



# Release Notes for the Cisco ASA Series, Version 9.1(x)

---

**Released: December 3, 2012**

**Updated: January 7, 2014**

This document contains release information for Cisco ASA software Version 9.1(1) through 9.1(4). This document includes the following sections:

- [Important Notes, page 1](#)
- [Limitations and Restrictions, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Upgrading the Software, page 13](#)
- [Open Caveats, page 23](#)
- [Resolved Caveats, page 24](#)
- [End-User License Agreement, page 36](#)
- [Related Documentation, page 36](#)
- [Obtaining Documentation and Submitting a Service Request, page 36](#)

## Important Notes

- ASA 9.1(3) features for the ASA CX require ASA CX Version 9.2(1).
- Upgrading ASA Clustering from 9.0(1) or 9.1(1)—Due to many caveat fixes, we recommend the 9.0(2) or 9.1(2) release or later for ASA clustering. If you are running 9.0(1) or 9.1(1), you should upgrade to 9.0(2) or 9.1(2) or later. Note that due to CSCue72961, hitless upgrading is not supported.
- Upgrading to 9.1(2.8) or 9.1(3) or later—See the [“Upgrade Path and Migrations”](#) section on [page 13](#).
- ASA CX software module SSD—An SSD is required to install the ASA CX software module on the ASA 5500-X series. Non-Cisco SSDs are not supported.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## Limitations and Restrictions

- Downgrading from 9.1(4) with failover and VPN using inner IPv6 with IKEv2—If you want to downgrade your failover pair, and you are using the 9.1(4) inner IPv6 VPN feature, then you must disconnect the connection before downgrading. If you downgrade without disconnecting, then any new AnyConnect connection that is assigned the same IP address as the previous connection will fail. (CSCul56646)
- Clientless SSL VPN with a self-signed certificate on the ASA—When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later and Safari are unable to add security exceptions when browsing using an IPv6 address HTTPS URL (FQDN URL is OK): the “Confirm Security Exception” button is disabled. See [https://bugzilla.mozilla.org/show\\_bug.cgi?id=633001](https://bugzilla.mozilla.org/show_bug.cgi?id=633001). This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including clientless SSL VPN connections, and ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority. For Internet Explorer 9 and later, use compatibility mode.
- When configuring for IKEv2, for security reasons you should use groups 21, 20, 19, 24, 14, and 5. We do not recommend Diffie Hellman Group1 or Group2. For example, use
 

```
crypto ikev2 policy 10
group 21 20 19 24 14 5
```
- With a heavy load of users (around 150 or more) using a WebVPN plugin, you may experience large delays because of the processing overload. Using Citrix web interface reduces the ASA rewrite overhead. To track the progress of the enhancement request to allow WebVPN plug files to be cached on the ASA, refer to CSCud11756.
- (ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing using the **crypto engine large-mod-accel** command instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware.



### Note

For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment.

The ASA 5580/5585-X platforms already integrate this capability; therefore, **crypto engine** commands are not applicable on these platforms.

## System Requirements

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

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html>

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

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html>

# New Features

- [New Features in Version 9.1\(4\), page 3](#)
- [New Features in Version 9.1\(3\), page 5](#)
- [New Features in Version 9.1\(2\), page 6](#)
- [New Features in Version 9.1\(1\), page 12](#)



## Note

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

## New Features in Version 9.1(4)

**Released: December 9, 2013**

[Table 1](#) lists the new features for ASA Version 9.1(4).

**Table 1**      **New Features for ASA Version 9.1(4)**

Feature	Description
<b>Remote Access Features</b>	
HTML5 WebSocket proxying	<p>HTML5 WebSockets provide persistent connections between clients and servers. During the establishment of the clientless SSL VPN connection, the handshake appears to the server as an HTTP Upgrade request. The ASA will now proxy this request to the backend and provide a relay after the handshake is complete. Gateway mode is not currently supported.</p> <p>We did not modify any commands.</p>
Inner IPv6 for IKEv2	<p>IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to AnyConnect VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic are being tunneled, and when both the client and headend support GRE. For a single traffic type, or when GRE is not supported by the client or the headend, we use straight IPsec.</p> <p><b>Note</b> This feature requires AnyConnect Client Version 3.1.05 or later.</p> <p>Output of the <b>show ipsec sa</b> and <b>show vpn-sessiondb detail anyconnect</b> commands has been updated to reflect the assigned IPv6 address, and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.</p> <p>The <b>vpn-filter</b> command must now be used for both IPv4 and IPv6 ACLs. If the deprecated <b>ipv6-vpn-filter</b> command is used to configure IPv6 ACLs the connection will be terminated.</p>
Mobile Devices running Citrix Server Mobile have additional connection options	<p>Support for mobile devices connecting to Citrix server through the ASA now includes selection of a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select different tunnel-groups allows the administrator to use different authentication methods.</p> <p>We introduced the <b>application-type</b> command to configure the default tunnel group for VDI connections when a Citrix Receiver user does not choose a tunnel-group. A <b>none</b> action was added to the <b>vd</b> command to disable VDI configuration for a particular group policy or user.</p>

**Table 1**      ***New Features for ASA Version 9.1(4) (continued)***

<b>Feature</b>	<b>Description</b>
Split-tunneling supports exclude ACLs	<p>Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACLs. Exclude ACLs were previously ignored.</p> <p><b>Note</b>    This feature requires AnyConnect Client Version 3.1.03103 or later.</p> <p>We did not modify any commands.</p>
<b>High Availability and Scalability Features</b>	
ASA 5500-X support for clustering	<p>The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license.</p> <p>We did not modify any commands.</p>
Improved VSS and vPC support for health check monitoring	<p>If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them.</p> <p>We modified the following command: <b>health-check [vss-enabled]</b></p>
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	<p>You can now place cluster members at different geographical locations when using individual interface mode. See the configuration guide for inter-site guidelines.</p> <p>We did not modify any commands.</p>
<b>Basic Operation Features</b>	
DHCP rebind function	<p>During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew.</p> <p>We introduced the following commands: <b>show ip address dhcp lease proxy</b>, <b>show ip address dhcp lease summary</b>, and <b>show ip address dhcp lease server</b>.</p>

**Table 1**      ***New Features for ASA Version 9.1(4) (continued)***

Feature	Description
<b>Troubleshooting Features</b>	
Crashinfo dumps include AK47 framework information	<p>Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in crashinfo dumps. A new option, <b>ak47</b>, has been added to the <b>debug menu</b> command to help in debugging AK47 framework issues. The framework-related information in the crashinfo dump includes the following:</p> <ul style="list-style-type: none"> <li>• Creating an AK47 instance.</li> <li>• Destroying an AK47 instance.</li> <li>• Generating an crashinfo with a memory manager frame.</li> <li>• Generating a crashinfo after fiber stack overflow.</li> <li>• Generating a crashinfo after a local variable overflow.</li> <li>• Generating a crashinfo after an exception has occurred.</li> </ul>

## New Features in Version 9.1(3)

**Released: September 18, 2013**

[Table 2](#) lists the new features for ASA Version 9.1(3).

**Table 2**      ***New Features for ASA Version 9.1(3)***

Feature	Description
<b>Module Features</b>	
Support for the ASA CX module in multiple context mode	<p>You can now configure ASA CX service policies per context on the ASA.</p> <p><b>Note</b> Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We did not modify any commands.</p>
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	<p>ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We did not modify any commands.</p>

**Table 2**      **New Features for ASA Version 9.1(3) (continued)**

Feature	Description
Filtering packets captured on the ASA CX backplane	<p>You can now filter packets that have been captured on the ASA CX backplane using the <b>match</b> or <b>access-list</b> keyword with the <b>capture interface asa_dataplane</b> command. Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic. In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because only control traffic cannot be filtered using an access list or match, these options are not available in the system execution space.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We modified the following command: <b>capture interface asa_dataplane</b>.</p>
<b>Monitoring Features</b>	
Ability to view top 10 memory users	<p>You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the <b>show memory detail</b> command and the <b>show memory binsize</b> command); the new command provides for quicker analysis of memory issues.</p> <p>We introduced the following command: <b>show memory top-usage</b>.</p> <p><i>Also available in 8.4(6).</i></p>
Smart Call Home	<p>We added a new type of Smart Call Home message to support ASA clustering.</p> <p>A Smart Call Home clustering message is sent for only the following three events:</p> <ul style="list-style-type: none"> <li>• When a unit joins the cluster</li> <li>• When a unit leaves the cluster</li> <li>• When a cluster unit becomes the cluster master</li> </ul> <p>Each message that is sent includes the following information:</p> <ul style="list-style-type: none"> <li>• The active cluster member count</li> <li>• The output of the <b>show cluster info</b> command and the <b>show cluster history</b> command on the cluster master</li> </ul> <p>We modified the following commands: <b>show call-home</b>, <b>show running-config call-home</b>.</p> <p><i>Also available in 9.0(3).</i></p>
<b>Remote Access Features</b>	
<b>user-storage value</b> command password is now encrypted in <b>show</b> commands	<p>The password in the <b>user-storage value</b> command is now encrypted when you enter <b>show running-config</b>.</p> <p>We modified the following command: <b>user-storage value</b>.</p> <p><i>Also available in 8.4(6).</i></p>

## New Features in Version 9.1(2)

Released: May 14, 2013

Table 3 lists the new features for ASA Version 9.1(2).

