Release Notes for the Cisco ASA 5500 Series, Version 8.4(x)

Released: January 31, 2011
Updated: January 9, 2012

This document contains release information for Cisco ASA 5500 software Version 8.4(1) through 8.4(3).

This document includes the following sections:

- Important Notes, page 2
- Limitations and Restrictions, page 4
- System Requirements, page 5
- New Features, page 8
- Upgrading the Software, page 25
- Open Caveats, page 27
- Resolved Caveats, page 30
- End-User License Agreement, page 46
- Related Documentation, page 46
- Obtaining Documentation and Submitting a Service Request, page 46

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

Important Notes

- Increased SSH security; the SSH default username is no longer supported—Starting in 8.4(2), you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the **username** command (CLI) or choosing Configuration > Device Management > Users/AAA > User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
- Configuration Migration for Transparent Mode—In 8.4, all transparent mode interfaces now belong to a bridge group. When you upgrade to 8.4, the existing two interfaces are placed in bridge group 1, and the management IP address is assigned to the Bridge Group Virtual Interface (BVI). The functionality remains the same when using one bridge group. You can now take advantage of the bridge group feature to configure up to four interfaces per bridge group and to create up to eight bridge groups in single mode or per context.

Note In 8.3 and earlier, as an unsupported configuration, you could configure a management interface without an IP address, and you could access the interface using the device management address. In 8.4, the device management address is assigned to the BVI, and the management interface is no longer accessible using that IP address; the management interface requires its own IP address.

- You can upgrade from any previous release directly to 8.4. If you are upgrading from a pre-8.3 release, see the *Cisco ASA 5500 Migration Guide for Version 8.3 and Later* for important information about migrating your configuration to Version 8.3 and later.

  Upgrading from some releases may have consequences for downgrading; be sure to back up your configuration file in case you want to downgrade. For example, If you are upgrading from a pre-8.2 release, see the 8.2 release notes for downgrade issues after you upgrade the Phone Proxy and MTA instance, or for downgrade issues if you upgrade the activation key with new 8.2 features.
- For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) differs depending on the version to which you are upgrading. See the *Cisco ASA 5500 Migration Guide for Version 8.3 and Later* for more information.
- When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed.
- To run Version 8.3 and later in a production environment, you might need to upgrade the memory on the Cisco ASA 5505, 5510, 5520, or 5540. (For more information about upgrading, see the "Memory Information" section on page 5.) If you do not have enough memory, you receive the following message upon logging in:

```
**********************************************************************
**
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***
**
**          ----> Minimum Memory Requirements NOT Met! <----
**
**  Installed RAM:  512 MB
**  Required  RAM: 2048 MB
**  Upgrade part#: ASA5520-MEM-2GB=
**
**  This ASA does not meet the minimum memory requirements needed to
```

```
**  run this image. Please install additional memory (part number
**  listed above) or downgrade to ASA version 8.2 or earlier.
**  Continuing to run without a memory upgrade is unsupported, and
**  critical system features will not function properly.
**
************************************************************************
*
```

- The Advanced Inspection and Prevention Security Services Card (AIP SSC) can take up to 20 minutes to initialize the first time it boots after a new image is applied. This initialization process must complete before configuration changes can be made to the sensor. Attempts to modify and save configuration changes before the initialization completes will result in an error.
- When you downgrade, you must manually restore the old configuration prior to downgrading.
- Connection Profile/Tunnel Group terminology in CLI vs. ASDM—The ASA tunnel groups define the initial connection parameters and attributes (such as AAA, client address assignment, and connection alias/group-url) for a remote access VPN session. In the CLI they are referred to as *tunnel groups*, whereas in ASDM they are referred to as *Connection Profiles*. A VPN policy is an aggregation of Connection Profile, Group Policy, and Dynamic Access Policy authorization attributes.
- Cosmetic startup message issue on the ASA 5585-X—Cisco manufacturing recently discovered a process error that resulted in loading a test build of BIOS firmware on many early shipments of the ASA 5585-X. On the affected units, more text than usual displays on the console during startup before reaching the “rommon>” prompt. Included in the extra output is the following message banner:

  ```
  CISCO SYSTEMS Spyker Build, TEST build not for Customer Release
  Embedded BIOS Version 2.0(7)2 19:59:57 01/04/11
  ```

  While you may see this additional text, there is no functional impact to the ASA operation; you can ignore the additional text. The test build provides additional information that can be used by engineers to pinpoint hardware problems during the manufacturing process. Unfortunately, there is no field-upgradeable resolution to eliminate this message that does not require replacing the hardware.

  Hardware with a serial number that falls within the following ranges could be impacted by this cosmetic issue. Note that not all serial numbers within these ranges are impacted.

  - JMX1449xxxx – JMX1520xxxx
  - JAF1450xxxx – JAF1516xxxx (for ASA-SSP-20-K8= only)

  Hardware with the following Product IDs for the preceding serial numbers could be impacted by this cosmetic issue:

  - ASA5585-S20-K8
  - ASA5585-S20-K9
  - ASA5585-S20P20-K8
  - ASA5585-S20P20-K9
  - ASA5585-S20P20XK9
  - ASA5585-S20X-K9
  - ASA-SSP-20-K8=

Limitations and Restrictions

- Currently in 8.4(2) and later, the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT. For example, if you enter the following twice NAT command that configures a PAT pool (object2) for fallback when the addresses in object1 are used up, you see the following error message:

  ```
  hostname(config)# nat (inside,outside) source dynamic any object1 pat-pool object2
  interface round-robin
  ERROR: Same mapped parameter cannot be used to do both NAT and PAT.
  ERROR: NAT pool allocation failed.
  ```

  You can alter this command to make it PAT-pool only by removing object1; the PAT pool is used as the primary method, instead of as a fallback method:

  ```
  hostname(config)# nat (inside,outside) source dynamic any pat-pool object2 interface
  round-robin
  ```

  (CSCtq20634)

- No Payload Encryption for export—You can purchase the ASA 5585-X with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA software senses a No Payload Encryption model, and disables the following features:
  - Unified Communications
  - VPN

  You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).
- Stateful Failover with Phone Proxy—When using Stateful Failover with phone proxy, information is not passed to the standby unit; when the active unit goes down, the call fails, media stops flowing, and the call must be re-established.
- Clientless SSL VPN .NET limitation—Clientless SSL sessions might not properly support .NET framework applications. In some cases, you need to enable the application for use with Smart Tunnels; however, there is a chance it could still fail. For example, it might fail when an executable binary (.exe) is created using the .NET framework (CSCsv29942).
- The ASA does not support phone proxy with CIPC for remote access.
- The AIP SSC-5 does not support virtualization, unretiring default retired signatures, creating custom signatures, adding signatures, cloning signatures, or anomaly detection.
- ASA cannot fully support domain-based DFS. To support this, the ASA would need to join the Active Directory and query the Active Directory server for DFS referral. Instead the ASA sends the DFS referral to the DNS servers configured for the users. Because the AD server is the DNS server in most cases, the majority of customer configurations are covered.
- The Active Directory Agent, which is used for the Identity Firewall feature, does not support French. When IP-user mappings appear in French, the AD Agent drops the mapping because it parses the event based on the English language. The ASA cannot accept non-English characters in the console; therefore, users cannot configure an access rule with non-English usernames or user groups.

System Requirements

The sections that follow list the system requirements for operating an adaptive security appliance. This section includes the following topics:

- Minimum Active Directory PC Requirements for Identity Firewall in 8.4(2) and Later, page 5
- Memory Information, page 5
- ASDM, Module, and VPN Compatibility, page 8

Minimum Active Directory PC Requirements for Identity Firewall in 8.4(2) and Later

The Identity Firewall feature provides more granular access control based on user identities. You can configure access control and security policies based on usernames and groups rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses.

The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses.

You can install the Active Directory Agent on a separate server or on the server where the Active Directory Domain Controller is installed.

Table 1 lists the minimum hardware requirements for the AD agent and the Active Directory Server Domain Controller.

Table 1 Minimum Hardware Requirements

Component	OS	Hardware
AD Agent	Windows 2003 Server, Windows 2008 Server, Windows 2008 R2 Server	Intel Quad-core CPU, 4GB of RAM, 2 x 250GB of HDD, 1GE Network Interface
Active Directory Server Domain Controller	Windows 2003 Server, Windows 2008 Server, Windows 2008 R2 Server	Intel Quad-core CPU, 4GB of RAM, 2 x 250GB of HDD, 1GE Network Interface

Memory Information

The ASA includes DRAM and an internal CompactFlash card. On some models, you can optionally use an external CompactFlash card as well. This section includes the following topics:

- Memory Requirements, page 6
- Memory Upgrade Kits, page 6
- Viewing Flash Memory, page 7
- DRAM, Flash Memory, and Failover, page 7

Memory Requirements

Table 2 lists the standard and recommended flash memory and DRAM. Note that the shipping DRAM increased after February 2010; the DRAM requirements for 8.3 and higher match the newer default shipping sizes. See the "Memory Upgrade Kits" section on page 6 to order an upgrade kit.

Note ASA 5520 and ASA 5540 adaptive security appliances that were manufactured before August 2011 have 4 DIMM sockets. ASA 5520 and ASA 5540 adaptive security appliances manufactured after this date have 2 DIMM sockets.

Note If a memory upgrade might be required, the required memory is in **bold**. See the "Memory Upgrade Kits" section on page 6.

Table 2 Standard Memory and Memory Requirements for the Cisco ASA 5500 Series

ASA Model	Internal Flash Memory (Default Shipping)[1,2]	DRAM (Default Shipping)	
		Before Feb. 2010	After Feb. 2010 (Required for 8.3 and Higher)
5505	128 MB	256 MB	**512 MB**[3]
5510	256 MB	256 MB	**1 GB**
5520	256 MB	512 MB	**2 GB**
5540	256 MB	1 GB	**2 GB**
5550	256 MB	4 GB	4GB
5580-20	1 GB	8 GB	8GB
5580-40	1 GB	12 GB	12 GB
5585-X with SSP-10	2 GB	N/A	6 GB
5585-X with SSP-20	2 GB	N/A	12 GB
5585-X with SSP-40	2 GB	N/A	12 GB
5585-X with SSP-60	2 GB	N/A	24 GB

1. For the ASA 5510 through 5550, you might need to upgrade the internal flash memory to 512 MB or add external flash memory if you load multiple images of the AnyConnect client along with one or more images of the ASA software, ASDM, client/server plugins, or Cisco Secure Desktop. In particular, you might need to upgrade for multiple AnyConnect 3.0 and higher clients with optional modules. The ASA 5505 does not have a flash memory upgrade available.
2. The default internal flash memory for some models was 64 MB in the past; if you have one of these early units, we recommend upgrading your flash memory to at least the new shipping default.
3. For the ASA 5505, only the Unlimited Hosts license and the Security Plus license with failover enabled require 512 MB; other licenses can use 256 MB.

