LDAP CLI: Quotes removed if ldap attribute-map name has spaces
CSCuq53421	ASA can use wrong trustpoint with rekeyed CAs are cfg in trustpoints.
CSCuq54553	with Anyconnect deflate compression ASA gives ASA-3-722021 syslog
CSCuq57188	ASA returns wrong content-length for cut-thru proxy authentication page
CSCuq59667	ASA tracebacks in Thread Name: ssh due to watchdog
CSCuq60566	Incorrect content-length when maddr present with URI in SIP message body
CSCuq62164	IPv6 stateless autoconfiguration fails if managed config flag in RA
CSCuq65542	Cisco ASA Software Version Information Disclosure Vulnerability
CSCuq66078	Traceback in clacp_enforce_load_balance with ASA Clustering
CSCuq68271	ASA Cluster slave unit loses default route due to sla monitor
CSCuq68888	Cisco ASA SSL VPN Memory Blocks Exhaustion Vulnerability
CSCuq72664	ASA - 80 Byte memory block depletion
CSCuq75981	ASA traceback in DATAPATH-0-2078 thread

Table 5 Resolved Bugs in ASA Version 9.2(3) (continued)

Bug	Description
CSCuq76847	ASA:Page fault traceback ACL FQDN Object-group
CSCuq77228	ASA Cluster: IDFW traceback inThread Name: DATAPATH-3-132
CSCuq80639	ASA5580 speed nonegotiate settings kept link down after shut/no shut
CSCur07061	Traceback on standby ASA during hitless upgrade
CSCur16793	xlate per-session commands are not synchronized
CSCur17329	SDI authentication doesn't work in more than one contexts.
CSCur23709	ASA : evaluation of SSLv3 POODLE vulnerability
CSCur24059	Control Plane ACL Not Working for Redirected HTTP Traffic
CSCur27845	ASA Client login timeout issue due to proxy match inconsistency
CSCur36898	EIGRP tag incorrectly send by ASA
CSCur42907	Failed to allocate global ID when adding service-policy
CSCur47804	ASA Crash in vpnfol_thread_msg thread
CSCur52712	Webvpn: Support for XFRAME for non-critical URL's
CSCur54570	ASA accounting request does not contain radius-class(25) attribute
CSCur55388	Usernames obscured with asterisks in logs after upgrade to ASA 9.1(5.16)
CSCur59397	ASA SCP Client does not prompt for password when not inc. in copy string
CSCur59704	ASA: Traceback in idfw_proc
CSCur64589	DATAPATH Traceback in snp_mp_svc_udp_upstream_data function
CSCur64659	ASA Traceback in Thread Name: DATAPATH-6-2544
CSCur66635	ASA Traceback in Thread Name: DATAPATH-3-1274
CSCur71254	ASA crash loop while upgrading when FIPS enabled
CSCur77736	ASA : 256 Byte Block Depletion with CoA enabled

Resolved Bugs in Version 9.2(2.4)

Table 6 contains resolved bugs in ASA Version 9.2(2.4).

If you are a registered Cisco.com user, view more information about each bug using Bug Search at the following website:

https://bst.cloudapps.cisco.com/bugsearch/

Table 6 Resolved Bugs in ASA Version 9.2(2.4)

Bug	Description
CSCsz39633	Double auth not triggered if using secondary-aaa-server per interface
CSCtz53586	ASA: Crash when out of stack memory with call-home configured
CSCub05888	Asa 5580-20: object-group-search access-control causes failover problem
CSCuc80975	ASA5500-x: "speed nonegotiate" command not available for fiber interface
CSCue87407	DNS: Inspection drops non in-addr.arpa PTR queries
CSCug14102	Need Syslog containing assigned IP address for AnyConnect IKEv2
CSCuh79288	ASA 9.1.2 DHCP - Wireless Apple devices are not getting an IP via DHCPD

Table 6 Resolved Bugs in ASA Version 9.2(2.4) (continued)