**Note**

Features added in 8.4(6) are not included in 9.1(2) unless they are explicitly listed in this table.

**Table 3**      **New Features for ASA Version 9.1(2)**

Feature	Description
<b>Certification Features</b>	
FIPS and Common Criteria certifications	<p>The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and the ASA Services Module.</p> <p>The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions.</p>
<b>Encryption Features</b>	
Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications	<p>Instead of using the proprietary encryption for the failover key (the <b>failover key</b> command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption.</p> <p><b>Note</b> Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.</p> <p>We introduced or modified the following commands: <b>failover ipsec pre-shared-key</b>, <b>show vpn-sessiondb</b>.</p>
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	<p>The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites:</p> <ul style="list-style-type: none"> <li>DHE-AES128-SHA1</li> <li>DHE-AES256-SHA1</li> </ul> <p>These cipher suites are specified in RFC 3268, <i>Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)</i>.</p> <p>When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations:</p> <ul style="list-style-type: none"> <li>DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server.</li> </ul> <pre>!! set server version hostname(config)# ssl server-version tlsv1 sslv3 !! set client version hostname(config) # ssl client-version any</pre> <ul style="list-style-type: none"> <li>Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used.</li> <li>Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0.</li> </ul> <p>We modified the following command: <b>ssl encryption</b>.</p> <p><i>Also available in 8.4(4.1).</i></p>
<b>Management Features</b>	

**Table 3**      **New Features for ASA Version 9.1(2) (continued)**

Feature	Description
Support for administrator password policy when using the local database	<p>When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters.</p> <p>We introduced the following commands: <b>change-password</b>, <b>password-policy lifetime</b>, <b>password-policy minimum changes</b>, <b>password-policy minimum-length</b>, <b>password-policy minimum-lowercase</b>, <b>password-policy minimum-uppercase</b>, <b>password-policy minimum-numeric</b>, <b>password-policy minimum-special</b>, <b>password-policy authenticate enable</b>, <b>clear configure password-policy</b>, <b>show running-config password-policy</b>.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for SSH public key authentication	<p>You can now enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits).</p> <p>We introduced the following commands: <b>ssh authentication</b>.</p> <p><i>Also available in 8.4(4.1); PKF key format support is only in 9.1(2).</i></p>
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	<p>An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.</p> <p>We introduced the following command: <b>show ssh sessions detail</b>.</p>
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	<p>Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported.</p> <p>We introduced the following command: <b>ssh key-exchange</b>.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for a maximum number of management sessions	<p>You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions.</p> <p>We introduced the following commands: <b>quota management-session</b>, <b>show running-config quota management-session</b>, <b>show quota management-session</b>.</p> <p><i>Also available in 8.4(4.1).</i></p>
The default Telnet password was removed	<p>To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. <b>Note:</b> The login password is only used for Telnet if you do not configure Telnet user authentication (the <b>aaa authentication telnet console</b> command).</p> <p>Formerly, when you cleared the password, the ASA restored the default of “cisco.” Now when you clear the password, the password is removed.</p> <p>The login password is also used for Telnet sessions from the switch to the ASASM (see the <b>session</b> command). For initial ASASM access, you must use the <b>service-module session</b> command, until you set a login password.</p> <p>We modified the following command: <b>passwd</b>.</p> <p><i>Also available in 9.0(2).</i></p>
<b>Platform Features</b>	



**Table 3**      **New Features for ASA Version 9.1(2) (continued)**

Feature	Description
Support for Power-On Self-Test (POST)	<p>The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140-2-compliant mode.</p> <p>Additional tests have been added to the POST to address the changes in the AES-GCM/GMAC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Validation System (DRBGVS).</p>
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3DES encryption to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	<p>Support for SHA-512 image integrity checking was added.</p> <p>We modified the following command: <b>verify</b>.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.
CPU profile enhancements	<p>The <b>cpu profile activate</b> command now supports the following:</p> <ul style="list-style-type: none"> <li>• Delayed start of the profiler until triggered (global or specific thread CPU%)</li> <li>• Sampling of a single thread</li> </ul> <p>We modified the following command: <b>cpu profile activate</b> [<i>n-samples</i>] [<b>sample-process</b> <i>process-name</i>] [<b>trigger cpu-usage</b> <i>cpu%</i> [<i>process-name</i>]].</p> <p><i>Also available in 8.4(6).</i></p>
<b>DHCP Features</b>	
DHCP relay servers per interface (IPv4 only)	<p>You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay.</p> <p>We introduced or modified the following commands: <b>dhcprelay server</b> (interface config mode), <b>clear configure dhcprelay</b>, <b>show running-config dhcprelay</b>.</p>
DHCP trusted interfaces	<p>You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface.</p> <p>We introduced or modified the following commands: <b>dhcprelay information trusted</b>, <b>dhcprelay informarion trust-all</b>, <b>show running-config dhcprelay</b>.</p>
<b>Module Features</b>	

**Table 3**      ***New Features for ASA Version 9.1(2) (continued)***

<b>Feature</b>	<b>Description</b>
ASA 5585-X support for network modules	<p>The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules:</p> <ul style="list-style-type: none"> <li>• ASA 4-port 10G Network Module</li> <li>• ASA 8-port 10G Network Module</li> <li>• ASA 20-port 1G Network Module</li> </ul> <p><i>Also available in 8.4(4.1).</i></p>
ASA 5585-X DC power supply support	<p>Support was added for the ASA 5585-X DC power supply.</p> <p><i>Also available in 8.4(5).</i></p>
Support for ASA CX monitor-only mode for demonstration purposes	<p>For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected.</p> <p>Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA.</p> <p>We modified or introduced the following commands: <b>cxsc {fail-close   fail-open} monitor-only, traffic-forward cxsc monitor-only.</b></p>
Support for the ASA CX module and NAT 64	<p>You can now use NAT 64 in conjunction with the ASA CX module.</p> <p>We did not modify any commands.</p>
<b>NetFlow Features</b>	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	<p>In addition to adding the flow-update events, there are now NetFlow templates that allow you to track flows that experience a change to their IP version with NAT, as well as IPv6 flows that remain IPv6 after NAT.</p> <p>Two new fields were added for IPv6 translation support.</p> <p>Several NetFlow field IDs were changed to their IPFIX equivalents.</p> <p>For more information, see the <i>Cisco ASA Implementation Note for NetFlow Collectors</i>.</p>
<b>Firewall Features</b>	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	<p>In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL.</p> <p>We modified the following command: <b>access-list ethertype {permit   deny} is-is.</b></p> <p><i>Also available in 8.4(5).</i></p>
Decreased the half-closed timeout minimum value to 30 seconds	<p>The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection.</p> <p>We modified the following commands: <b>set connection timeout half-closed, timeout half-closed.</b></p>
<b>Remote Access Features</b>	

**Table 3**      **New Features for ASA Version 9.1(2) (continued)**

Feature	Description
IKE security and performance improvements	The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as well as IKE v2.  We modified the following command: <b>crypto ikev1 limit</b> .
	The IKE v2 Nonce size has been increased to 64 bytes.  There are no ASDM screen or CLI changes.
	For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used by child IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be downgraded to the IKE level.  This new algorithm is enabled by default. We recommend that you do not disable this feature.  We introduced the following command: <b>crypto ipsec ikev2 sa-strength-enforcement</b> .
	For Site-to-Site, IPsec data-based rekeying can be disabled.  We modified the following command: <b>crypto ipsec security-association</b> .
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy.  <i>Also available in 8.4(5).</i>
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems.  We support the following browsers on Windows 8: <ul style="list-style-type: none"> <li>• Internet Explorer 10 (desktop only)</li> <li>• Firefox (all supported Windows 8 versions)</li> <li>• Chrome (all supported Windows 8 versions)</li> </ul> See the following limitations: <ul style="list-style-type: none"> <li>• Internet Explorer 10: <ul style="list-style-type: none"> <li>– The Modern (AKA Metro) browser is not supported.</li> <li>– If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone.</li> <li>– If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported.</li> </ul> </li> <li>• A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.</li> </ul> <i>Also available in 9.0(2).</i>

**Table 3**      **New Features for ASA Version 9.1(2) (continued)**

Feature	Description
Cisco Secure Desktop: Windows 8 Support	<p>CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check.</p> <p>See the following limitations:</p> <ul style="list-style-type: none"> <li>Secure Desktop (Vault) is not supported with Windows 8.</li> </ul> <p><i>Also available in 9.0(2).</i></p>
<b>Monitoring Features</b>	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	<p>Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP.</p> <p>This data is equivalent to the <b>show xlate count</b> command.</p> <p><i>Also available in 8.4(5).</i></p>
NSEL	<p>Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent.</p> <p>We introduced or modified the following commands: <b>flow-export active refresh-interval</b>, <b>flow-export event-type</b>.</p> <p><i>Also available in 8.4(5).</i></p>

## New Features in Version 9.1(1)

**Released: December 3, 2012**

[Table 4](#) lists the new features for ASA Version 9.1(1).