Memory Upgrade Kits

Table 3 lists the DRAM upgrade kits.

Table 3 DRAM Upgrade Kits

Model	Size	Part Number
ASA 5505	512 MB	ASA5505-MEM-512=
ASA 5510[1]	1 GB	ASA5510-MEM-1GB=

Table 3 DRAM Upgrade Kits (continued)

Model	Size	Part Number
ASA 5520	2 GB	ASA5520-MEM-2GB=
ASA 5540	2 GB	ASA5540-MEM-2GB=

1. If you previously purchased the 512 MB upgrade kit for the ASA 5510 (ASA5510-MEM-512=), you must upgrade to the 1 GB memory upgrade kit to run Version 8.3.

Table 4 lists the CompactFlash upgrade kits available for the ASA 5510 through ASA 5550, for use as internal or external flash memory.

Table 4 CompactFlash Upgrade Kits

Model	Size	Part Number
ASA 5510 through ASA 5550	256 MB	ASA5500-CF-256MB=
ASA 5510 through ASA 5550	512 MB	ASA5500-CF-512MB=

Viewing Flash Memory

You can check the size of internal flash and the amount of free flash memory on the ASA by doing the following:

- ASDM—Choose **Tools > File Management**. The amounts of total and available flash memory appear on the bottom left in the pane.
- CLI—In Privileged EXEC mode, enter the **dir** command. The amounts of total and available flash memory appear on the bottom of the output.

For example:

```
hostname # dir
Directory of disk0:/

43      -rwx  14358528    08:46:02 Feb 19 2007  cdisk.bin
136     -rwx  12456368    10:25:08 Feb 20 2007  asdmfile
58      -rwx  6342320     08:44:54 Feb 19 2007  asdm-600110.bin
61      -rwx  416354      11:50:58 Feb 07 2007  sslclient-win-1.1.3.173.pkg
62      -rwx  23689       08:48:04 Jan 30 2007  asa1_backup.cfg
66      -rwx  425         11:45:52 Dec 05 2006  anyconnect
70      -rwx  774         05:57:48 Nov 22 2006  cvcprofile.xml
71      -rwx  338         15:48:40 Nov 29 2006  tmpAsdmCustomization430406526
72      -rwx  32          09:35:40 Dec 08 2006  LOCAL-CA-SERVER.ser
73      -rwx  2205678     07:19:22 Jan 05 2007  vpn-win32-Release-2.0.0156-k9.pkg
74      -rwx  3380111     11:39:36 Feb 12 2007  securedesktop_asa_3_2_0_56.pkg

62881792 bytes total (3854336 bytes free)

hostname #
```

DRAM, Flash Memory, and Failover

In a failover configuration, the two units must have the same amount of DRAM. You do not have to have the same amount of flash memory. For more information, see the failover chapters in the configuration guide.

Note If you use two units with different flash memory sizes, make sure that the unit with the smaller flash memory has enough space for the software images and configuration files.

ASDM, Module, and VPN Compatibility

Table 5 lists information about ASDM, module, and VPN compatibility with the ASA 5500 series.

Table 5 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA 5500 Version 8.4 requires ASDM Version 6.4 or later. For information about ASDM requirements for other releases, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
SSM and SSC applications	For information about SSM and SSC application requirements, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

This section includes the following topics:

- New Features in Version 8.4(3), page 9
- New Features in Version 8.4(2.8), page 11
- New Features in Version 8.4(2), page 13
- New Features in Version 8.4(1.11), page 18
- New Features in Version 8.4(1), page 19

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

New Features in Version 8.4(3)

Released: January 9, 2012

Table 6 lists the new features for ASA Version 8.4(3).

Table 6 New Features for ASA Version 8.4(3)

Feature	Description
NAT Features	
Round robin PAT pool allocation uses the same IP address for existing hosts	When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. We did not modify any commands. *This feature is not available in 8.5(1).*
Flat range of PAT ports for a PAT pool	If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535. We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] (object network configuration mode) and **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] (global configuration mode). *This feature is not available in 8.5(1).*
Extended PAT for a PAT pool	Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] (object network configuration mode) and **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]] (global configuration mode). *This feature is not available in 8.5(1).*
Configurable timeout for PAT xlate	When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the port for a new translation, some upstream routers might reject the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a value between 30 seconds and 5 minutes. We introduced the following command: **timeout pat-xlate**. *This feature is not available in 8.5(1).*

Table 6 New Features for ASA Version 8.4(3) (continued)

Feature	Description
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the **show nat** command. **Note** Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations: • Only supports Cisco IPsec and AnyConnect Client. • Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied. • Does not support load-balancing (because of routing issues). • Does not support roaming (public IP changing). We introduced the following command: **nat-assigned-to-public-ip** *interface* (tunnel-group general-attributes configuration mode).
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4.
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** | **none**] and **anyconnect ssl compression** [**deflate** | **lzs** | **none**].
VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle-timeout alert-interval**.
AAA Features	

Table 6 New Features for ASA Version 8.4(3) (continued)

Feature	Description
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode).
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.
Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA	Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RADIUS access request packets from the ASA. Session Type (151) and Session Subtype (152) are sent in RADIUS accounting request packets from the ASA. All four attributes are sent for all accounting request packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS and ISE) can then enforce authorization and policy attributes or use them for accounting and billing purposes.
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*.

New Features in Version 8.4(2.8)

Released: August 31, 2011

Table 7 lists the new features for ASA interim Version 8.4(2.8).

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 7 New Features for ASA Interim Version 8.4(2.8)

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.2(5.13) and 8.3.2(25).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** | **none**] and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. *Also available in Version 8.2(5.13) and 8.3.2(25).*
VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle-timeout alert-interval**.
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode).
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. *Also available in Version 8.2(5.13) and 8.3.2(25).*

New Features in Version 8.4(2)

Released: June 20, 2011

Table 8 lists the new features for ASA Version 8.4(2).

Table 8 New Features for ASA Version 8.4(2)

Feature	Description
Firewall Features	
Identity Firewall	Typically, a firewall is not aware of the user identities and, therefore, cannot apply security policies based on identity. The Identity Firewall in the ASA provides more granular access control based on users' identities. You can configure access rules and security policies based on usernames and user groups name rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses. The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses. In an enterprise, some users log onto the network by using other authentication mechanisms, such as authenticating with a web portal (cut-through proxy) or by using a VPN. You can configure the Identity Firewall to allow these types of authentication in connection with identity-based access policies. We introduced or modified the following commands: **user-identity enable**, **user-identity default-domain**, **user-identity domain**, **user-identity logout-probe**, **user-identity inactive-user-timer**, **user-identity poll-import-user-group-timer**, **user-identity action netbios-response-fail**, **user-identity user-not-found**, **user-identity action ad-agent-down**, **user-identity action mac-address-mismatch**, **user-identity action domain-controller-down**, **user-identity ad-agent active-user-database**, **user-identity ad-agent hello-timer**, **user-identity ad-agent aaa-server**, **user-identity update import-user**, **user-identity static user**, **ad-agent-mode**, **dns domain-lookup**, **dns poll-timer**, **dns expire-entry-timer**, **object-group user, show user-identity, show dns**, **clear configure user-identity**, **clear dns, debug user-identity, test aaa-server ad-agent**.

Table 8 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Identity NAT configurable proxy ARP and route lookup	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed. We modified the following commands: **nat static** [**no-proxy-arp**] [**route-lookup**] (object network) and **nat source static** [**no-proxy-arp**] [**route-lookup**] (global).
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. **Note** Currently in 8.4(2), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (global).

Table 8 New Features for ASA Version 8.4(2) (continued)

Feature	Description
IPv6 Inspection	You can configure IPv6 inspection by configuring a service policy to selectively block IPv6 traffic based on the extension header. IPv6 packets are subjected to an early security check. The ASA always passes hop-by-hop and destination option types of extension headers while blocking router header and no next header. You can enable default IPv6 inspection or customize IPv6 inspection. By defining a policy map for IPv6 inspection you can configure the ASA to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet: • Hop-by-Hop Options • Routing (Type 0) • Fragment • Destination Options • Authentication • Encapsulating Security Payload We modified the following commands: **policy-map type inspect ipv6, verify-header, match header, match header routing-type**, **match header routing-address count gt, match header count gt**.
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources. We modified the following command: **webvpn portal-access-rule**. *Also available in Version 8.2(5).*
Clientless support for Microsoft Outlook Web App 2010	The ASA 8.4(2) clientless SSL VPN core rewriter now supports Microsoft Outlook Web App 2010.
Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF	This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashing security for IPsec/IKEv2 AnyConnect Secure Mobility Client connections to the ASA. SHA-2 includes hash functions with digests of 256, 384, or 512 bits, to meet U.S. government requirements. We modified the following commands: **integrity**, **prf, show crypto ikev2 sa detail**, **show vpn-sessiondb detail remote**.
Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2	This release supports the use of SHA-2 compliant signature algorithms to authenticate IPsec IKEv2 VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, and SHA-512. SHA-2 digital signature for IPsec IKEv2 connections is supported with the AnyConnect Secure Mobility Client, Version 3.0.1 or later.

Table 8 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy: tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list. We introduced the following command: **split-tunnel-all-dns**. *Also available in Version 8.2(5).*
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per group bases, and gather information about connected mobile devices based on a mobile device's posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. **Licensing Requirements** Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install: • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the following: – Enable or disable mobile device access on a per group basis and to configure that feature using ASDM. – Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices. *Also available in Version 8.2(5).*
SSL SHA-2 digital signature	You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This release does not support SHA-2 for other uses or products. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. We modified the following command: **show crypto ca certificate** (the Signature Algorithm field identifies the digest algorithm used when generating the signature). *Also available in Version 8.2(5).*

Table 8 New Features for ASA Version 8.4(2) (continued)

Feature	Description
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol. We did not modify any commands. *Also available in Version 8.2(5).*
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases. We introduced the following command: **tunnel-group-preference**. *Also available in Version 8.2(5).*
ASA 5585-X Features	
Support for Dual SSPs for SSP-40 and SSP-60	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. **Note** When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled. We modified the following commands: **show module**, **show inventory**, **show environment**.
Support for the IPS SSP-10, -20, -40, and -60	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10. *Also available in Version 8.2(5).*
CSC SSM Features	
CSC SSM Support	For the CSC SSM, support for the following features has been added: • HTTPS traffic redirection: URL filtering and WRS queries for incoming HTTPS connections. • Configuring global approved whitelists for incoming and outgoing SMTP and POP3 e-mail. • E-mail notification for product license renewals. We did not modify any commands.
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. We introduced the following commands: **call-home reporting anonymous, call-home test reporting anonymous**. *Also available in Version 8.2(5).*

Table 8 New Features for ASA Version 8.4(2) (continued)

Feature	Description
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description. *Also available in Version 8.2(5).*
Interface Features	
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following command: **flowcontrol**. *Also available in Version 8.2(5).*
Management Features	
Increased SSH security; the SSH default username is no longer supported	Starting in 8.4(2), you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the **username** command (CLI) or choosing Configuration > Device Management > Users/AAA > User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
Unified Communications Features	
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video). We did not modify any commands. *Also available in Version 8.2(5).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value. We modified the following command: **timeout floating-conn**. *Also available in Version 8.2(5).*

New Features in Version 8.4(1.11)

Released: May 20, 2011

Table 9 lists the new features forASA interim Version 8.4(1.11).