Bug	Description
CSCuh84378	ASA: Last packet in PCAP capture file not readable
CSCul22575	ASA 8.4.6 MAC Address flapping with Port-Channels and IPv6
CSCul33381	ASA 5505 SIP packets may have extra padding one egress of 5505
CSCul46971	ASA Transparent mode doesn't pass DHCP discover message
CSCul68338	WEBVPN IE 11: CIFS bookmarks showing with unicode
CSCum00360	ASA - DHCP Discover Sent out during boot process
CSCum75214	ASA5585-SSP60 Teardown process is delayed under heavy traffic condition
CSCum76734	ASA Backup scansafe tower is never polled
CSCum80899	ASA: Watchdog traceback in Unicorn Admin Handler with TopN host stats
CSCum85047	Traceback in Thread: IPsec message handler with rip-tlog_event_allocate
CSCum86538	SunRPC GETPORT Reply dropped when two active sessions use same xid
CSCum92080	Sourcefire Defense Center not able to be rendered via Clientless SSL VPN
CSCun12838	ASA Traceback in DATAPATH-1-1400 with error message shrlock_join_domain
CSCun15560	ASA-IC-6GE-SFP-C SFP port doesn't come up
CSCun25809	AnyConnect Password Management Fails with SMS Passcode
CSCun28999	When long line is entered on cli, all chars > 510 silentl y discarded
CSCun40620	ASA IPSec - DNS reply for RA client dropped when LZS compression enabled
CSCun41817	Hash calculated for multiple ACEs on ASA are same
CSCun41818	ASA: Traceback in thread Name: DATAPATH-1-2581
CSCun43082	ASA Tears Down Connections With Reason of 'snp_drop_none'
CSCun44541	ASA cut a part of credential data during cut-thru proxy authentication
CSCun45520	Cisco ASA DHCPv6 Denial of Service Vulnerability
CSCun59095	ASDM interface graph showing bogus values in S/W and H/W output queue
CSCun66306	IDM/IME/File Transfer Slow For Certain Source and Destination IP Pairs
CSCun69669	Posture assement failing after HS upgrade to 3.1.05152
CSCun78551	Cisco ASA Information Disclosure Vulnerability
CSCun81982	Packet-tracer showing incorrect result for certain NAT configurations
CSCun83186	Nameif command not allowed on TFW multimode ASA with clustering
CSCun85465	'ASA modifies Request Host Part under 'ACK' packet for SIP connection'
CSCun86984	ASA 5505 u-turned/hairpinned conn counts toward license local-host limit
CSCun88276	High CPU with IKE daemon Process
CSCun95075	ASA drops packet due to nat-no-xlate-to-pat-pool after removing NAT rule
CSCun96170	ASA 8.4.6: Traceback with fover_FSM_thread
CSCuo00627	Saleen copper module port speed/duplex changes ineffective
CSCuo02948	To the box traffic dropped due to vpn load-balancing (mis)configuration
CSCuo03555	SNMP: cpmCPUTotal5sec/1min/5min return " 0"
CSCuo03569	VPN client firewall and split-tunneling mishandle " inactive" acl rules
CSCuo04965	Clientless scrollbar on right hand side of the screen doesn't render

Table 6 Resolved Bugs in ASA Version 9.2(2.4) (continued)

Bug	Description
CSCuo05186	ASA 9.1 DMA Memory exhaustion in 240 binsize
CSCuo08511	ASA 9.0.4.1 traceback in webvpn datapath
CSCuo10869	VPN-filter ACL drops all traffic after upgrade for pre 8.3 to 9.x
CSCuo11057	IPsec transform sets mode changes from transport to tunnel after editing
CSCuo11867	CSCub92315 fix is incomplete
CSCuo14701	Interop: relax PrintableString encoding enforcement in PKI
CSCuo19916	ASA - Cut Through Proxy sends empty redirect w/ Virtual HTTP and Telnet
CSCuo23892	ASA SIP Inspect:'From: header' in the INVITE not NATed for outbound flow
CSCuo26501	ASA: Traceback in Thread Name: Dispatch Unit when enable debug ppp int
CSCuo26632	ASA SSLVPN OWA 2007: Unable to attach files >= 1 MB with KCD enabled
CSCuo27866	Traceback on DATAPATH-7-1524 Generating Botnet Filter Syslog
CSCuo32369	ASA WebVPN Rewriter: CSCOGet_location Improperly Pulls Full Web Address
CSCuo33186	Traceback with thread DATAPATH-2-1181
CSCuo37603	object nat config getting deleted after reloaded with vpdn config
CSCuo42563	Traceback DHCP 'IP Address Assign' while upgrading ASAs in Failover
CSCuo44216	ASA traceback (Page fault) during xlate replication in a failover setup
CSCuo46136	ASA does not relay BOOTP packets
CSCuo48593	ASA with SFP+4GE-SSM sends flow-control packets at line rate
CSCuo49385	Multicast - ASA doesn't populate mroutes after failover
CSCuo53772	CWS: Large downloads on HTTPS fail when server side seq number wraps
CSCuo54393	ASA: HTTP searchPendingOrders.do function failing over WebVPN
CSCuo54448	WebVPN capture causes conflict with other capture types
CSCuo58411	ASA IKEv2 " Duplicate entry in tunnel manager" (post 9.1.5)
CSCuo60435	ASA: Webvpn using incorrect password for auto-signon with Radius/OTP
CSCuo61372	ASA doesn't send invalid SPI notify for non-existent NAT-T IPSec SA
CSCuo63172	ASA 9.1.(3)4 Memory Leak in KCD
CSCuo64803	ASA Rewriter does not support encoded values for characters like " ' "
CSCuo70963	WebVPN: Javascript rewrite issue with Secret Server Application
CSCuo73792	ASA 9.x Management Port-Channel Cannot configure management-only in TFW
CSCuo78285	Firewall may crash while clearing the configuration
CSCuo78892	Traceback when using IDFW ACL's with VPN VPN Filters
CSCuo82612	5585-20 9.2.1 Traceback in Thread Name: DATAPATH-1-1567
CSCuo84225	CIFS drag & drop not working with remote file explorer over webvpn
CSCuo88253	ASA NAT: Some NAT removed after upgrade from 8.6.1.5 to 9.x
CSCuo89924	Giaddr to be set to the address of interface facing the client.
CSCuo91763	ASA allows to empty an access-list referenced elsewhere
CSCuo93225	Windriver: Traceback during AnyConnect IPv6 TLS TPS Test
CSCuo95074	ASA AnyConnect failure or crash in SSL Client compression with low mem