**Note**

Features added in 8.4(4.x), 8.4(5), 8.4(6), and 9.0(2) are not included in 9.1(1) unless they were listed in the 9.0(1) feature table.

**Table 4**      **New Features for ASA Version 9.1(1)**

Feature	Description
<b>Module Features</b>	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	<p>We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX software module requires a Cisco solid state drive (SSD) on the ASA. For more information about the SSD, see the ASA 5500-X hardware guide.</p> <p>We modified the following commands: <b>session cxsc</b>, <b>show module cxsc</b>, <b>sw-module cxsc</b>.</p>

# Upgrading the Software

This section describes how to upgrade to the latest version and includes the following topics:

- [Upgrade Path and Migrations, page 13](#)
- [Viewing Your Current Version, page 14](#)
- [Downloading the Software from Cisco.com, page 14](#)
- [Upgrading a Standalone Unit, page 15](#)
- [Upgrading a Failover Pair or ASA Cluster, page 16](#)



**Note**

For ASDM procedures, see the ASDM documentation.

## Upgrade Path and Migrations

- If you are upgrading from a pre-8.3 release:
  - See the [Cisco ASA 5500 Migration Guide to Version 8.3 and Later](#) for important information about migrating your configuration.
  - You cannot upgrade directly to 9.0 or later. You must first upgrade to Version 8.3 or 8.4 for a successful migration.
- If you are upgrading from a pre-9.0 release, because of ACL migration, you cannot later perform a downgrade; be sure to back up your configuration file in case you want to downgrade. See the ACL migration section in the 9.0 release notes for more information.
- If you are upgrading from one of the following versions, you can successfully upgrade to 9.1(2.8) and 9.1(3) or later:
  - 8.4(5) or later
  - 9.0(2) or later
  - 9.1(2)

However, if you are running any earlier versions, you cannot upgrade directly to 9.1(2.8) or 9.1(3) or later without *first* upgrading to one of the above versions. For example:



ASA Version	First Upgrade to:	Then Upgrade to:
8.2(1)	8.4(6)	9.1(2.8) or 9.1(3) or later
8.4(4)	8.4(6)	9.1(2.8) or 9.1(3) or later
9.0(1)	9.0(3)	9.1(2.8) or 9.1(3) or later
9.1(1)	9.1(2)	9.1(2.8) or 9.1(3) or later

- Software Version Requirements for Zero Downtime Upgrading:

The units in a failover configuration or ASA cluster should have the same major (first number) and minor (second number) software version. However, you do not need to maintain version parity on the units during the upgrade process; you can have different versions on the software running on each unit and still maintain failover support. To ensure long-term compatibility and stability, we recommend upgrading all units to the same version as soon as possible.

Table 1-5 shows the supported scenarios for performing zero-downtime upgrades.

**Table 1-5 Zero-Downtime Upgrade Support**

Type of Upgrade	Support
Maintenance Release	<p>You can upgrade from any maintenance release to any other maintenance release within a minor release.</p> <p>For example, you can upgrade from 8.4(1) to 8.4(6) without first installing the maintenance releases in between.</p>
Minor Release	<p>You can upgrade from a minor release to the next minor release. You cannot skip a minor release.</p> <p>For example, you can upgrade from 8.2 to 8.3. Upgrading from 8.2 directly to 8.4 is not supported for zero-downtime upgrades; you must first upgrade to 8.3. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.2 to 8.4 (the model is not supported on 8.3).</p> <div>  <p><b>Note</b> Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.2 to 8.3.</p> </div>
Major Release	<p>You can upgrade from the last minor release of the previous version to the next major release.</p> <p>For example, you can upgrade from 8.6 to 9.0, assuming that 8.6 is the last minor version in the 8.x release series for your model. Upgrading from 8.6 directly to 9.1 is not supported for zero-downtime upgrades; you must first upgrade to 9.0. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.4 to 9.0 (the model is not supported on 8.5 or 8.6).</p> <div>  <p><b>Note</b> Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.4 to 9.0.</p> </div>

## Viewing Your Current Version

Use the **show version** command to verify the software version of your ASA.

## Downloading the Software from Cisco.com

If you have a Cisco.com login, you can obtain the OS and ASDM images from the following website:

<http://www.cisco.com/go/asa-software>

This procedure assumes you put the images on a TFTP server, although other server types are supported.

## Upgrading a Standalone Unit

This section describes how to install the ASDM and operating system (OS) images using TFTP. For FTP or HTTP, see the **copy** command.

### Detailed Steps

	Command	Purpose
Step 1	<b>more system:running-config</b>  <b>Example:</b> hostname# more system:running-config	(If there is a configuration migration) The output shows the configuration on the terminal so that you can back up your configuration. Copy the output from this command, then paste the configuration in to a text file.  <b>Note</b> If you are upgrading from a pre-8.3 version, then the running configuration is backed up automatically.  For other methods of backing up, see the configuration guide.
Step 2	<b>copy tftp://server[/path]/asa_image_name {disk0:/   disk1:/}[/path]/asa_image_name</b>  <b>Example:</b> hostname# copy tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin	Copies the ASA software to the active unit flash memory. For other methods than TFTP, see the <b>copy</b> command.
Step 3	<b>copy tftp://server[/path]/asdm_image_name {disk0:/   disk1:/}[/path]/asdm_image_name</b>  <b>Example:</b> hostname# copy tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin	Copies the ASDM image to the active unit flash memory.
Step 4	<b>configure terminal</b>  <b>Example:</b> hostname(config)# configure terminal	If you are not already in global configuration mode, accesses global configuration mode.
Step 5	<b>show running-config boot system</b>  <b>Example:</b> hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k8.bin	Shows the current boot images configured (up to 4). The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to <a href="#">Step 6</a> and <a href="#">Step 7</a> .
Step 6	<b>no boot system {disk0:/   disk1:/}[/path]/asa_image_name</b>  <b>Example:</b> hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k8.bin	Removes any existing boot image configurations so that you can enter the new boot image as your first choice.

	Command	Purpose
Step 7	<b>boot system</b> { <b>disk0:/</b>   <b>disk1:/</b> } [ <i>path/</i> ] <i>asa_image_name</i>  <b>Example:</b> hostname(config)# boot system disk0://asa911-smp-k8.bin	Sets the ASA image to boot (the one you just uploaded).  Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in <a href="#">Step 6</a> .
Step 8	<b>asdm image</b> { <b>disk0:/</b>   <b>disk1:/</b> } [ <i>path/</i> ] <i>asdm_image_name</i>  <b>Example:</b> hostname(config)# asdm image disk0:/asdm-711.bin	Sets the ASDM image to use (the one you just uploaded). You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.
Step 9	<b>write memory</b>  <b>Example:</b> hostname(config)# write memory	Saves the new settings to the startup configuration.
Step 10	<b>reload</b>  <b>Example:</b> hostname# reload	Reloads the ASA.

## Upgrading a Failover Pair or ASA Cluster

- [Upgrading an Active/Standby Failover Pair, page 16](#)
- [Upgrading an Active/Active Failover Pair, page 19](#)
- [Upgrading an ASA Cluster, page 21](#)

### Upgrading an Active/Standby Failover Pair

To upgrade the Active/Standby failover pair, perform the following steps.

#### Requirements

Perform these steps on the active unit.



## Detailed Steps

	Command	Purpose
Step 1	<b>more system:running-config</b>  <b>Example:</b> active# more system:running-config	(If there is a configuration migration) The output shows the configuration on the terminal so that you can back up your configuration. Copy the output from this command, then paste the configuration in to a text file.  <b>Note</b> If you are upgrading from a pre-8.3 version, then the running configuration is backed up automatically.  For other methods of backing up, see the configuration guide.
Step 2	<b>copy tftp://server[/path]/asa_image_name {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> active# copy tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin	Copies the ASA software to the active unit flash memory. For other methods than TFTP, see the <b>copy</b> command.
Step 3	<b>failover exec mate copy /noconfirm tftp://server[/path]/filename {disk0:/   disk1:/} [path/] filename</b>  <b>Example:</b> active# failover exec mate copy /noconfirm tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin	Copies the software to the standby unit; be sure to specify the same path as for the active unit.
Step 4	<b>copy tftp://server[/path]/asdm_image_name {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> active# copy tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin	Copies the ASDM image to the active unit flash memory.
Step 5	<b>failover exec mate copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> active# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin	Copies the ASDM image to the standby unit; be sure to specify the same path as for the active unit.
Step 6	<b>configure terminal</b>  <b>Example:</b> active(config)# configure terminal	If you are not already in global configuration mode, accesses global configuration mode.