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the interim release notes available on the Cisco.com software download site.

Table 9 New Features for ASA Version 8.4(1.11)

Feature	Description
Firewall Features	
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. **Note** Currently in 8.4(1.11), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (global).

New Features in Version 8.4(1)

Released: January 31, 2011

Table 10 lists the new features for ASA Version 8.4(1).

Table 10 New Features for ASA Version 8.4(1)

Feature	Description
Hardware Features	
Support for the ASA 5585-X	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10, -20, -40, and -60. **Note** Support was previously added in 8.2(3) and 8.2(4); the ASA 5585-X is not supported in 8.3(x).

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
No Payload Encryption hardware for export	You can purchase the ASA 5585-X with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA software senses a No Payload Encryption model, and disables the following features: • Unified Communications • VPN You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).
Remote Access Features	
L2TP/IPsec Support on Android Platforms	We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1, or later, operating system. *Also available in Version 8.2(5).*
UTF-8 Character Support for AnyConnect Passwords	AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.
IPsec VPN Connections with IKEv2	Internet Key Exchange Version 2 (IKEv2) is the latest key exchange protocol used to establish and control Internet Protocol Security (IPsec) tunnels. The ASA now supports IPsec with IKEv2 for the AnyConnect Secure Mobility Client, Version 3.0(1), for all client operating systems. On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile. IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses. Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license. We modified the following commands: **vpn-tunnel-protocol**, **crypto ikev2 policy**, **crypto ikev2 enable**, **crypto ipsec ikev2**, **crypto dynamic-map**, **crypto map**.
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. **Caution**: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the **show crypto ca certificate command** to identify the digest algorithm used when generating the signature.

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
SCEP Proxy	SCEP Proxy provides the AnyConnect Secure Mobility Client with support for automated third-party certificate enrollment. Use this feature to support AnyConnect with zero-touch, secure deployment of device certificates to authorize endpoint connections, enforce policies that prevent access by non-corporate assets, and track corporate assets. This feature requires an AnyConnect Premium license and will not work with an Essentials license. We introduced or modified the following commands: **crypto ikev2 enable**, **scep-enrollment enable**, **scep-forwarding-url**, **debug crypto ca scep-proxy**, **secondary-username-from-certificate**, **secondary-pre-fill-username**.
Host Scan Package Support	This feature provides the necessary support for the ASA to install or upgrade a Host Scan package and enable or disable Host Scan. This package may either be a standalone Host Scan package or one that ASA extracts from an AnyConnect Next Generation package. In previous releases of AnyConnect, an endpoint's posture was determined by Cisco Secure Desktop (CSD). Host Scan was one of many features bundled in CSD. Unbundling Host Scan from CSD gives AnyConnect administrators greater freedom to update and install Host Scan separately from the other features of CSD. We introduced the following command: **csd hostscan image path**.
Kerberos Constrained Delegation (KCD)	This release implements the KCD protocol transition and constrained delegation extensions on the ASA. KCD provides Clientless SSL VPN (also known as WebVPN) users with SSO access to any web services protected by Kerberos. Examples of such services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server(IIS). Implementing protocol transition allows the ASA to obtain Kerberos service tickets on behalf of remote access users without requiring them to authenticate to the KDC (through Kerberos). Instead, a user authenticates to ASA using any of the supported authentication mechanisms, including digital certificates and Smartcards, for Clientless SSL VPN (also known as WebVPN). When user authentication is complete, the ASA requests and obtains an impersonate ticket, which is a service ticket for ASA on behalf of the user. The ASA may then use the impersonate ticket to obtain other service tickets for the remote access user. Constrained delegation provides a way for domain administrators to limit the network resources that a service trusted for delegation (for example, the ASA) can access. This task is accomplished by configuring the account under which the service is running to be trusted for delegation to a specific instance of a service running on a specific computer. We modified the following commands: **kcd-server**, **clear aaa**, **show aaa**, **test aaa-server authentication**.
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Apple Safari 5.

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
Clientless VPN Auto Sign-on Enhancement	Smart tunnel now supports HTTP-based auto sign-on on Firefox as well as Internet Explorer. Similar to when Internet Explorer is used, the administrator decides to which hosts a Firefox browser will automatically send credentials. For some authentication methods, if may be necessary for the administrator to specify a realm string on the ASA to match that on the web application (in the Add Smart Tunnel Auto Sign-on Server window). You can now use bookmarks with macro substitutions for auto sign-on with Smart tunnel as well. POST plug-in is now obsolete. The former POST plug-in was created so that administrators could specify a bookmark with sign-on macros and receive a kick-off page to load prior to posting the POST request. The post plug-in approach allows requests that required the presence of cookies, and other header items, fetched ahead of time to go through. The administrator can now specify pre-load pages when creating bookmarks to achieve the same functionality. Same as the POST plug-in, the administrator specifies the pre-load page URL and the URL to send the POST request to. You can now replace the default preconfigured SSL VPN portal with your own portal. The administrators do this by specifying a URL as an External Portal. Unlike group-policy home page, External Portal supports POST requests with macro substitution (for auto sign-on) as well as pre-load pages. We introduced or modified the following command: **smart-tunnel auto-signon**.
Expanded Smart Tunnel application support	Smart Tunnel adds support for the following applications: • Microsoft Outlook Exchange Server 2010 (native support). Users can now use Smart Tunnel to connect Microsoft Office Outlook to a Microsoft Exchange Server. • Microsoft Sharepoint/Office 2010. Users can now perform remote file editing using Microsoft Office 2010 Applications and Microsoft Sharepoint by using Smart Tunnel.
Interface Features	
EtherChannel support (ASA 5510 and higher)	You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. **Note** You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel. We introduced the following commands: **channel-group**, **lacp port-priority**, **interface port-channel**, **lacp max-bundle**, **port-channel min-bundle**, **port-channel load-balance**, **lacp system-priority**, **clear lacp counters**, **show lacp**, **show port-channel**.

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
Bridge groups for transparent mode	If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups. You can configure up to 8 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. **Note** Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group. We introduced the following commands: **interface bvi**, **show bridge-group**.
Scalability Features	
Increased contexts for the ASA 5550, 5580, and 5585-X	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Additional platform support	Google Chrome has been added as a supported platform for ASA Version 8.4. Both 32-bit and 64-bit platforms are supported on Windows XP, Vista, and 7 and Mac OS X Version 6.0.
Increased connections for the ASA 5580 and 5585-X	We increased the firewall connection limits: • ASA 5580-20—1,000,000 to 2,000,000. • ASA 5580-40—2,000,000 to 4,000,000. • ASA 5585-X with SSP-10: 750,000 to 1,000,000. • ASA 5585-X with SSP-20: 1,000,000 to 2,000,000. • ASA 5585-X with SSP-40: 2,000,000 to 4,000,000. • ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.
Increased AnyConnect VPN sessions for the ASA 5580	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	The other VPN session limit was increased from 5,000 to 10,000.
High Availability Features	
Stateful Failover with Dynamic Routing Protocols	Routes that are learned through dynamic routing protocols (such as OSPF and EIGRP) on the active unit are now maintained in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, traffic on the secondary active unit now passes with minimal disruption because routes are known. We modified the following commands: **show failover**, **show route**, **show route failover**.
Unified Communication Features	

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
UC Protocol Inspection Enhancements	SIP Inspection and SCCP Inspection are enhanced to support new features in the Unified Communications Solutions; such as, SCCP v2.0 support, support for GETPORT messages in SCCP Inspection, SDP field support in INVITE messages with SIP Inspection, and QSIG tunneling over SIP. Additionally, the Cisco Intercompany Media Engine supports Cisco RT Lite phones and third-party video endpoints (such as, Tandberg). We did not modify any commands.
Inspection Features	
DCERPC Enhancement	DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC messages. We did not modify an commands.
Troubleshooting and Monitoring Features	
SNMP traps and MIBs	Supports the following additional keywords: **connection-limit-reached**, **entity cpu-temperature**, **cpu threshold rising**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. The entPhysicalTable reports entries for sensors, fans, power supplies, and related components. Supports the following additional MIBs: ENTITY-SENSOR-MIB, CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, NAT-MIB, EVENT-MIB, EXPRESSION-MIB Supports the following additional traps: warmstart, cpmCPURisingThreshold, mteTriggerFired, cirResourceLimitReached, natPacketDiscard, ciscoEntSensorExtThresholdNotification. We introduced or modified the following commands: **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
TCP Ping Enhancement	TCP ping allows users whose ICMP echo requests are blocked to check connectivity over TCP. With the TCP ping enhancement you can specify a source IP address and a port and source interface to send pings to a hostname or an IPv4 address. We modified the following command: **ping tcp**.
Show Top CPU Processes	You can now monitor the processes that run on the CPU to obtain information related to the percentage of the CPU used by any given process. You can also see information about the load on the CPU, broken down per process, at 5 minutes, 1 minute, and 5 seconds prior to the log time. Information is updated automatically every 5 seconds to provide real-time statistics, and a refresh button in the pane allows a manual data refresh at any time. We introduced the following command: **show process cpu-usage sorted**.

Table 10 New Features for ASA Version 8.4(1) (continued)

Feature	Description
General Features	
Password Encryption Visibility	You can show password encryption in a security context. We modified the following command: **show password encryption**.

Upgrading the Software

Note You can upgrade from any previous release (if available for your model) directly to the latest release. If you are upgrading from a pre-8.3 release to a post-8.3 release, see the *Cisco ASA 5500 Migration Guide to Version 8.3 and Later* for important information about migrating your configuration to Version 8.3 or later.

Upgrading from some releases may have consequences for downgrading; be sure to back up your configuration file in case you want to downgrade.

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

- Viewing Your Current Version, page 25
- Upgrading the Operating System and ASDM Images, page 25

Note For ASDM procedures, see the ASDM release notes.

Viewing Your Current Version

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

Upgrading the Operating System and ASDM Images

This section describes how to install the ASDM and operating system (OS) images using TFTP. For FTP or HTTP, see the "Managing Software and Configurations" chapter in CLI configuration guide.

We recommend that you upgrade the ASDM image before the OS image. ASDM is backward compatible, so you can upgrade the OS using the new ASDM; however you cannot use an old ASDM image with a new OS.

For information about upgrading software in a failover pair, see the "Performing Zero Downtime Upgrades for Failover Pairs" chapter in the CLI configuration guide.