Table 6 Resolved Bugs in ASA Version 9.2(2.4) (continued)

Bug	Description
CSCuo95602	Standby ASA traceback on Fover_Parse with Botnet Filter
CSCuo97036	show vpn load-balancing shows Public addr as Cluster IP addr for Master
CSCuo99186	Inconsistencies seen while sending warmstart trap on reload
CSCup00433	Failover Standby unit has higher memory utilization
CSCup01676	ASA: Crash in DATAPATH
CSCup05772	Snmp-server hosts entries are lost when upgrading from 9.1(4) to 9.1(5)
CSCup07447	ASA WebVPN: Script error when using port-forwarding
CSCup08262	9.0(4)5 - Unable to access internal site via clientless SSLVPN
CSCup08912	ASA SSLVPN Java plugins fail through proxy with Connection Exception
CSCup08934	ASA WebVPN Rewriter: Custom HTTP Headers Not Properly Rewritten
CSCup09236	L2TP/IPsec fragmentation change causing ICMP-PMTU being sent
CSCup09881	show webvpn kcd Error code 2 (ERROR_FILE_NOT_FOUND)
CSCup09958	ASA: Webvpn Clientless - certificate authentication fails intermittently
CSCup13265	ASA - Traceback in thread name: sch_prompt anonymous reporting
CSCup16512	ASA traceback in Thread Name : Checkheaps when snmp config is cleared
CSCup16860	IKEv2 DPD is sent at an interval not correlating to the specified value
CSCup24465	Jumbo frame calculations are incorrect or hard coded
CSCup26021	TCP intercept does not work after embryonic connection ends
CSCup26347	ASA Panic: CP Processing - ERROR: shrlock_join_domain
CSCup32973	ASA EIGRP does not reset hold time after receiving update
CSCup33868	ASA doesn't apply vpn-filter if group policy is assigned by Cisco VSA 25
CSCup36543	WebVPN Problem- icons missing, buttons not working
CSCup40357	SNMP: Unable to verify presence of second power supply in ASA 5545
CSCup43257	ASA Traceback in Thread name: ci/console while modifying an object-group
CSCup47885	ASA: Page fault traceback in DATAPATH when DNS inspection is enabled
CSCup48772	ASA - Wrong object-group migration during upgrade from 8.2
CSCup48979	ASA - Permitting/blocking traffic based on wrong IPs in ACL
CSCup59774	No syslogs for ASDM or clientless access with blank username/password
CSCup68697	WebVPN: uploading customized portal.css breaks the portal login page
CSCup76212	ASA rewrites incorrect content-length in SIP message

Resolved Bugs in Version 9.2(1)

Table 7 contains resolved bugs in ASA Version 9.2(1).

If you are a registered Cisco.com user, view more information about each bug using Bug Search at the following website:

https://bst.cloudapps.cisco.com/bugsearch/

Table 7 Resolved Bugs in ASA Version 9.2(1)

Bug	Description
CSCty28878	ASA SSLVPN/DTLS: Copy inner packet TOS field to outer header
CSCud94029	Local CA rollover: reloading ASA deletes original CA cert before expiry
CSCue38161	wr mem all produces traceback on console
CSCuj09444	ASA:Difference in replication result of initial sync and boot sequence
CSCuj49205	SNMP: OID(1.3.6.1.4.1.99.X) inadvertently added
CSCuj62017	ASA doesn't RST conn for same sec-level int (resetoutbound/inbound only)
CSCul16778	vpn load-balancing configuration exits sub-command menu unexpectedly
CSCul61545	ASA Page Fault Traceback in 'vpnfol_thread_msg' Thread
CSCul65863	ASA IGMP receiver-specific filter blocks all multicast receivers
CSCul94773	ASA TCP Proxy can corrupt data, cause ACK storms and session hangs
CSCum03212	URLF: Websense v4 message length calculation is incorrect by 2 bytes
CSCum28756	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
CSCum51780	Problem configuring QOS priority with user-statistic on same policy-map
CSCun20457	ASA 9.1.x should accept RIP V1 updates
CSCun32388	ASA 5585 cluster indicating SSM card down but no SSM module
CSCun48868	ASA changes to improve CX throughput and prevent unnecessary failovers

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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.