	Command	Purpose
Step 7	<b>show running-config boot system</b>  <b>Example:</b> hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k8.bin	Shows the current boot images configured (up to 4). The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to <a href="#">Step 8</a> and <a href="#">Step 9</a> .
Step 8	<b>no boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k8.bin	Removes any existing boot image configurations so that you can enter the new boot image as your first choice.
Step 9	<b>boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> hostname(config)# boot system disk0://asa911-smp-k8.bin	Sets the ASA image to boot (the one you just uploaded).  Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in <a href="#">Step 8</a> .
Step 10	<b>asdm image {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> hostname(config)# asdm image disk0:/asdm-711.bin	Sets the ASDM image to use (the one you just uploaded). You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.
Step 11	<b>write memory</b>  <b>Example:</b> active(config)# write memory	Saves the new settings to the startup configuration.
Step 12	<b>failover reload-standby</b>  <b>Example:</b> active# failover reload-standby	Reloads the standby unit to boot the new image.  Wait for the standby unit to finish loading. Use the <b>show failover</b> command to verify that the standby unit is in the Standby Ready state.
Step 13	<b>no failover active</b>  <b>Example:</b> active# no failover active	Forces the active unit to fail over to the standby unit.
Step 14	<b>reload</b>  <b>Example:</b> active# reload	Reloads the former active unit (now the new standby unit). If you want to restore this unit to be active after it reloads, enter the <b>failover active</b> command.

## Upgrading an Active/Active Failover Pair

To upgrade two units in an Active/Active failover configuration, perform the following steps.

### Requirements

Perform these steps in the system execution space of the *primary* unit.

### Detailed Steps

	Command	Purpose
Step 1	<b>more system:running-config</b>  <b>Example:</b> <pre>primary# more system:running-config</pre>	(If there is a configuration migration) The output shows the configuration on the terminal so that you can back up your configuration. Copy the output from this command, then paste the configuration in to a text file.  <b>Note</b> If you are upgrading from a pre-8.3 version, then the running configuration is backed up automatically.  For other methods of backing up, see the configuration guide.
Step 2	<b>copy tftp://server[/path]/asa_image_name {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> <pre>primary# copy tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin</pre>	Copies the ASA software to the primary unit flash memory. For other methods than TFTP, see the <b>copy</b> command.
Step 3	<b>failover exec mate copy /noconfirm tftp://server[/path]/filename {disk0:/   disk1:/} [path/] filename</b>  <b>Example:</b> <pre>primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin</pre>	Copies the software to the secondary unit; be sure to specify the same path as for the primary unit.
Step 4	<b>copy tftp://server[/path]/asdm_image_name {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> <pre>primary# copy tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin</pre>	Copies the ASDM image to the primary unit flash memory.
Step 5	<b>failover exec mate copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> <pre>primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin</pre>	Copies the ASDM image to the secondary unit; be sure to specify the same path as for the active unit.

	Command	Purpose
Step 6	<b>failover active group 1</b> <b>failover active group 2</b>  <b>Example:</b> primary# failover active group 1 primary# failover active group 2	Makes both failover groups active on the primary unit.
Step 7	<b>configure terminal</b>  <b>Example:</b> primary(config)# configure terminal	If you are not already in global configuration mode, accesses global configuration mode.
Step 8	<b>show running-config boot system</b>  <b>Example:</b> hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k8.bin	Shows the current boot images configured (up to 4). The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to <a href="#">Step 9</a> and <a href="#">Step 10</a> .
Step 9	<b>no boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k8.bin	Removes any existing boot image configurations so that you can enter the new boot image as your first choice.
Step 10	<b>boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> hostname(config)# boot system disk0://asa911-smp-k8.bin	Sets the ASA image to boot (the one you just uploaded). Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in <a href="#">Step 9</a> .
Step 11	<b>asdm image {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> hostname(config)# asdm image disk0:/asdm-711.bin	Sets the ASDM image to use (the one you just uploaded). You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.
Step 12	<b>write memory</b>  <b>Example:</b> primary(config)# write memory	Saves the new settings to the startup configuration.
Step 13	<b>failover reload-standby</b>  <b>Example:</b> primary# failover reload-standby	Reloads the secondary unit to boot the new image.  Wait for the secondary unit to finish loading. Use the <b>show failover</b> command to verify that both failover groups are in the Standby Ready state.

	Command	Purpose
Step 14	<pre>no failover active group 1 no failover active group 2</pre> <p><b>Example:</b></p> <pre>primary# no failover active group 1 primary# no failover active group 2</pre>	Forces both failover groups to become active on the secondary unit.
Step 15	<pre>reload</pre> <p><b>Example:</b></p> <pre>primary# reload</pre>	Reloads the primary unit. If the failover groups are configured with the <b>preempt</b> command, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with the <b>preempt</b> command, you can return them to active status on their designated units using the <b>failover active group</b> command.

## Upgrading an ASA Cluster

To upgrade all units in an ASA cluster, perform the following steps on the master unit. For multiple context mode, perform these steps in the system execution space.

### Detailed Steps

	Command	Purpose
Step 1	<pre>more system:running-config</pre> <p><b>Example:</b></p> <pre>master# more system:running-config</pre>	<p>(If there is a configuration migration) Back up your configuration file. Copy the output from this command, then paste the configuration in to a text file.</p> <p>For other methods of backing up, see the configuration guide.</p>
Step 2	<pre>cluster exec copy /noconfirm tftp://server[/path]/asa_image_name {disk0:/   disk1:/}[path/]asa_image_name</pre> <p><b>Example:</b></p> <pre>master# cluster exec copy /noconfirm tftp://10.1.1.1/asa911-smp-k8.bin disk0:/asa911-smp-k8.bin</pre>	Copies the ASA software to all units in the cluster. For other methods than TFTP, see the <b>copy</b> command.
Step 3	<pre>cluster exec copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/   disk1:/}[path/]asdm_image_name</pre> <p><b>Example:</b></p> <pre>master# cluster exec copy /noconfirm tftp://10.1.1.1/asdm-711.bin disk0:/asdm-711.bin</pre>	Copies the ASDM image to all units in the cluster.
Step 4	<pre>configure terminal</pre> <p><b>Example:</b></p> <pre>master(config)# configure terminal</pre>	If you are not already in global configuration mode, accesses global configuration mode.

	Command	Purpose
Step 5	<b>show running-config boot system</b>  <b>Example:</b> <pre>hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k8.bin</pre>	Shows the current boot images configured (up to 4). The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to <a href="#">Step 6</a> and <a href="#">Step 7</a> .
Step 6	<b>no boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> <pre>hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k8.bin</pre>	Removes any existing boot image configurations so that you can enter the new boot image as your first choice.
Step 7	<b>boot system {disk0:/   disk1:/} [path/] asa_image_name</b>  <b>Example:</b> <pre>hostname(config)# boot system disk0://asa911-smp-k8.bin</pre>	Sets the ASA image to boot (the one you just uploaded).  Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in <a href="#">Step 6</a> .
Step 8	<b>asdm image {disk0:/   disk1:/} [path/] asdm_image_name</b>  <b>Example:</b> <pre>hostname(config)# asdm image disk0:/asdm-711.bin</pre>	Sets the ASDM image to use (the one you just uploaded). You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.
Step 9	<b>write memory</b>  <b>Example:</b> <pre>master(config)# write memory</pre>	Saves the new settings to the startup configuration.
Step 10	<b>cluster exec unit slave-unit reload noconfirm</b>  <b>Example:</b> <pre>master# cluster exec unit unit2 reload noconfirm</pre>	Reload each slave unit by repeating this command for each unit name. To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up (approximately 5 minutes) before reloading the next unit.  To view member names, enter <b>cluster exec unit ?</b> , or enter the <b>show cluster info</b> command.
Step 11	<b>no enable</b>  <b>Example:</b> <pre>master(config)# no enable</pre>	Disables clustering on the master unit. Wait for 5 minutes for a new master to be selected and traffic to stabilize.  Do not enter <b>write memory</b> ; when the master unit reloads, you want clustering to be enabled on it.
Step 12	<b>reload noconfirm</b>  <b>Example:</b> <pre>master# reload noconfirm</pre>	Reloads the master unit. A new election takes place for a new master unit. When the former master unit rejoins the cluster, it will be a slave.

# Open Caveats

Table 6 contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in these sections to the resolved caveats from later releases. For example, if you are running Version 9.1(1), then you need to add the caveats in this section to the resolved caveats from 9.1(2) and higher to determine the complete list of open caveats.