Detailed Steps

Step 1 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

Step 2 Back up your configuration file. To print the configuration to the terminal, enter the following command:

```
hostname# show running-config
```

Copy the output from this command, then paste the configuration in to a text file.

Note 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 "Managing Software and Configurations" chapter in the CLI configuration guide.

Step 3 Install the new images using TFTP. Enter this command separately for the OS image and the ASDM image:

```
hostname# copy tftp://server[/path]/filename {disk0:/ | disk1:/}[path/]filename
```

For example:

```
hostname# copy tftp://10.1.1.1/asa840-4-k8.bin disk0:/asa841-k8.bin
...
hostname# copy tftp://10.1.1.1/asdm-64099.bin disk0:/asdm-641.bin
```

If your ASA does not have enough memory to hold two images, overwrite the old image with the new one by specifying the same destination filename as the existing image.

Step 4 To change the OS boot image to the new image name, enter the following commands:

```
hostname(config)# clear configure boot
hostname(config)# boot system {disk0:/ | disk1:/}[path/]new_filename
```

For example:

```
hostname(config)# clear configure boot
hostname(config)# boot system disk0:/asa841-k8.bin
```

Step 5 To configure the ASDM image to the new image name, enter the following command:

```
hostname(config)# asdm image {disk0:/ | disk1:/}[path/]new_filename
```

Step 6 To save the configuration and reload, enter the following commands:

```
hostname(config)# write memory
hostname(config)# reload
```

Open Caveats

Table 11 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 8.4(1), then you need to add the caveats in this section to the resolved caveats from 8.4(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 Toolkit at the following website:

http://tools.cisco.com/Support/BugToolKit/

Table 11 Open Caveats in ASA Version 8.4

Caveat	Description
CSCtj19462	Static PAT augment fails with manual nat configuration
CSCtk60416	Config load time of 500k ACLs in Routed is 3 times faster than Transp
CSCtk97719	WebVPN & ASDM doesn't work on Chrome with AES & 3DES ciphers
CSCtk98002	ASA WebVPN: code enhancement in ifs_read() in read_file_header()
CSCtl44287	Routing:Traceback observed on standby unit when exec clear conf all
CSCtl86521	IKEv2:Sometimes tunnels in Standby unit will be automatically deleted
CSCtn69856	ASA 5585-X : 1550 byte block depletion in ctm_frag_list
CSCtn72884	IKEv2 - ASA to IOS cert based fails - Interop Issue
CSCto32012	Routing: page fault traceback in Thread Name: EIGRP-IPv4: PDM
CSCto45855	ASA: IPSec RA directed DNS requests sent to different server
CSCto59377	Traceback in Thread Name: DATAPATH-6-2319
CSCto84108	ASA generated ICMP unreachables show up on wrong interface
CSCto88410	unable to install security rules on NP after same-security-traffic
CSCto88412	Radius Proxy to SDI - AnyConnect prompts for next PASSCODE but shouldn't
CSCtq20634	NAT config line with dynamic NAT and pat-pool fallback rejected
CSCtq43504	ASA: Traceback in SSH thread when removing manual NAT rule
CSCtq47028	ASA: Manual NAT rules are not processed in order
CSCtq58621	ASA 8.4 BGP with encryption with IPv6 through ASA doesn't work
CSCtq58983	'DHCP Client' Interface Mode Commands Not Available
CSCtq88111	object group not cleared when used for pat pool
CSCtq92619	ASA: IPsec P2 is not initiated even though P1 is up
CSCtq94990	Stale context present on active unit after vpn system test against 5585
CSCtr17899	Some legitimate traffic may get denied with ACL optimization
CSCtr24705	Traceback in Thread Name: telnet/ci
CSCtr35503	IPV6 router advertisements dropped by multicontext firewall
CSCtr38739	Link outage in Etherchannel causes interface down and failover
CSCtr44930	Nested obj does not work if contained in src and dst of ACL

Table 11 Open Caveats in ASA Version 8.4 (continued)

Caveat	Description
CSCtr65927	dynamic policy PAT fails with FTP data due to latter staic NAT entry
CSCtr67875	HW accelerator error PKCS1 v1.5 RSA - cert auth fails with certain certs
CSCtr68045	IPv4 packets denied with uRPF on interfaces with IPv6-only interfaces
CSCtr76874	SNMP trap for Power Supply does not generate
CSCtr82247	ASA 5505 8.4.2 traceback
CSCtr84249	False Context memory usage
CSCtr85499	ASA: Radius MS-CHAPV2 with challenge fails
CSCtr92976	ESMTP inspection corrupts data
CSCtr99267	WebVPN KCD: ASA may use incorrect principal name in Kerberos AS-REQ
CSCts11800	Phone proxy phones fail to register through failover ASA
CSCts18480	ASA IKEv1 Traceback in vpnfol_thread_msg ike_fo_create_new_sa on Standby
CSCts28455	ASA-radius passwords with NON-ASCII characters fail after 8.4.2 upgrade
CSCts35498	ICMP and TCP Ping command should honor a timeout of zero seconds
CSCts42362	Message from ASA is not displayed about password complexity requirements
CSCts45189	ASA exhausting DHCP pool when acting as a relay agent for VPN clients
CSCts50056	1st interface of port-channel is in down state when f/o is configured
CSCts50584	ASA may reload with traceback in Thread Name scmd reader thread
CSCts50723	ASA: Builds conn for packets not destined to ASA's MAC in port-channel
CSCts68257	ASA: May crash in Thread Name: Dynamic Filter VC Housekeeper
CSCts86224	ASA 8.4.1 traceback when replacing primary unit in a failover pair
CSCts89806	'Route-Lookup' Option Should be Allowed if One Real Interface is Known
CSCts97375	IPv6 neighbor discovery activity of ASA is slow
CSCts98806	Standby ASA 5585 Reporting Service Card Failure on Signature Update
CSCtt02427	5585 producing 402123 logs and denying AC users w/ aaa failing
CSCtt05491	Connections are not replicated with %ASA-3-210007 on Standby
CSCtt16000	Upto 93% CPU utllization due to spin_lock when traffic is low
CSCtt23255	Overlaping Twice NAT Rules Applied Out of Order
CSCtt29653	ASA may reload with traceback in Thread Name: netfs_thread_init
CSCtt31972	ASA: AC unable enroll to local CA unless tunnel-group-list is enabled
CSCtt45090	ASA5505: Primary active unit may crash after config sync
CSCtt47502	show vpn-sessiondb does not show LZS compression stats for Anyconnect
CSCtt88306	Syslog 106100 not generated on second context when cascading contexts.
CSCtt96195	Adding new object network for a previlige level 13 granted user fails
CSCtt98033	Allow Concurrency of 'Unidirectional' and 'No-Proxy-Arp' Keywords
CSCtt98991	Checksum failed for Decrypted VPN packets going to SSP-IPS
CSCtu10505	ASA: Nested page fault traceback in vpnfol_thread_timer

Table 11 Open Caveats in ASA Version 8.4 (continued)

Caveat	Description
CSCtu15134	ASA: 8.4 Multicontext, Legacy cut through proxy configuration, traceback
CSCtu32847	ASA 8.4(2.1) high memory and crash in aaa_shim_thread
CSCtu34793	ASA 5580 Multicontext ERROR: unable to create listener on interface
CSCtu42594	Traceback in Thread Name fover_parse
CSCtu42663	Traceback in thread name OSPF Router
CSCtu42834	Traceback in dispatch unit due to netflow
CSCtu51799	Traceback in Thread Name: CP Processing
CSCtu96588	HTTP1.1 persistent connections left open and not reused
CSCtv00813	ASA NAT fails to due route look with any as destination interface
CSCtw31001	Unexpected overrun during connection high load test
CSCtw45576	TCP sequence space check ignored in some cases
CSCtw48411	ASA 8.4.2 crash in thread IPsec message handler
CSCtw50424	FTP inspection does not work when using overlapping NAT
CSCtw52332	LU allocate conn failed due to port number 0 in SIP traffic
CSCtw56298	AnyConnect IKEv2 3.0.1047 can't connect if 3.0.4235 loaded on ASA 8.4.2+
CSCtw56859	Natted traffic not getting encrypted after reconfiguring the crypto ACL
CSCtw58682	SSLVPN Portal uses incorrect DNS Group after failover
CSCtw58945	L2TP over IPSec connections fail with ldap authorization and mschapv2
CSCtw59136	ASA: 8.3+ NAT overlap with failover IP cause both units to go active
CSCtw59562	ACL Hashes calculated during config migration are wrong
CSCtw60220	Port Address Translation (PAT) causes higher CPU after upgrade
CSCtw62745	Inspection configurations do not appear after disk format and reload
CSCtw63996	Page fault traceback with thread name "pix_flash_config_thread".
CSCtw66453	Certificate request is not sent when connecting via AC
CSCtw68023	ASA Traceback in Thread Name PIX Garbage Collector
CSCtw69488	IPv6 Neighbor information is not synced to Standby after failover
CSCtw71829	ASA: 8.4 traceback while modifying WebType ACL
CSCtw78415	ASA may reload with traceback in Dispatch Unit related to WAAS inspect
CSCtw79213	ASA 5585 traceback in thread ci/console when adding a BVI int
CSCtw82147	ASA lets static NAT mapped IP to be same as standby address on interface
CSCtw82573	Failover monitor may unexpectedly become Unknown (Waiting) status.
CSCtw82612	capture trace detail unreliable when TX queue is oversubscribed
CSCtw82904	ESP packet drop due to failed anti-replay checking after HA failovered
CSCtw84007	ASA does not recognize IPv6 VPN filter access-list for AnyConnect client
CSCtw84249	ASA 8.4 Email Proxy causes corruption of some email attachments
CSCtw90005	ASA 8.4.2(16) traceback in thread fover_parse

Table 11 Open Caveats in ASA Version 8.4 (continued)

Caveat	Description
CSCtw90179	ASA:In a rare corner case ASA may crash while modifying FQDN object/acl
CSCtw92877	ASDM may not pull up the stats for mem, cpu and simply say "Please wait"
CSCtw93804	CPU-HOG is detected after configuring speed 10/100,duplex full on MGMT
CSCtw95487	ASA memory leak from failed EZVPN cert auth while parsing OU
CSCtw97279	WebVPN: RE: corrupted CPS files with user information storage enabled
CSCtx01251	ASA: May traceback in DATAPATH during capture
CSCtx02122	Post request for OCSP using non default port is missing the port number
CSCtx02241	ASA (8.4.2.8) : traceback in thread SSL
CSCtx03901	1550 byte block leak in socks_proxy_datarelay
CSCtx05052	ASA 8.4.2 Crash - Thread Name: EIGRP-IPv4: PDM, eip subnet_lookup_inline
CSCtx08182	Nas-Port attribute different for authentication and accounting
CSCtx08310	ASA stops responding to management traffic
CSCtx08346	Dissimilar behavior for Group URL precedence via browser or AC Client
CSCtx12834	%ASA-3-210007: LU allocate xlate failed
CSCtx13772	IPv6 EIGRP pass through not working in transparent mode ASA 8.4.2
CSCtx16166	ASA may not log syslogs 611101, 605005 for asdm sessions to certain int
CSCtx18026	PAT Pool exhaustion log
CSCtx20108	TCP conns between ASA and Websense server disappear over lossy link
CSCtx21383	Traceback in DATAPATH thread: Abort with unknown rason

Resolved Caveats

This section includes the following topics:

- Resolved Caveats in Version 8.4(3), page 31
- Resolved Caveats in Version 8.4(2), page 38
- Resolved Caveats in Version 8.4(1), page 42

Note For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Resolved Caveats in Version 8.4(3)

Table 12 contains resolved caveats in ASA software Version 8.4(3).