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

<https://tools.cisco.com/bugsearch>

**Table 6** *Open Caveats in ASA Version 9.1*

Caveat	Description
CSCug24468	Unable to associate PRSM with AD_Realm.
CSCug66471	ASA: Form on sharepoint 2010 does not open when accessing through webvpn
CSCui30278	ASA will traceback if anyconnect configuration is deleted
CSCui44095	ASA 9.1 : timer app id was corrupted and leading to dispatch Unit crash
CSCui63001	ASA traceback in Thread Name: fover_parse during command replication
CSCuj50870	ASA in failover pair may panic in shrlock_unjoin
CSCuj98977	ASA Traceback in thread SSH when ran "show service set conn detail"
CSCuj99176	Make ASA-SSM cplane keepalives more tolerable to communication delays
CSCul00624	ASA: ARP Fails for Subinterface Allocated to Multiple Contexts on Gi0/6
CSCul07504	Scansafe: ASA forwards https packets to SS tower in wrong sequence
CSCul16778	vpn load-balancing configuration exits sub-command menu unexpectedly
CSCul20046	ASA 9.1.3 - %ASA-4-402124: CRYPTO: ASA hardware accelerator error
CSCul22237	ASA may drop all traffic with Hierarchical priority queuing
CSCul24557	TFW Dropping fragmented V6 mcast traffic with 3 intf in a bridge group
CSCul37888	traffic does not match time-rang access-list configured with policy-maps
CSCul46000	2048 byte block depletion with Smart-Tunnel Application
CSCul46582	ASA: Out of order Fin packet leaves connection half closed
CSCul47395	ASA should allow out-of-order traffic through nromalizer for ScanSafe
CSCul48246	ASA: HTTP URL based cert lookup causes ikev2 tunnel to fail
CSCul49901	ASA 9.1.3 traffic hairpinning from AC client over L2L is dropped
CSCul51932	ASA : Incorrect ACL log when traffic is implicitly denied by global ACL
CSCul55863	ASA with ICMP insp. drops replies with 'seq num not matched' code
CSCul61545	ASA Page Fault Traceback in 'vpnfal_thread_msg' Thread
CSCul64645	WebVpn: d3 library is not working
CSCul67325	Rekey intermittently fails when ASA is EZVPN headend
CSCul67705	ASA sends RST to both ends when CX policy denies based on destination IP
CSCul68246	ASA TCP Normalizer does not handle OOO TCP ACKs to the box

**Table 6**      *Open Caveats in ASA Version 9.1 (continued)*

<b>Caveat</b>	<b>Description</b>
CSCul68419	ASA 9.1.2 crashing in checkHeap
CSCul70712	ASA: ACL CLI not converting 0.0.0.0 0.0.0.0 to any4
CSCul73785	WEBVPN multiple issues with LMS application
CSCul74286	ASA: Phy setting change on member interfaces not seen on port-channel
CSCul77465	BPDU's on egress from ASA-SM dropped on backplane
CSCul77722	Traceback with assertion "0" failed: file "malloc.c", line 5839
CSCul78021	Webvpn rewriter javascript debugger error on page Oracle E-Business

## Resolved Caveats

- [Resolved Caveats in Version 9.1\(4\), page 24](#)
- [Resolved Caveats in Version 9.1\(3\), page 27](#)
- [Resolved Caveats in Version 9.1\(2\), page 31](#)
- [Resolved Caveats in Version 9.1\(1\), page 36](#)

## Resolved Caveats in Version 9.1(4)

[Table 7](#) contains resolved caveats in ASA Version 9.1(4).

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

<https://tools.cisco.com/bugsearch>

**Table 7**      *Resolved Caveats in ASA Version 9.1(4)*

<b>Caveat</b>	<b>Description</b>
CSCtd57392	Unable to create policy map depending on existing maps and name
CSCtg31077	DHCP relay binding limit of 100 should be increased to 500
CSCtg63826	ASA: multicast 80-byte block leak in combination with phone-proxy
CSCtr80800	Improve HTTP inspection's logging of proxied HTTP GETs
CSCtu37460	Backup Shared License Server unable to open Socket
CSCtw82904	ESP packet drop due to failed anti-replay checking after HA failovered
CSCty13865	ASA DHCP proxy for VPN clients should use ARP cache to reach server
CSCtz70573	SMP ASA traceback on periodic_handler for inspecting icmp or dns traffic
CSCub43580	Traceback during child SA rekey
CSCud16208	ASA 8.4.4.5 - Traceback in Thread Name: Dispatch Unit
CSCue33632	ASA 5500x on 9.1.1 IPS SW module reset causes ASA to reload.
CSCug33233	ASA Management lost after a few days of uptime



**Table 7**      **Resolved Caveats in ASA Version 9.1(4) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCug48732	Crash when loading configuration from TFTP multiple contexts
CSCug97772	Watchdog due to access-list change during uauth
CSCuh03193	ASA - Not all GRE connections are replicated to the standby unit
CSCuh12279	ASA: Data packets with urgent pointer dropped with IPS as bad-tcp-cksum
CSCuh21682	ASA traceback with less PAT with huge traffic
CSCuh32106	ASA KCD is broken in 8.4.5 onwards
CSCuh38785	Improve ScanSafe handling of Segment HTTP requests
CSCuh70040	Renew SmartTunnel Web Start .jnlp Certificate 9/7/2013
CSCui00618	ASA does not send Gratuitous ARP(GARP) when booting
CSCui01258	limitation of session-threshold-exceeded value is incorrect
CSCui06108	LU allocate xlate failed after Standby ASA traceback
CSCui08074	ak47 instance got destroyed issue
CSCui12430	ASA: SIP inspection always chooses hairpin NAT/PAT for payload rewrite
CSCui19504	ASA: HA state progression failure after reload of both units in HA
CSCui20216	ASA CX Fail-Open Drops traffic during reload
CSCui20346	ASA: Watchdog traceback in DATAPATH thread
CSCui22862	ASA traceback when using "Capture Wizard" on ASDM
CSCui24669	ASA PAT rules are not applied to outbound SIP traffic version 8.4.5/6
CSCui25277	ASA TFW doesn't rewrite VLAN in BPDU packets containing Ethernet trailer
CSCui36033	PP: VoIP interface fails replication on standby due to address overlap
CSCui36550	ASA crashes in Thread Name: https_proxy
CSCui38495	ASA Assert in Checkheaps chunk create internal
CSCui41794	ASA A/A fover automatic MAC address change causes i/f monitoring to fail
CSCui45340	ASA-SM assert traceback in timer-infra
CSCui45606	ASA traceback upon resetting conn due to filter and inspect overlap
CSCui51199	Cisco ASA Clientless SSL VPN Rewriter Denial of Service
CSCui55190	Failover cluster traceback while modifying object groups via SSH
CSCui55510	ASA traceback in Thread Name: DATAPATH-2-1140
CSCui55978	ASA 8.2.5 snmpEngineTime displays incorrect values
CSCui57181	ASA/IKEv1-L2L: Do not allow two IPsec tunnels with identical proxy IDs
CSCui61335	Traceback in Thread: DATAPATH-3-1281 Page fault: Address not mapped
CSCui61822	ASA 5585 - traceback after reconnect failover link and 'show run route'
CSCui63322	ASA Traceback When Debug Crypto Archives with Negative Pointers
CSCui65495	ASA 5512 - Temporary security plus license does not add security context
CSCui66657	Safari crashes when use scroll in safari on MAC 10.8 with smart-tunnel
CSCui70562	AnyConnect Copyright Panel and Logon Form message removed after upgrade

**Table 7**      **Resolved Caveats in ASA Version 9.1(4) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCui75284	ASA: Summary IPv6 range not advertised by ABR for OSPFv3
CSCui76124	ASA telnet limit reached 9.0.3
CSCui78992	ASA after fover may not flush routes for an active grp in active/standby
CSCui80059	ASA traceback in pix_startup_thread
CSCui80835	ASA drops packet as PAWS failure after incorrect TSecr is seen
CSCui85750	ASA SCH Inventory message incorrectly set at Severity 10
CSCui88578	Failure when accessing CIFS share with period character in username
CSCui91247	ASA does not pass calling-station-id when doing cert base authentication
CSCui94757	ASA tears down SIP signaling conn w/ reason Connection timeout
CSCui98879	Clientless SSL VPN:Unable to translate for Japanese
CSCuj00614	SNMP environmental parameters oscillate on 5512,25,45 and 5550 platforms
CSCuj06865	ASA traceback when removing more than 210 CA certificates at once
CSCuj08004	AnyConnect states: "VPN configuration received... has an invalid format"
CSCuj10559	ASA 5505: License Host limit counts non-existent hosts
CSCuj13728	ASA unable to remove ipv6 address from BVI interface
CSCuj16320	ASA 8.4.7 Multi Context TFW not generating any syslog data
CSCuj23632	Certificate CN and ASA FQDN mismatch causes ICA to fail.
CSCuj26709	ASA crashes on access attempt via Citrix Receiver
CSCuj28701	ASA - Default OSPF/EIGRP route gone in Active unit
CSCuj28861	Cisco ASA Malformed DNS Reply Denial of Service Vulnerability
CSCuj28871	ASA WebVPN: Rewriter doesn't work well with Base path and HTTP POST
CSCuj29434	ASA5505 - Max Conn Limit Does Not Update When Adding Temp Sec Plus Key
CSCuj33401	vpn_sanity script ipv4 DTLS RA testing using load-balancing fails
CSCuj33701	traceback ABORT(-87): strcpy_s: source string too long for dest
CSCuj34124	Sustained high cpu usage in Unicorn proxy thread with jar file rewrite
CSCuj34241	no debug all, undebg all CLI commands doesnt reset unicorn debug level
CSCuj39040	syslog 402123 CRYPTO: The ASA hardware accelerator encountered an error
CSCuj39069	ASA:"IKEv2 Doesn't have a proposal specified" though IKEv2 is disabled
CSCuj39727	Unable to modify existing rules/network groups after few days up time
CSCuj42515	ASA reloads on Thread name: idfw_proc
CSCuj43339	Add X-Frame-Options: SAMEORIGIN to ASDM HTTP response
CSCuj44998	ASA drops inbound traffic from AnyConnect Clients
CSCuj47104	EIGRP routes on the active ASA getting deleted after the ASA failover
CSCuj49690	ikev2 L2L cannot be established between contexts on the same ASA
CSCuj50376	ASA/Access is denied to the webfolder applet for a permitted cifs share
CSCuj51075	Unable to launch ASDM with no username/password or with enable password