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

http://tools.cisco.com/Support/BugToolkit/

Table 12 Resolved Caveats in ASA Version 8.4(3)

Caveat	Description
CSCsi29725	SIP: options/update_handler do not open pinhole for response
CSCsy68961	ASA 5580 reboots with traceback in threat detection
CSCta94935	show failover shows incorrect interface status when Standby powered off
CSCtc79873	ASA 8.2 may calculate memory usage incorrectly
CSCtc95264	ASA Increase LDAP & DAP max instances per attribute > 999
CSCtd73605	ASA RIP: "no redistribute static" breaks "default-information originate"
CSCtd73901	Linkdown, Coldstart SNMP Traps not sent with certain snmp-server config
CSCte01475	EIGRP : static route redistribution with distribute-list not working
CSCte08816	ASA NAT: LU allocate xlate failed error with Twice NAT
CSCtf09840	ENH: Enable Flow Control (Sending Pause Frames) on 1GE Interfaces
CSCtf51346	ASA may leave connection in half-closed state
CSCtg06320	DHCP ACK not sent by the firewall.
CSCtg76404	Traceback in Thread Name: Checkheaps due to logging
CSCth14248	ASA not sending all logging messages via TCP logging
CSCth34278	Clientless WebVPN Memory Leak Causes Blank Page after Authentication
CSCth37641	Write Mem on active ASA 8.3 produces log 742004 on standby
CSCth40316	Unable to edit the privilege level for cmd object & object-group in 8.3
CSCth48476	ASA WebVPN doesnt rewrite URL Encoded Data in Location Response Header
CSCth58048	Assert Failure caused Traceback in Thread Name: Dispatch Unit
CSCth77370	IPv6 : ASA Stops responding to IPv6 ND sollicitation
CSCth96829	IPv6 ACL Allowing IPv4 Addresses
CSCti10186	ASA 8.0.5.9 Standby with a traceback in Thread Name:Checkheaps
CSCti11757	SNMP: ASA responds after two SNMP requests
CSCti16604	ASA fails to delete an existing object in object-group
CSCti29274	Cannot switchover member with two 10G interfaces redundant interface
CSCti54387	ASA 8.2.2.x traceback in Thread Name: Dispatch Unit
CSCti54545	EIGRP metrics will not update properly on ASA
CSCti62667	Connections stay open w/ 'sysopt connection timewait' & NetFlow
CSCtj20724	ASA hitless upgrade from 8.2 to 8.3: upgraded unit reload upon conf sync
CSCtj32735	DAP: Change error message when adding non supported IPv6 or standard ACL

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCtj76066	L2TPOverIPsecOverNatT public IP displayed in reverse octet order
CSCtj80580	ASA route-map doesn't have correct set metric statement for EIGRP
CSCtk07521	ASA slow response to autocomplete word host in cmd "network-object host"
CSCtk09626	traceback in AAA eip AAA_BindServer+118 during AC connection
CSCtk19285	ASA H323 allow unidirectional OpenLogicalChannel media through
CSCtk84288	Syslog %ASA-7-108006 generated erroneously
CSCtk93754	Change in Layered Object Group Does Not Update NAT Table
CSCtk98431	Slow xlate expiration rate
CSCtl06156	NAT Xlate idle timer doesn't reset with Conn.
CSCtl21765	Cut-through Proxy - Inactive users unable to log out
CSCtl22195	ASA CLI split dns should warn that AnyConnect supports ten (10) entries
CSCtl23397	ASA may log negative values for Per-client conn limit exceeded messg
CSCtl41335	ASA traceback when layer-2 adjacent TCP syslog server is unavailable
CSCtl54580	Telnet connection is permitted inappropriately in some situation
CSCtl86184	ASA 8.2 flow control might not work for redundant interfaces
CSCtl93641	ASA: Traceback in fover_parse thread after making NAT changes
CSCtl93907	TCP state bypass flags shown as "b" and "-b"
CSCtn00318	ASA Unexpectedly Reloads with a Traceback due to a Watchdog Failure
CSCtn09117	ASA 8.2.4 402126: CRYPTO: The ASA created Crypto Archive File
CSCtn14091	ASA reuses tcp port too quickly
CSCtn38474	Interface warning on ASA - install the interface in a PCI-e x"nn" slot
CSCtn38584	the packet is discarded when the specific xlate is exist.
CSCtn41118	ASA fails over under intensive single-flow traffic
CSCtn48877	Traceback in fover_FSM_thread with IPv6 failover on SSM-4GE-INC
CSCtn56501	ASA 8.2 Crypto Engine Tracebacks Multiple Times
CSCtn60457	ASA 8.4.1 traceback on thread name ldap_client_thread with kerberos
CSCtn66992	egress ACL packet drops erroneously counted on ingress interface
CSCtn74485	ASA5580 traceback in DATAPATH-7-1353
CSCtn74652	Search query timeout/errors in SAP purchasing portal via clientless
CSCtn77962	Tmatch: Traceback on Primary when adding User Group based ACL
CSCtn93345	ASA Broadview deny lines in NAT exemption ACL are migrated as permits
CSCtn96679	IPv6 HA: Standby uses same Link-Local as ACTIVE if standby IP not cfg'd
CSCtn99124	Dynamic Filter DNS Snooping Database size too small
CSCtn99416	WebVPN: Dropdown menu doesn't work in customized SharePoint 2010
CSCto05449	WebVPN:Ability to configure and show session timer countdown on portal
CSCto06207	ASA 8.4.1 traceback in Thread UserFromCert

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCto08497	ASA: dynamic-filter database update may trigger cpu-hogs
CSCto08752	ASA traceback in 8.4.1 with memory failure errors on IKE daemon
CSCto11365	ASA: Ldap attributes not returned for disabled account
CSCto16917	DAP terminate msg not showing for clientless, cert only authentication
CSCto23149	Standby ASA sends out IPv6 RA when IPv6 address is configured.
CSCto31425	ASA: L2TP and NAT-T overhead not included in fragmentation calculation
CSCto34150	ASA SMR - multicast packets no longer forwarded upon interface failure
CSCto34573	ASA: 8.3 upgrade to 8.4, Shared VPN Licensing config lost unable to conf
CSCto34823	multicast packets dropped in the first second after session creation
CSCto42990	ASA fails to process the OCSP response resulting in the check failure
CSCto43075	'help clock' output needs to reflect usage of command better
CSCto49160	can not access cifs folder with japanese character
CSCto49472	ASA running 8.4.1 does not detect external flash, needs a reload
CSCto50936	SAP Portal - Event Tracking Script fails to display correclty
CSCto53199	Traceback with phone-proxy Thread Name: Dispatch Unit
CSCto62660	ASA 8.4.1 traceback in Thread Name: Unicorn Proxy Thread
CSCto63702	ASA's ARP table will populate with non connected subnets
CSCto67979	ASA with SSM - specifying "sensor vs0" breaks ASA<->IPS configuration
CSCto73569	ASA WebVPN clientless not possible to access ipv6 services on the inside
CSCto76621	FO cluster lic doesnt work if primary reboots while secondary is down
CSCto76775	ASA AC failure due to slow memory leak: "Lua runtime: not enough memory"
CSCto80254	ASA does not send Anyconnect profile when Radius pushes profile
CSCto81636	IPv6 traffic not updated after neighbor changes
CSCto82315	Traceback in Thread Name: gtp ha bulk sync with failover config
CSCto83156	ASA Sequence of ACL changes when changing host IP of object network
CSCto87589	Access-list remarks are lost during migration to 8.3
CSCto87674	ST not injected in mstsc.exe on 32-bit Win 7 when started through TSWeb
CSCto89607	ASA sends invalid XML when tunnel-group name contains &
CSCto96832	Unable to login to SAP application via WebVPN portal
CSCto99389	External Portal Page Macro substitution fails
CSCtq00144	VPN RA session DAP processing fails with memberOf from OpenLDAP
CSCtq07658	ASA: Traceback in ci/console on Standby unit
CSCtq08208	ISAKMP dropped after boot if ASA doesn't have IP address while booting
CSCtq10528	Host listed in object group TD shun exception gest shunned
CSCtq10654	Threat-detecton stats showing incorrect output
CSCtq12037	WebVPN : bytes lost in ftp uploading using IE via smart tunnel

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCtq13070	DAP VPN-Filter Not Applied When AC Initiated Through Weblaunch
CSCtq15197	WebVPN:flv file within the Flowplayer object is not mangled correctly
CSCtq19611	IPSec - Error message trying to reserve UDP port in Multicontext mod
CSCtq21535	ASA traceback when connecting with Android L2TP/IPsec client
CSCtq27530	Java RDP plugin doesn't work with sslv3 on ASAs
CSCtq27873	AC can not connect to the ASA if the no. of group aliases is >190
CSCtq28561	asa 8.4, failover , ospf routing can not update rightly.
CSCtq30051	ASA5580: Mate ASA5580 card in slot 0 is different from mine ASA5580
CSCtq30094	CSD scan happens for SSL VPN when connecting via group alias
CSCtq33081	Traceback during certificate operation in IKEv2 EAP processing
CSCtq34233	ASA traceback in thread emweb/https
CSCtq35045	HA: Monitored interfaces fail to move out of waiting state
CSCtq37772	asa 8.2(2) traceback with TN : Unicorn Proxy Thread
CSCtq40553	Unable to remove trustpoint - ERROR: The trustpoint appears to be in use
CSCtq42954	ASA calculates ACL hash inorrectly
CSCtq45177	1550 or 2048 byte block leak due to originate-only keyword in crypto map
CSCtq46808	ASA rebooted unit always become active on failover setup
CSCtq50523	Using non-ASCII chars in interf desc makes the ASA reload with no config
CSCtq52342	OWA 2007 via WebVPN Sessions fail to get notifications of new emails
CSCtq57642	Cannot point IPv6 route to a link-local that matches other intf
CSCtq57752	ASA: IPSec outbound SA data lifetime rekey fails
CSCtq58884	AC 3.0x - LDAP Secondary Auth successfully connects with blank password
CSCtq60450	Degraded Xlate Teardown Performance
CSCtq62572	Webvpn/mus memory leak observed in 8.4.1.63
CSCtq65262	ASA: SSH sessions return extra characters when using CR+LF
CSCtq65479	IKEv2 - ASA does not send intermediate certs for server cert
CSCtq67230	IKEv2 DPD is sent at an interval not correlating to the specified value
CSCtq70326	Interface "description" command allows for more than 200 characters.
CSCtq72776	ASA may reload in threadname Dispatch unit
CSCtq73340	After the interface IP is changed, ASA does not allow UDP 500 to new IP
CSCtq75817	Oracle Jinitiator over WebVPN sends incorrect HTTP request
CSCtq78280	invalid command dhcp client xxx on ASA 8.4
CSCtq79834	ASA traceback due to dcerpc inspection.
CSCtq84364	High CPU and Orphaned SSH session for on ASA 8.3(2.8)
CSCtq84759	ASA wont take "ip audit info action alarm" under "crypto ca" subcommand
CSCtq86859	Traceback in Thread Name: IP SLA Mon Event Processor

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCtq90084	ASA traceback in thread Dispatch Unit
CSCtq94775	Unable to get block detail about 2048 byte blocks
CSCtq96332	ASA 5505 logs "INVALID_NICNUM" messages to console
CSCtq96616	ASA - LU allocate connection failed with conn-max policy
CSCtq97430	Coverity 100595: FORWARD_NULL in ppp_auth_process_attributes()
CSCtr00315	Active SSH connection orphaned if 'clear config all' is run
CSCtr00526	L2TP over IPSec session fails after IPSec P2 rekey
CSCtr03453	Zimbra email suite not usable through WebVPN
CSCtr03856	Failure to migrate named interfaces in ctx to 8.4 bridge group syntax
CSCtr12176	L2L - IPSEC Backup- Peer list is not rotated/cycled with dual failure
CSCtr12333	Webvpn portal contents disappear once bookmark user-storage is enabled
CSCtr14920	lightview based Modal Elements do not work with webvpn
CSCtr15722	Memory fragmentation issue with dscp
CSCtr16184	To-the-box traffic fails from hosts over vpn after upgrade to 8.4.2
CSCtr20809	ICMP inspection permits echo-reply packets with code set to non-zero
CSCtr23854	traceback in Crypto CA during multiple ocsp requests
CSCtr23914	ASA: Certificate renewal from same CA breaks SSLVPN
CSCtr26724	ASA threat detection does not show multicast sender IP in statistics
CSCtr27000	ASA fails to send Radius attribute 8 framed IP address for IKEv2
CSCtr27161	EIGRP 'no default-information in' does not work
CSCtr33228	Traceback in Dispatch Unit when replicating xlates to standby
CSCtr36022	Java AJAX session does not work over SSLVPN
CSCtr39013	ASA - panic traceback when issuing show route interface_name
CSCtr44913	ASA 5580 traceback with DATAPATH-2-1024 thread
CSCtr47517	Protocol-Independent Multicast Denial of Service Vulnerability
CSCtr50413	Clientless webvpn remove forward slash in POST Request-URI
CSCtr55374	ASA: asr-group in TFW A/A FO doesn't rewrite dst MAC for IP fragments
CSCtr63071	5585 735XXX syslogs reporting wrong id
CSCtr63101	5585 show environment power output unclear
CSCtr63728	ASA reloads with traceback in Thread Name : Dispatch Unit
CSCtr65785	Enabling AC Essentials should logoff webvpn sess automatically
CSCtr66582	Memory leak on ASA 5585-increase of 1% everyday
CSCtr69771	backslash in username for ftp over webvpn changed to semi-colon
CSCtr72514	ASA: Traceback in telnet/ci thread when running 'show webvpn svc'
CSCtr74940	Active ASA traceback Thread: DATAPATH-3-1290, rip spin_lock_get_actual
CSCtr74983	ASA LDAP support for searching with value range retrieval

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCtr78703	ASA 8.4.2 http inspection might break certain flows intermittently
CSCtr80605	ASA5580 traceback with Thread name telnet/ci
CSCtr83349	ASA logs "INVALID_NICNUM" messages to console
CSCtr91981	LDAP authentication fails when no RootDSE info returned
CSCtr93086	ASA Failover: 106017 Deny IP due to Land Attack on Normal(Waiting) ifc
CSCtr93621	Show resource usage displays wrong Conns Limit for ASA5580-20
CSCtr94429	ASA: Local-host and all conns are torn down when client hits conn limit
CSCtr96686	Java RDP plugin traceback when using empty user in URL to Win2008 server
CSCtr99598	ASA doesn't classify MIME type correctly for .exe and .dmg in Firefox
CSCts00158	ASA EIGRP route not updated after failover
CSCts07069	ASA: Packet classifier fails with 'any' in Object NAT rule
CSCts07650	Traceback in "clear config all" when active telnet connection exists
CSCts09257	Traceback in sch_dispatcher thread
CSCts10797	Webvpn :Support for XFRAME: DENY option in portal
CSCts10887	ASA sends Server Identifier field in DHCP REQUESTS duirng renewal
CSCts13848	ASA may crash in dns_process
CSCts14130	100% CPU Object Group Search under low traffic due to spin_lock
CSCts15920	ASA: WCCP with authentication fails in 8.3 and 8.4
CSCts18026	ASA 5520 8.2.5 : traceback at thread name snmp
CSCts24804	ASA 5580 DAP Network ACL Errors:user, user-group or FQDN objects
CSCts26909	CPU spikes to 100% and causes traceback when Syslog interface is down
CSCts30839	ASA5510, 8.4(2) - page fault traceback accessing a bookmarked DFS share
CSCts32313	ASA 8.4(1) - mailto for xmpp protocol mail clients fails
CSCts32474	Incorrect time displayed on cut through proxy auth page
CSCts33551	NAT-T compatibility improvement with Windows 7
CSCts35339	Close non-persistent CSD conns
CSCts36777	Manual Redundant Failover Link Switchover Causes a Flap
CSCts41215	NAC Framework - Status Query triggers full Posture Revalidation
CSCts43136	ESMTP drops email with DKIM header
CSCts45638	8.4.2.2: Thread Name: DATAPATH-0-1272 Page fault: Unknown
CSCts46366	Slow memory leak by skinny
CSCts48937	Memory leak in DP udp host logging resulting in 1550 byte blocks leak
CSCts52885	Unexpected packet denials during large ACL compilation
CSCts54522	Inspect PPTP does not change CALL-id for inbound Set-Link-Info Packet
CSCts61811	idfw_nb_process traceback because thread stack appears corrupt
CSCts64849	ASA: 8.3/8.4 no longer logs %ASA-3-713167 syslog for rejected user

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCts68268	PIX-ASA: Route command should validate next hop IP before accepting
CSCts69531	Traceback in Dispatch Unit on Standby with timeout floating-conn
CSCts72339	L2 table entried for identity i/f not handle properly when add/del i/f
CSCts76258	xlate objects with no associated conns and idle timer > timeout
CSCts80367	AnyConnect 3.0 for Mac gets "Certificate Validation Failure" w/ ASA 8.4
CSCtt00286	ASA5585 Page fault traceback in Thread Name: DATAPATH-5-2312
CSCtt02123	WebVPN: Multiple tracebacks seen in WebVPN in Unicorn Proxy thread
CSCtt02413	DCERPC inspection does not properly fix up port and IP in Map Response
CSCtt02423	ASA: May traceback when adding ipv6 route before enabling ipv6
CSCtt03480	ASA Radius User-Password attribute is not included in Access-Request
CSCtt04614	webvpn - ES keyboard diacritics incorrectly managed by RDP plugin
CSCtt04665	Traceback in Thread Name: IP Address Assign
CSCtt07749	ASA is responding to IKE request when in vpnclient mode
CSCtt11835	Traceback in Thread Name: tacplus_snd
CSCtt14922	ASA5585: Redundant interface doesn't switchover on IPS module shutdown
CSCtt18185	ASA traceback cause by Global Policy
CSCtt19760	ASA may traceback in a DATAPATH thread
CSCtt22540	Secondary Auth successfully connects with blank password
CSCtt25173	ASA 5520 8.2.5 memory leak in the inspect/gtp area
CSCtt27599	Standby Firewall traceback citing nat_remove_policy_from_np+383
CSCtt29654	Outbound IPsec traffic interruption after successful Phase2 rekey
CSCtt29810	AAA Command Authorization Reactivates Failed Server on Every Attempt
CSCtt32565	Specific closing sequence may cause ESMTP inspect to hog CPU for 1+ sec
CSCtt34959	ASA and apple L2TP IPSec client disconnects
CSCtt36737	After upgrade, AnyConnect causes 1550 or 2048 block depletion
CSCtt41809	ASASM traceback in DATAPATH-3-2265
CSCtt42405	AnyConnect fails authentication for some passwords with brackets
CSCtt45496	ASA traceback in thread ci/console with names > 48 char in prefix-list
CSCtt96550	ASA - Dispatch unit traceback - snp_nat_xlate_timeout
CSCtu02060	Changing IPv4 FQDN network object to IPv6 FQDN causes traceback
CSCtu07278	Corrupted route-map output for 'config' URL used by ASDM
CSCtu10620	WebVPN:flv file within the Flowplayer object is not played over webvpn
CSCtu19300	ASA may reload with traceback in Thread Name: kerberos_recv
CSCtu25253	'show shared license' after toggle license-server crashed ASA
CSCtu33068	WebVPN URL Mangler does not handle encoded value of "&#47"
CSCtu34217	High CPU usage during bulk sync on spin_lock used by tmatch lookup

Table 12 Resolved Caveats in ASA Version 8.4(3) (continued)

Caveat	Description
CSCtu34220	High CPU usage during bulk sync when allocating NAT xlate
CSCtu40752	5580: assert failure in thread CP Processing
CSCtu43137	ASA traceback in Thread Name: IKE Daemon
CSCtw35765	Thread Detection Denial Of Service Vulnerability
CSCtw81408	Apple Lion OS L2TP Client behind NAT device does not connect

Resolved Caveats in Version 8.4(2)

Table 13 contains resolved caveats in ASA software Version 8.4(2).