**Table 7**      **Resolved Caveats in ASA Version 9.1(4) (continued)**

Caveat	Description
CSCuj54287	ASA ACL not applied object-group-search enabled & first line is remark
CSCuj58096	Crypto chip resets with large SRTP payload on 5555
CSCuj58670	Local CA server doesn't notify the first time allowed user
CSCuj60572	Unable to assign ip address from the local pool due to 'Duplicate local'
CSCuj62146	RU : Traceback on Thread Name : Cluster show config
CSCuj74318	ASA: crypto engine large-mod-accel support in multiple context
CSCuj81046	ASA defaults to incorrect max in-negotiation SA limit
CSCuj81157	ASA does not enforce max in-negotiation SA limit
CSCuj85424	Transparent ASA in Failover : Management L2L VPN termination fails
CSCuj88114	WebVPN Java rewriter issue: Java Plugins fail after upgrade to Java 7u45
CSCuj95555	SNMP: ccaAcclEntity MIB info for 5585 not consistent with CLI
CSCuj97361	DNS request failing with debugs "unable to allocate a handle"
CSCuj99263	Wrong ACL seq & remarks shown when using Range object w/ object-group
CSCul00917	SNMP: ccaGlobalStats values do not include SW crypto engine
CSCul19727	NPE: Querying unsupported IKEv2 MIB causes crash
CSCul35600	WebVPN: sharepoint 2007/2010 and Office2007 can't download/edit pictures

## Resolved Caveats in Version 9.1(3)

Table 8 contains resolved caveats in ASA Version 9.1(3).

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

<https://tools.cisco.com/bugsearch>

**Table 8**      **Resolved Caveats in ASA Version 9.1(3)**

Caveat	Description
CSCsv41155	reload due to block depletion needs post-event detection mechanism
CSCtg63826	ASA: multicast 80-byte block leak in combination with phone-proxy
CSCtw57080	Protocol Violation does not detect violation from client without a space
CSCua69937	Traceback in DATAPATH-1-1143 thread: abort with unknown reason
CSCua98219	Traceback in ci/console during context creation - ssl configuration
CSCub50435	Proxy ARP Generated for Identity NAT Configuration in Transparent Mode
CSCub52207	Nested Traceback from Watchdog in tmatch_release_recursive_locks()
CSCuc00279	ASA doesn't allow reuse of object when pat-pool keyword is configured
CSCuc66362	CP Processing hogs in SMP platform causing failover problems, overruns
CSCud05798	FIPS Self-Test failure, fips_continuous_rng_test [-1:8:0:4:4]
CSCud20080	ASA Allows duplicate xlate-persession config lines

**Table 8**      **Resolved Caveats in ASA Version 9.1(3) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCud21312	ASA verify /md5 shows incorrect sum for files
CSCud34973	ASA stops decrypting traffic after phase2 rekey under certain conditions
CSCud50997	ASA IKEv2 fails to accept incoming IKEV2 connections
CSCud76481	ASA 8.6/9.x : Fails to parse symbols in LDAP attribute name
CSCud84290	ASA: Random traceback with HA setup with 9.1.(1)
CSCud98455	ASA: 256 byte blocks depleted when syslog server unreachable across VPN
CSCue11738	ACL migration issues with NAT
CSCue27223	Standby sends proxy neighbor advertisements after failover
CSCue34342	ASA may traceback due to watchdog timer while getting mapped address
CSCue46275	Connections not timing out when the route changes on the ASA
CSCue46386	Cisco ASA Xlates Table Exhaustion Vulnerability
CSCue48432	Mem leak in PKI: crypto_get_DN_DER
CSCue51796	OSPF routes missing for 10 secs when we failover one of ospf neighbour
CSCue60069	ENH: Reload ASA when free memory is low
CSCue62422	Multicast,Broadcast traffic is corrupted on a shared interface on 5585
CSCue67198	Crypto accelerator resets with error code 23
CSCue78836	ASA removes TCP connection prematurely when RPC inspect is active
CSCue88423	ASA traceback in datapath thread with netflow enabled
CSCue90343	ASA 9.0.1 & 9.1.1 - 256 Byte Blocks depletion
CSCue95008	ASA - Threat detection doesn't parse network objects with IP 'range'
CSCue98716	move OSPF from the punt event queue to its own event queue
CSCuf07393	ASA assert traceback during xlate replication in a failover setup
CSCuf27008	Webvpn: Cifs SSO fails first attempt after AD password reset
CSCuf29783	ASA traceback in Thread Name: ci/console after write erase command
CSCuf31253	Floating route takes priority over the OSPF routes after failover
CSCuf31391	ASA failover standby unit keeps reloading while upgrade 8.4.5 to 9.0.1
CSCuf64977	No debug messages when DHCP OFFER packet dropped due to RFC violations
CSCuf67469	ASA sip inspection memory leak in binsize 136
CSCuf68858	ASA: Page fault traceback in dbgtrace when running debug in SSH session
CSCuf71119	Incorrect NAT rules picked up due to divert entries
CSCuf79091	Cisco ASA time-range object may have no effect
CSCuf85295	ASA changes user privilege by vpn tunnel configuration
CSCuf85524	Traceback when NULL pointer was passed to the l2p function
CSCuf90410	ASA LDAPS authorization fails intermittently
CSCuf92320	ASA-CX: Cosmetic parser error "'sw-module cxsc recover configure image"
CSCuf93071	ASA 8.4.4.1 traceback in threadname Datapath

**Table 8**      **Resolved Caveats in ASA Version 9.1(3) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCuf93843	No value or incorrect value for SNMP OIDs needed to identify VPN clients
CSCug03975	ASA 9.1(1) Reboot while applying regex dns
CSCug08285	Webvpn: OWA 2010 fails to load when navigating between portal and OWA
CSCug10123	ASA sends ICMP Unreach. thro wrong intf. under certain condn.
CSCug13534	user-identity will not retain group names with spaces on reboot
CSCug23311	cannot access Oracle BI via clientless SSL VPN
CSCug25761	ASA has inefficient memory use when cumulative AnyConnect session grows
CSCug29809	Anyconnect IKEv2:Truncated/incomplete debugs,missing 3 payloads
CSCug31704	ASA - "Show Memory" Output From Admin Context is Invalid
CSCug33233	ASA Management lost after a few days of uptime
CSCug39080	HA sync configuration stuck - "Unable to sync configuration from Active"
CSCug45645	Standby ASA continues to forward Multicast Traffic after Failover
CSCug45674	ASA : HTTP Conn from the box, broken on enabling TCP-State-Bypass
CSCug51148	Responder uses pre-changed IP address of initiator in IKE negotiation
CSCug53708	Thread Name: Unicorn Proxy Thread
CSCug55657	ASA does not assign MTU to AnyConnect client in case of IKEv2
CSCug55969	ASA uses different mapped ports for SDP media port and RTP stream
CSCug56940	ASA Config Locked by another session prevents error responses.
CSCug58801	ASA upgrade from 8.4 to 9.0 changes context's mode to router
CSCug63063	ASA 9.x: DNS inspection corrupts RFC 2317 PTR query
CSCug64098	ASA 9.1.1-7 traceback with Checkheaps thread
CSCug66457	ASA : "ERROR:Unable to create router process" & routing conf is lost
CSCug71714	DHCPD appends trailing dot to option 12 [hostname] in DHCP ACK
CSCug72498	ASA scansafe redirection drops packets if tcp mss is not set
CSCug74860	Multiple concurrent write commands on ASA may cause failure
CSCug75709	ASA terminates SIP connections prematurely generating syslog FIN timeout
CSCug76763	Cannot login webvpn portal when Passwd mgmt is enabled for Radius server
CSCug77782	ASA5585 - 9.1.1 - Traceback on IKEv2Daemon Thread
CSCug78561	ASA Priority traffic not subject to shaping in Hierarchical QoS
CSCug79778	ASA standby traceback in fover_parse when upgrading to 9.0.2
CSCug82031	ASA traceback in Thread Name: DATAPATH-4-2318
CSCug83036	L2TP/IPSec traffic fails because UDP 1701 is not removed from PAT
CSCug83080	Cross-site scripting vulnerability
CSCug86386	Inconsistent behavior with dACL has syntax error
CSCug87482	webvpn redirection fails when redirection FQDN is same as ASA FQDN
CSCug90225	ASA: EIGRP Route Is Not Updated When Manually Adding Delay on Neighbor