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

http://tools.cisco.com/Support/BugToolkit/

Table 13 Resolved Caveats in ASA Version 8.4(2)

Caveat	Description
CSCsg26647	CS: undebug all command doesn't disable debug crypto ca server
CSCsy19222	Conns should update when using dynamic protocol and floating statics
CSCsy93944	Traceback on ACL modify: assertion "status" at "stride_terminal_node.c"
CSCtb63515	Clientless webvpn on ASA cannot save .html attached file with IE6 OWA
CSCtd73901	Linkdown, Coldstart SNMP Traps not sent with certain snmp-server config
CSCte08816	ASA NAT: LU allocate xlate failed error
CSCte76002	Low performance over shared vlans in multi-mode
CSCtf96635	Removing HTTP server caused page fault traceback
CSCtg41691	dynamic-filter database update triggers cpu-hog
CSCtg50770	Mngt-access (ASDM,SSH) to inside intf of 5580 fails over RA VPN session
CSCtg99798	ASA Traceback in Thread Name: snmp / checkheaps
CSCth08903	WebVPN: "Invalid Canary" error for different options in OWA 2010
CSCth08965	WebVPN: Bad performance on Internet Explorer 8 for OWA 2010 Premium
CSCth12612	ASA - VPN load balancing is disabled after failover
CSCth35722	WebVPN CIFS: 'Authentication error', when DFS host is not reachable
CSCth35961	WebVPN: Preview mode for emails works improperly for DWA 8.5.1
CSCth77370	IPv6 : ASA Stops responding to IPv6 ND sollicitation
CSCth81601	ASA tracebacks in Thread Name: Dispatch Unit
CSCth84519	PIM packet with own source address seen after failover on standby peer
CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently
CSCti11757	SNMP: ASA responds after two SNMP requests
CSCti13482	BG: Same MAC-address not allowed in two different bridge groups

Table 13 Resolved Caveats in ASA Version 8.4(2) (continued)

Caveat	Description
CSCti16604	ASA fails to delete an existing object in object-group
CSCti26874	Control-plane feature not working for https traffic to-the-box
CSCti34213	The file name is garbled as downloading through SSLVPN and CIFS.
CSCti54545	EIGRP metrics will not update properly on ASA
CSCti88463	WebVPN: Empty emails content for OWA 2010 through Firefox
CSCti89628	ARP table not updated by failover when interface is down on standby
CSCtj14005	Traceback with thread name netfs_thread_init
CSCtj16627	DAP:Control access of AnyConnect Apple iOS Mobile without CSD
CSCtj20691	ASA traceback when using a file management on ASDM
CSCtj25717	CPU Hog in "NIC status poll" when failing over redundant intf members
CSCtj29076	ASR trans FW rewrites wrong dst. MAC when FO peers active on same ASA
CSCtj37404	Traceback in mmp inspection when connecting using CUMA proxy feature.
CSCtj45688	ASA: SYN may change close-wait conn to SYN state
CSCtj47335	Problems with Intranet Page displaying when defined as Home Page w/ASA
CSCtj48788	Page fault traceback on standby in QOS metrics during idb_get_ifc_stats
CSCtj50580	ASA - VPN outbound traffic stalling intermittently after phase 2 rekey
CSCtj55822	ASA webvpn; certain ASP elements may fail to load/display properly
CSCtj58420	Failed to update IPSec failover runtime data on the standby unit
CSCtj62266	ldap-password-management fails if user password contained & (ampersand)
CSCtj73930	IPSec/TCP fails due to corrupt SYN ACK from ASA when SYN has TCP option
CSCtj77222	WebVPN: ASA fails to save HTTP basic authentication credential
CSCtj77909	ASA: multiple rules in Name Contraints certificate extension fails
CSCtj78200	certificate name contraints parsing fails when encoding is IA5String
CSCtj78425	Customers Application HQMS being broken by Webvpn Rewriter
CSCtj79795	WebVPN:flv file within the Flowplayer object is not played over webvpn
CSCtj83995	ASA - no names applied to the config when refreshing the config on ASDM
CSCtj84665	Primary stays in Failed state while all interfaces are up
CSCtj85005	ASA as EasyVPN Client failure on WAN IP Change when using 'mac-exempt'
CSCtj90315	Traceback in transparent mode due to tcp reset
CSCtj93922	Standby unit sends ARP request with Active MAC during config sync
CSCtj95695	Webvpn: Java-Trustpoint cmd error, doesn't accept MS code-signing cert
CSCtj96108	Group enumeration possible on ASA
CSCtj97800	a space inserted behind video port number after SIP inspect with PAT on
CSCtk00068	Watchdog timeout traceback following "show route"
CSCtk04293	Webvpn, SSO with Radius, CSCO_WEBVPN_PASSWORD rewritten with OTP, 8.3

Table 13 Resolved Caveats in ASA Version 8.4(2) (continued)

Caveat	Description
CSCtk10185	OWA login page strip "\" from "domain\username"
CSCtk10911	HA replication code stuck - "Unable to sync configuration from Active"
CSCtk12556	timeout command for LDAP in aaa-server section doesn't work
CSCtk12864	Memory leak in occam new arena
CSCtk15258	ASA traceback in Thread Name:radius_rcv_auth
CSCtk15538	IKE Session : Cumulative Tunnel count always shows Zero
CSCtk34526	SSH processes stuck in ssh_init state
CSCtk54282	Webvpn memory pool may report negative values in "% of current" field.
CSCtk61257	ASA locks up port with mus server command
CSCtk62536	WebVPN incorrectly rewrite logout link of Epic app through Firefox
CSCtk63515	MUS debugs are running with no mus configured
CSCtk84716	IKE proposal for L2TP over IPSec global IKE entry match is duplicated
CSCtk95435	ASA rewriter: radcontrols based AJAX/ASP website not working properly
CSCtk96848	snmpwalk for crasLocalAddress reports: No Such Instance currently exists
CSCtl05205	Error entering object group with similar name as network object
CSCtl06889	Failover interface monitoring only works with the first ten interfaces.
CSCtl09314	"clear conn" behaviour is inconsistent with "show conn"
CSCtl10398	Traceback in Dispatch Unit due to dcerpc inspection
CSCtl10877	ASA reload in thread name rtcli when removing a plugin
CSCtl17877	SSL handshake - no certificate for uauth users after 8.2.3 upgrade
CSCtl18462	ASA not posting correct link with Protegent Surveillance application
CSCtl20963	DAP ACL in L2TP doesn't get applied after successful connection
CSCtl20966	The javascript is truncated when accessing via WebVPN portan on ASA
CSCtl21314	vpn-filter removed incorrectly from ASP table with EzVPN hw clients
CSCtl21765	Cut-through Proxy - Inactive users unable to log out
CSCtl51919	ASA 8.3 with Static NAT - passes traffic with translated IP in the acl
CSCtl54976	Redundant switchover occurs simultaneously on failover pair
CSCtl56719	Default "username-from-certificate CN OU" doesn't work after reload
CSCtl57784	ASA TCP sending window 700B causing CSM deployment over WAN slow
CSCtl58069	ASA - Traceback in thread DATAPATH-6-1330
CSCtl66155	Invalid internal Phone Proxy trustpoint names generated by imported CTL
CSCtl66339	Traceback in DATAPATH-2-1361, eip snp_fp_punt_block_free_cleanup
CSCtl72355	ASA WEBVPN: POST plugin - Can not find server .plugins. or DNS error
CSCtl74435	VPN ports not removed from PAT pool
CSCtl86372	IKE fails to initialize when minimal data is sent to pub int.
CSCtl87114	'show mem' reports erroneous usage in a virtual context

Table 13 Resolved Caveats in ASA Version 8.4(2) (continued)

Caveat	Description
CSCtl95958	Timeout needs twice time of configured timeout for LDAP in aaa-server
CSCtn01794	IPv6 ping fails when ping command includes interface name.
CSCtn02684	ASA SAP purchasing app may display incorrectly over webvpn
CSCtn07431	L2L IPv6 tunnel with failover not supported Syslog Broken
CSCtn08326	ESMTP Inspection Incorrectly Detects End of Data
CSCtn09117	ASA 8.2.4 402126: CRYPTO: The ASA created Crypto Archive File
CSCtn11061	ASA 5520 traceback in thread emweb/https
CSCtn20148	EIGRP default-route is not displayed w/ "ip default-route" route removed
CSCtn25702	URLs in Hidden Input Fields not Rewritten Across WebVPN
CSCtn27365	ASDM causes traceback during context creation
CSCtn40210	FTP transfer fails on Standby ASA - uses wrong IP add. in PORT command
CSCtn41118	ASA fails over under intensive single-flow traffic
CSCtn42704	One-to-many NAT with "any" interface not working with PPTP and FTP
CSCtn53896	ASA: police command with exceed-action permit will not replicate to Stby
CSCtn57080	Bookmark macro in post parameters is not replaced with correct user/pass
CSCtn60457	ASA 8.4.1 traceback on thread name ldap_client_thread with kerberos
CSCtn61148	ASA stops handling ikev2 sessions after some time
CSCtn65995	ASA(8.3) adds a trailing space to the object name and the description
CSCtn69941	VPN ports not removed from PAT pool (UDP cases)
CSCtn74649	BTF DNS-Snooping TTL maxes out at 24 hours, less than actual TTL
CSCtn74652	Search query timeout/errors in SAP purchasing portal via clientless
CSCtn75476	ASA Traceback in Thread Name: snmp
CSCtn79449	Traceback: Thread Name: DATAPATH-3-1276
CSCtn80637	"Clear conf all" reboots ASA with EIGRP authentication key configuraiton
CSCtn80920	LDAP Authorization doesn't block AccountExpired VPN RA user session
CSCtn84047	ASA: override-account-disable does not work without password-management
CSCtn84312	AnyConnect DTLS Handshake failure during rekey causes packet loss
CSCtn89300	ASA: Memory leak in PKI CRL
CSCtn90643	Traceback while replicating xlates on standby
CSCtn93052	WebVPN: Office WebApps don't work for SharePoint 2010 in IE
CSCtn93345	ASA Broadview deny lines in NAT exemption ACL are migrated as permits
CSCtn96841	"ip local pool" incorrectly rejected due to overlap with existing NAT
CSCtn99847	Easy VPN authentication may consume AAA resources over time
CSCto05036	DTLS handshake fails on ASA when client retransmits ClientHello
CSCto05478	asa traceback on 8.3.2.13 Thread Name: Dispatch Unit
CSCto05640	call-home config auto repopulates after reboot

Table 13 Resolved Caveats in ASA Version 8.4(2) (continued)

Caveat	Description
CSCto08752	ASA traceback in 8.4.1 with memory failure errors on IKE daemon
CSCto09465	FTP transfers fail with NAT configured on multi-core ASAs (5580/5585)
CSCto11365	ASA: Ldap attributes not returned for disabled account
CSCto14043	ASA may traceback when using trace feature in capture
CSCto15003	ASA 8.4.1 traceback in Thread Name: ssh with Page fault
CSCto16917	DAP terminate msg not showing for clientless, cert only authentication
CSCto23713	ASA uses a case-sensitive string compare with IBM LDAP server
CSCto34573	ASA: 8.3 upgrade to 8.4, Shared VPN Licensing config lost unable to conf
CSCto48254	ASA reset TCP socket when RTP/RTCP arrives before SIP 200 OK using PAT
CSCto49499	HA: Failover LU xmit/rcv statistics is different on Active and Standby
CSCto62499	OSPF Failover causes 5 second convergence delay
CSCto62660	ASA 8.4.1 crashed in Thread Name: Unicorn Proxy Thread
CSCto80254	ASA does not send Anyconnect profile when Radius pushes profile
CSCto82315	Traceback in Thread Name: gtp ha bulk sync with failover config
CSCto83156	ASA Sequence of ACL changes when changing host IP of object network
CSCto87674	ST not injected in mstsc.exe on 32-bit Win 7 when started through TSWeb
CSCto96832	Unable to login to SAP application via WebVPN portal
CSCto99389	External Portal Page Macro substitution fails
CSCtq00144	VPN RA session DAP processing fails with memberOf from OpenLDAP
CSCtq10528	Host listed in object group TD shun exception gest shunned

Resolved Caveats in Version 8.4(1)

Table 14 contains resolved caveats in ASA software Version 8.4(1).

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

http://tools.cisco.com/Support/BugToolkit/

:.

Table 14 Resolved Caveats in ASA Version 8.4(1)

Caveat	Description
CSCeg69627	DHCPD: show binding should display client-id instead of hw address
CSCsk97762	ENH: Allow DCERPC inspect to open pin-holes for WMI queries. non epm map
CSCsw15355	ASA may crash when executing packet-tracer via console/ssh/telnet
CSCtc12240	Webvpn- rewrite : ASA inserts lang=VBScript incorrectly
CSCtc32872	TFW ENH: Management interface should operate in routed mode
CSCtc40183	8.2.1.11 Webvpn not able to show dropdowns items written in javascripts
CSCtd02193	Heap memory head magic verification failed on asdm access

Table 14 Resolved Caveats in ASA Version 8.4(1) (continued)

Caveat	Description
CSCtd71913	WebVPN Application Access page not displayed if AES chosen
CSCte55834	sev1 syslog seen after three failed authentication attempts
CSCte79575	ASA: TFW sh fail output shows Normal(waiting) when Sec unit is act
CSCtf01287	SSH to the ASA may fail - ASA may send Reset
CSCtf06303	Citrix plugin error with HTTPBrowserAddress parameter
CSCtf13774	ASA Traceback Thread Name: Dispatch Unit
CSCtf23147	ASA/PIX may generate an ACK packet using TTL received by sender
CSCtf25270	PP: MTA can be replaced with static/dynamic route
CSCtf28466	ASA Fails to assign available addresses from local pool
CSCtf50185	when doing DTLS rekey, AC may get disconnected with reason idle-timeout
CSCtf52903	Wrong url message is generated when access to group-url ended with "/"
CSCtf99449	Traceback in thread name Dispatch Unit
CSCtg09840	debug webvpn response does not generate any output
CSCtg22656	ASA local CA: not redirected to cert download page when user first login
CSCtg31015	EIGRP bandwidth value listed incorrectly for SFP gig link on SSM-4GE
CSCtg41163	ASA:high memory usage seen on ASA version 8.0.x onwards
CSCtg45489	Access List for L2L "show crypt ipsec sa" blank after FO and rekey
CSCtg65421	CIFS SSO fails with non-ASCII characters in username or password
CSCtg66583	RIP denial of service vulnerability
CSCtg74608	WEBVPN: PDF form button doesn't work with secure link
CSCtg78505	Cannot SSH to ASA after making changes to webvpn portal via ASDM
CSCtg80816	Clientless WebVPN: DWA 8.0.2 fails to forward attachments
CSCtg86810	show run all command causes SSH session hang
CSCtg89586	RTSP is not translating the client-ports correctly
CSCtg90646	ASA - webtype ACLs are not replicated to the standby
CSCtg94369	ASA 8.3 reboots after installing memory upgrade and copying file
CSCth06056	CWA doesn't login with IE 7 and IE8 or render properly with FireFox 3.x
CSCth09546	ASA 8.3 cut-through-proxy behavior change when authenticating to ASA ip
CSCth11779	ASA sends invalid XML when group-alias contains &
CSCth24465	show nat command shows incorrect line numbers for NAT config lines
CSCth26474	Inspection triggers block depletion resulting in traffic failure
CSCth28251	ASA:UDP conns not properly reclassified when tunnel bounces
CSCth31814	Changing interface config to dhcp will add AAA cmd and break EasyVPN
CSCth38721	Timer error on console not useful: init with uninitialized master
CSCth42526	ASA:vpn-sessiondb logoff ipaddress <peer> does not clear tunnelled flows
CSCth42839	show conn port functionality change

Table 14 Resolved Caveats in ASA Version 8.4(1) (continued)

Caveat	Description
CSCth43128	ASA WebVPN : Forms don't get saved in CRM due to no pop-up
CSCth48178	ha :Watchdog fover_FSM_thread during failover IPv6 on SSM-4GE-INC
CSCth49826	Traceback in Unicorn Proxy Thread, address not mapped
CSCth56065	DAP_ERROR:...dap_add_csd_data_to_lua: Unable to load Host Scan data:
CSCth60460	"show service-policy inspect <engine>" may leak 16384 bytes per output
CSCth63101	ASA HTTP response splitting on /+CSCOE+/logon.html
CSCth67419	WebVPN - rewriter inteprets "application/pdf" as generic link
CSCth67506	ST not injected in mstsc.exe on 64-bit Win 7 when started through TSWeb
CSCth68948	Memory not released after EZVPN client with cert fails authentication
CSCth72642	NAT on 8.3 fails during RPF check
CSCth75120	ASA 8.3; vpn db; IP information not consistent with previous versions
CSCth79877	ASA traceback due to memory corruption
CSCth85185	WebVPN: DWA 8.0.2 will hung up for message forwarding process
CSCth89217	After failover, CPU-hog and send out ND packet using Secondary MAC
CSCth91572	per-client-max and conn-max does not count half-closed connections
CSCth97330	MS-CHAP-Response generated by ASA has incorrect flags (0x11)
CSCti00289	ASA (8.3.1.9) traceback in Thread Name: DATAPATH-5-1315
CSCti03135	Search using Dojo Toolkit fails across WebVPN with 404 Error
CSCti06385	ASA XSS on /+CSCOE+/portal.html webvpnLang variable
CSCti06749	ASA: Session Cookies not Marked Secure
CSCti09288	crashed Thread Name: lu_rx - gtp_lu_process_pdpmcb_info
CSCti09672	vpn-access-hours does not work if client authenticated by certificate
CSCti16527	WEBVPN: Copying >2 GB files fails through CIFS
CSCti20506	Transparent fw w/ASR group sets dstMAC to other ctx for last ACK for 3WH
CSCti21427	Webvpn Customization, DfltCustomization form-order XML error
CSCti22636	"failover exec standby" TACACS+ authorization failure
CSCti24526	Flood of random IPv6 router advertisements causes high CPU and DoS
CSCti24787	Traceback: watchdog in tmatch_release_actual with large tmatch tree
CSCti26495	NAT portlist with failover enabled triggers tmatch assert
CSCti30663	TS Web AppSharing stops working across WebVPN in 8.3.2
CSCti34942	Changing configuration on FT INT not possible after disabling failover
CSCti35310	ISAKMP Phase 1 failure from Remote->ASA with default Phase 1 Values
CSCti35966	Traceback Thread Name: IKE Daemon Assert
CSCti37845	ASA - failover - packet loss when hw-mod reset of SSM mod in fail-open
CSCti38496	ASA SIP inspection does not rewrite with interface pat
CSCti39571	re-enter ipv6 enable does not bring back RRI routes

Table 14 Resolved Caveats in ASA Version 8.4(1) (continued)

Caveat	Description
CSCti39588	invalid ipv6 RRI routes remains after crypto acl changes
CSCti41422	VPN-Filter rules not being cleared even after all vpn sessions gone.
CSCti42879	ASA Crash in thread Dispatch Unit when executing command alias via https
CSCti43193	webvpn-other: assert crash Thread Name: Unicorn Proxy Thread
CSCti43763	Management connection fail after multiple tries with SNMP connections.
CSCti47991	timed mode does not fallback to LOCAL if all aaa server are FAILED
CSCti49212	interface command on vpn load-balancing should be shown
CSCti56362	ASA/ASDM history shows total SSL VPN sessions for clientless only
CSCti57516	ASA traceback when assigning priv level to mode ldap command "map-value"
CSCti57626	IUA Authentication appears to be broken
CSCti57825	ASA L2L VPN Negative packet encapsulation figures
CSCti62191	ASA traceback in Thread Name: emweb/https when DAP has IPv6 acl on it
CSCti62358	TFW mode regens cert every time 'no ip address' applied to mgmt int
CSCti65237	slow mem leak in ctm_sw_generate_dh_key_pair
CSCti70936	PKI session exhaustion
CSCti72411	ASA 8.2.3 may not accept management connections after failover
CSCti74419	Standby ASA may traceback in IKE Daemon while deleting a tunnel
CSCti76899	rtcli: traceback in rtcli async executor process, eip ci_set_mo
CSCti77545	ASA 5550 8.3.2 crashed in Thread Name: OSPF Router
CSCti87144	L2L traffic recovery fails following intermediary traffic disruption
CSCti88676	ASA Captures will not capture any traffic when match icmp6 is used
CSCti90767	ASA 5505 may traceback when booting with an AIP SSC card installed
CSCti92851	Deleting group-policy removes auto-signon config in other group-policies
CSCti93910	ASA automatically enables the 'service resetoutside' command
CSCti94480	Orphaned SSH sessions and High CPU
CSCti98855	Traceback in IKE Timekeeper
CSCti99476	Email Proxy leaking 80 block w/ each email sent
CSCtj01814	page fault traceback in IKE Daemon
CSCtj03800	Second L2TP session disconnects first one if NATed to the same public IP
CSCtj09945	Host Scan with Blank OU field in personal cert causes DAP to fail
CSCtj15898	ASA webvpn "csco_HTML" may be added to form
CSCtj19221	SYSLOG message 106102 needs to show Username for DAP/vpn-filter
CSCtj28057	Quitting "show controller"command with 'q' degrades firewall performance
CSCtj36804	Cut-through proxy sends wrong accounting stop packets
CSCtj43084	Tmatch insert and remove from datapath via NAT portlist causes crash
CSCtj46900	Last CSD data element is not being loaded into DAP

Table 14 Resolved Caveats in ASA Version 8.4(1) (continued)

Caveat	Description
CSCtj60839	WebVPN vmware view does not work after upgrade to ASA 8.2.3 and 8.3.2
CSCtj62266	ldap-password-management fails if user password contained & (ampersand)
CSCtj68188	Traceback in Thread Name: ldap_client_thread
CSCtj96230	H225 keepaplive ACK is dropped

End-User License Agreement

For information on the end-user license agreement, go to:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

Related Documentation

For additional information on the ASA, see *Navigating the Cisco ASA Series Documentation*:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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