**Table 8**      **Resolved Caveats in ASA Version 9.1(3) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCug94308	ASA: "clear config all" does not clear the enable password
CSCug95287	ASA IDFW: idle users not marked as 'inactive' after default idle timeout
CSCug98852	Traceback when using VPN Load balancing feature
CSCug98894	Traceback in Thread Name: OSPF Router during interface removal
CSCuh01167	Unable to display webpage via WebVPN portal, ASA 9.0(2)9
CSCuh01983	ASA tearsdown TCP SIP phone registration conn due to SIP inspection
CSCuh05751	WebVPN configs not synchronized when configured in certain order
CSCuh05791	Single Sign On with BASIC authentication does not work
CSCuh08432	Anyconnect sessions do not connect due to uauth failure
CSCuh08651	UDP ports 500/4500 not reserved from PAT on multicontext ASA for IKEv1
CSCuh10076	Some interface TLVs are not sent in a bridge group in trans mode ASA
CSCuh10827	Cisco ASA config rollback via CSM doesnt work in multi context mode
CSCuh12375	ASA multicontext transparent mode incorrectly handles multicast IPv6
CSCuh13899	ASA protocol inspection connection table fill up DOS Vulnerability
CSCuh14302	quota management-session not working with ASDM
CSCuh19234	Traceback after upgrade from 8.2.5 to 8.4.6
CSCuh19462	ASA 9.1.2 - Memory corruptions in ctm hardware crypto code.
CSCuh20372	ASA adds 'extended' keyword to static manual nat configuration line
CSCuh20716	Re-transmitted FIN not allowed through with sysopt connection timewait
CSCuh22344	ASA: WebVPN rewriter fails to match opening and closing parentheses
CSCuh23347	ASA:Traffic denied 'licensed host limit of 0 exceeded
CSCuh27912	ASA does not obfuscate aaa-server key when timeout is configured.
CSCuh33570	ASA: Watchdog traceback in SSH thread
CSCuh34147	ASA memory leaks 3K bytes each time executing the show tech-support.
CSCuh40372	ASA Round-Robin PAT doesn't work under load
CSCuh45559	ASA: Page fault traceback when changing ASP drop capture buffer size
CSCuh48005	ASA doesn't send NS to stale IPv6 neighbor after failback
CSCuh48577	Slow memory leak on ASA due to SNMP
CSCuh49686	slow memory leak due to webvpn cache
CSCuh52326	ASA: Service object-group not expanded in show access-list for IDFW ACLs
CSCuh56559	ASA removed from cluster when updating IPS signatures
CSCuh58576	Different SNMPv3 Engine Time and Engine Boots in ASA active / standby
CSCuh66892	ASA: Unable to apply "http redirect <interface_name> 80" for webvpn
CSCuh69818	ASA 9.1.2 traceback in Thread Name ssh
CSCuh69931	ASA 5512 - 9.1.2 Traceback in Thread Name: ssh
CSCuh73195	Tunneled default route is being preferred for Botnet updates from ASA

**Table 8**      *Resolved Caveats in ASA Version 9.1(3) (continued)*

<b>Caveat</b>	<b>Description</b>
CSCuh74597	ASA-SM multicast boundary command disappears after write standby
CSCuh78110	Incorrect substitution of 'CSCO_WEBVPN_INTERNAL_PASSWORD' value in SSO
CSCuh79288	ASA 9.1.2 DHCP - Wireless Apple devices are not getting an IP via DHCPD
CSCuh79587	ASA5585 SSM card health displays down in ASA version 9.1.2
CSCuh80522	nat config is missing after csm rollback operation.
CSCuh90799	ASA 5505 Ezvpn Client fails to connect to Load Balance VIP on ASA server
CSCuh94732	Traceback in DATAPATH-1-2533 after a reboot in a clustered environment
CSCuh95321	Not all contexts successfully replicated to standby ASA-SM
CSCui10904	Macro substitution fails on External portal page customization
CSCui13436	ASA-SM can't change firewall mode using session from switch
CSCui15881	ASA Cluster - Loss of CCL link causes clustering to become unstable
CSCui27831	Nested Traceback with No Crashinfo File Recorded on ACL Manipulation
CSCui42956	ASA registers incorrect username for SSHv2 Public Key Authenticated user
CSCui48221	ASA removes RRI-injected route when object-group is used in crypto ACL

## Resolved Caveats in Version 9.1(2)

Table 9 contains resolved caveats in ASA Version 9.1(2).

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

<https://tools.cisco.com/bugsearch>

**Table 9**      *Resolved Caveats in ASA Version 9.1(2)*

<b>Caveat</b>	<b>Description</b>
CSCti07431	1/5 minute input rate and output rate are always 0 with user context.
CSCti38856	Elements in the network object group are not converted to network object
CSCtj87870	Failover disabled due to license incompatible different Licensed cores
CSCto50963	ASA SIP inspection - To: in INVITE not translated after 8.3/8.4 upgrade
CSCtr04553	Traceback while cleaning up portlist w/ clear conf all or write standby
CSCtr17899	Some legitimate traffic may get denied with ACL optimization
CSCtr65927	dynamic policy PAT fails with FTP data due to latter static NAT entry
CSCts15825	RRI routes are not injected after reload if IP SLA is configured.
CSCts50723	ASA: Builds conn for packets not destined to ASA's MAC in port-channel
CSCtw56859	Natted traffic not getting encrypted after reconfiguring the crypto ACL
CSCtx55513	ASA: Packet loss during phase 2 rekey
CSCty18976	ASA sends user passwords in AV as part of config command authorization.
CSCty59567	Observing traceback @ ipigrp2_redist_metric_incompatible+88

**Table 9**      **Resolved Caveats in ASA Version 9.1(2) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCtz46845	ASA 5585 with IPS inline -VPN tunnel dropping fragmented packets
CSCtz47034	ASA 5585- 10 gig interfaces may not come up after asa reload
CSCtz56155	misreported high CPU
CSCtz64218	ASA may traceback when multiple users make simultaneous change to ACL
CSCtz70573	SMP ASA traceback on periodic_handler for inspecting icmp or dns traffic
CSCtz79578	Port-Channel Flaps at low traffic rate with single flow traffic
CSCua13405	Failover Unit Stuck in Cold Standby After Boot Up
CSCua20850	5500X Software IPS console too busy for irq can cause data plane down.
CSCua22709	ASA traceback in Unicorn Proxy Thread while processing lua
CSCua35337	Local command auth not working for certain commands on priv 1
CSCua44723	ASA nat-pat: 8.4.4 assert traceback related to xlate timeout
CSCua60417	8.4.3 system log messages should appear in Admin context only
CSCua87170	Interface oversubscription on active causes standby to disable failover
CSCua91189	Traceback in CP Processing when enabling H323 Debug
CSCua93764	ASA: Watchdog traceback from tmatch_element_release_actual
CSCua99091	ASA: Page fault traceback when copying new image to flash
CSCub04470	ASA: Traceback in Dispatch Unit with HTTP inspect regex
CSCub08224	ASA 210005 and 210007 LU allocate xlate/conn failed with simple 1-1 NAT
CSCub11582	ASA5550 continous reboot with tls-proxy maximum session 4500
CSCub14196	FIFO queue oversubscription drops packets to free RX Rings
CSCub16427	Standby ASA traceback while replicating flow from Active
CSCub23840	ASA traceback due to nested protocol object-group used in ACL
CSCub37882	Standby ASA allows L2 broadcast packets with asr-group command
CSCub58996	Cisco ASA Clientless SSLVPN CIFS Vulnerability
CSCub61578	ASA: Assert traceback in PIX Garbage Collector with GTP inspection
CSCub62584	ASA unexpectedly reloads with traceback in Thread Name: CP Processing
CSCub63148	With inline IPS and heavy load ASA could drop ICMP or DNS replies
CSCub72545	syslog 113019 reports invalid address when VPN client disconnects.
CSCub75522	ASA TFW sends broadcast arp traffic to all interfaces in the context
CSCub83472	VPNFO should return failure to HA FSM when control channel is down
CSCub84164	ASA traceback in threadname Logger
CSCub89078	ASA standby produces traceback and reloads in IPsec message handler
CSCub98434	ASA: Nested Crash in Thread Dispatch Unit - cause: SQLNet Inspection
CSCub99578	High CPU HOG when connect/disconnect VPN with large ACL
CSCub99704	WebVPN - mishandling of request from Java applet
CSCuc06857	Accounting STOP with caller ID 0.0.0.0 if admin session exits abnormally



**Table 9**      **Resolved Caveats in ASA Version 9.1(2) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCuc09055	Nas-Port attribute different for authentication/accounting Anyconnect
CSCuc12119	ASA: Webvpn cookie corruption with external cookie storage
CSCuc12967	OSPF routes were missing on the Standby Firewall after the failover
CSCuc14644	SIP inspect NATs Call-ID in one direction only
CSCuc16455	ASA packet transmission failure due to depletion of 1550 byte block
CSCuc16670	ASA - VPN connection remains up when DHCP rebind fails
CSCuc24547	TCP ts_val for an ACK packet sent by ASA for OOO packets is incorrect
CSCuc24919	ASA: May traceback in Thread Name: fover_health_monitoring_thread
CSCuc28903	ASA 8.4.4.6 and higher: no OSPF adj can be build with Portchannel port
CSCuc34345	Multi-Mode treceback on ci/console copying config tftp to running-config
CSCuc40450	error 'Drop-reason: (punt-no-mem) Punt no memory' need to be specific
CSCuc45011	ASA may traceback while fetching personalized user information
CSCuc46026	ASA traceback: ASA reloaded when call home feature enabled
CSCuc46270	ASA never removes qos-per-class ASP rules when VPN disconnects
CSCuc48355	ASA webvpn - URLs are not rewritten through webvpn in 8.4(4)5
CSCuc50544	Error when connecting VPN: DTLS1_GET_RECORD Reason: wrong version number
CSCuc55719	Destination NAT with non single service (range, gt, lt) not working
CSCuc56078	Traceback in threadname CP Processing
CSCuc60950	Traceback in snpi_divert with timeout floating-conn configured
CSCuc61985	distribute-list does not show in the router config.
CSCuc63592	HTTP inspection matches incorrect line when using header host regex
CSCuc65775	ASA CIFS UNC Input Validation Issue
CSCuc74488	ASA upgrade fails with large number of static policy-nat commands
CSCuc74758	Traceback: deadlock between syslog lock and host lock
CSCuc75090	Crypto IPsec SA's are created by dynamic crypto map for static peers
CSCuc75093	Log indicating syslog connectivity not created when server goes up/down
CSCuc78176	Cat6000/15.1(1)SY- ASASM/8.5(1.14) PwrDwn due to SW Version Mismatch
CSCuc79825	ASA: Traceback in Thread Name CP Midpath Processing eip pkp_free_ssl_ctm
CSCuc83059	traceback in fover_health_monitoring_thread
CSCuc83323	XSS in SSLVPN
CSCuc83828	ASA Logging command submits invalid characters as port zero
CSCuc89163	Race condition can result in stuck VPN context following a rekey
CSCuc92292	ASA may not establish EIGRP adjacency with router due to version issues
CSCuc95774	access-group commands removed on upgrade to 9.0(1)
CSCuc98398	ASA writes past end of file system then can't boot
CSCud02647	traffic is resetting uauth timer

**Table 9**      **Resolved Caveats in ASA Version 9.1(2) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCud16590	ASA may traceback in thread emweb/https
CSCud17993	ASA-Traceback in Dispatch unit due to dcerpc inspection
CSCud20887	ASA reloads after issuing "show inventory" command
CSCud21714	BTF traceback in datapth when apply l4tm rule
CSCud24452	ASA TACACS authentication on Standby working incorrectly
CSCud28106	IKEv2: ASA does not clear entry from asp table classify crypto
CSCud29045	ASASM forwards subnet directed bcast back onto that subnet
CSCud32111	Deny rules in crypto acl blocks inbound traffic after tunnel formed
CSCud36686	Deny ACL lines in crypto-map add RRI routes
CSCud37992	SMP ASA traceback in periodic_handler in proxyi_rx
CSCud41507	Traffic destined for L2L tunnels can prevent valid L2L from establishing
CSCud41670	ASA nested traceback with url-filtering policy during failover
CSCud57759	DAP: debug dap trace not fully shown after +1000 lines
CSCud62661	STI Flash write failure corrupts large files
CSCud65506	ASA5585: Traceback in Thread Name:DATAPATH when accessing webvpn urls
CSCud67282	data-path: ASA-SM: 8.5.1 traceback in Thread Name: SSH
CSCud69251	traceback in ospf_get_authtype
CSCud69535	OSPF routes were missing on the Active Firewall after the failover
CSCud70273	ASA may generate Traceback while running packet-tracer
CSCud77352	Upgrade ASA causes traceback with assert during spinlock
CSCud81304	TRACEBACK, DATAPATH-8-2268, Multicast
CSCud84454	ASA in HA lose shared license post upgrade to 9.x
CSCud89974	flash in ASA5505 got corrupted
CSCud90534	ASA traceback with Checkheaps thread
CSCue02226	ASA 9.1.1 - WCCPv2 return packets are dropped
CSCue03220	Anyconnect mtu config at ASA not taking effect at client
CSCue04309	TCP connection to multicast MAC - unicast MAC S/ACK builds new TCP conn
CSCue05458	16k blocks near exhaustion - process emweb/https (webvpn)
CSCue11669	ASA 5505 not Forming EIGRP neighborship after failover
CSCue15533	ASA:Crash while deleting trustpoint
CSCue18975	ASA: Assertion traceback in DATAPATH thread after upgrade
CSCue25524	Webvpn: Javascript based applications not working
CSCue31622	Secondary Flows Lookup Denial of Service Vulnerability
CSCue32221	LU allocate xlate failed (for NAT with service port)
CSCue34342	ASA may crash due to watchdog timer while getting mapped address
CSCue35150	ASA in multicontext mode provides incorrect SNMP status of failover

**Table 9**      **Resolved Caveats in ASA Version 9.1(2) (continued)**

<b>Caveat</b>	<b>Description</b>
CSCue35343	Memory leak of 1024B blocks in webvpn failover code
CSCue49077	ASA: OSPF fails to install route into asp table after a LSA update
CSCue54264	WebVPN: outside PC enabled webvpn to management-access inside interface
CSCue55461	ESMTP drops due to MIME filename length >255
CSCue59676	ASA shared port-channel subinterfaces and multicontext traffic failure
CSCue62470	mrrib entries may not be seen upon failover initiated by auto-update
CSCue62691	ASASM Traceback when issue 'show asp table interface' command
CSCue63881	ASA SSHv2 Denial of Service Vulnerability
CSCue67446	The ASA hardware accelerator encountered an error (Bad checksum)
CSCue73708	Group enumeration still possible on ASA
CSCue77969	Character encoding not visible on webvpn portal pages.
CSCue82544	ASA5585 8.4.2 Traceback in Thread Name aaa while accessing Uauth pointer
CSCue88560	ASA Traceback in Thread Name : CERT API
CSCue99041	Smart Call Home sends Environmental message every 5 seconds for 5500-X
CSCuf02988	ASA: Page fault traceback in aaa_shim_thread
CSCuf06633	ASA crash in Thread Name: UserFromCert
CSCuf07810	DTLS drops tunnel on a crypto reset
CSCuf11285	ASA 9.x cut-through proxy ACL incorrectly evaluated
CSCuf16850	split-dns cli warning msg incorrect after client increasing the limit
CSCuf27811	ASA: Pending DHCP relay requests not flushed from binding table
CSCuf34123	ASA 8.3+ I2I tunnel-group name with a leading zero is changed to 0.0.0.0
CSCuf34754	Framed-IP-Address not sent with AC IKEv2 and INTERIM-ACCOUNTING-UPDATE
CSCuf47114	ASA 9.x: DNS inspection corrupts PTR query before forwarding packet
CSCuf52468	ASA Digital Certificate Authentication Bypass Vulnerability
CSCuf57102	FIPS: Continuous RNG test reporting a length failure
CSCuf58624	snmp engineID abnormal for asa version 8.4.5 after secondary asa reload
CSCuf65912	IKEv2: VPN filter ACL lookup failure causing stale SAs and crash
CSCuf77065	Arsenal: Single Core Saleen Admin Driver Fix Revert Bug
CSCuf77294	ASA traceback with Thread Name: DATAPATH-3-1041
CSCuf77606	ASA-SM crash in Thread Name: accept/http
CSCuf89220	ASA IDFW : Unable to handle contacts in DC user groups
CSCug03975	ASA 9.1(1) Reboot while applying regex dns
CSCug14707	ASA 8.4.4.1 Keeps rebooting when FIPS is enabled: FIPS Self-Test failure
CSCug19491	ASA drops some CX/CSC inspected HTTP packets due to PAWS violation
CSCug22787	Change of behavior in Prefill username from certificate SER extraction

**Table 9**      **Resolved Caveats in ASA Version 9.1(2) (continued)**

Caveat	Description
CSCug30086	ASA traceback on thread Session Manager
CSCug59177	Page fault on ssh thread

## Resolved Caveats in Version 9.1(1)

There are no resolved caveats in Version 9.1(1).

## 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*:

<http://www.cisco.com/go/asadocs>

## 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/en/US/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.

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1110R)

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.

©2012-2014 Cisco Systems, Inc. All rights reserved.