Release Notes for the Cisco ASA 5500-X Series, Version 8.6(x)

Released: February 28, 2012
Update: July 12, 2016

This document contains release information for the Cisco ASA 5500-X software Version 8.6(1).

This document includes the following sections:

Important Notes

- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.

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

System Requirements

Version 8.6.(1) supports only the Cisco ASA 5500-X series, which includes the Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X. This version is not available for the ASA 5585-X.

Table 1 lists information about ASDM, module, and VPN compatibility with the ASA 5500 series.

Table 1 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA Version 8.6 requires ASDM Version 6.6 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
Module applications	For information about module application requirements, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

Released: February 28, 2012

Table 2 lists the new features for ASA Version 8.6(1). This ASA software version is only supported on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Note Version 8.6(1) includes all features in 8.4(2), plus the features listed in this table.

Features added in 8.4(3) are not included in 8.6(1) unless they are explicitly listed in this table.

Table 2 New Features forASA Version 8.6(1)

Feature	Description
Hardware Features	
Support for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.
IPS Features	
Support for the IPS SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the IPS SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. We introduced or modified the following commands: **session**, **show module**, **sw-module**.
Remote Access Features	

Table 2 New Features forASA Version 8.6(1) (continued)

Feature	Description
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.4(3).*
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 8.4(3).*
Clientless SSL 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**. *Also available in Version 8.4(3).*
Multiple Context Mode Features	
Automatic generation of a MAC address prefix	In multiple context mode, the ASA now converts the automatic MAC address generation configuration to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of the interface MAC address. This conversion happens automatically when you reload, or if you reenable MAC address generation. The prefix method of generation provides many benefits, including a better guarantee of unique MAC addresses on a segment. You can view the auto-generated prefix by entering the **show running-config mac-address** command. If you want to change the prefix, you can reconfigure the feature with a custom prefix. The legacy method of MAC address generation is no longer available. **Note** To maintain hitless upgrade for failover pairs, the ASA does *not* convert the MAC address method in an existing configuration upon a reload if failover is enabled. However, we strongly recommend that you manually change to the prefix method of generation. After upgrading, to use the prefix method of MAC address generation, reenable MAC address generation to use the default prefix. We modified the following command: **mac-address auto**.
AAA Features	

Table 2 New Features forASA Version 8.6(1) (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). *Also available in Version 8.4(3).*
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. *Also available in Version 8.4(3).*
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 8.4(3).*

Upgrading the Software

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

- Viewing Your Current Version, page 4
- Upgrading the Operating System and ASDM Images, page 5
- Installing the IPS Software Module, page 6
- Installing or Upgrading Cisco Secure Desktop, page 6

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/cisco/software/navigator.html

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

```
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:/[path/]filename
```

For example:

```
hostname# copy tftp://10.1.1.1/asa840-4-k8.bin disk0:/asa861-k8.bin
...
hostname# copy tftp://10.1.1.1/asdm-64099.bin disk0:/asdm-661.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 in global configuration mode.

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

For example:

```
hostname(config)# clear configure boot
hostname(config)# boot system disk0:/asa861-k8.bin
```

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

```
hostname(config)# asdm image disk0:/[path/]new_filename
```

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

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

Installing the IPS Software Module

Your ASA typically ships with IPS module software present on Disk0. If the module is not running, however, you need to install the module.

Detailed Steps

Step 1 To view the IPS module software filename in flash memory, enter:.

```
hostname# dir disk0:
```

For example, look for a filename like IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip. Note the filename; you will need this filename later in the procedure.

Step 2 If you need to copy a new image to disk0, download the image from Cisco.com to a TFTP server, and then enter:

```
hostname# copy tftp://server/file_path disk0:/file_path
```

For other server types, see the "Downloading a File" section on page 23.

Step 3 To identify the IPS module software location in disk0, enter the following command:

```
hostname# sw-module module ips recover configure image disk0:file_path
```

For example, using the filename in the example in Step 1, enter:

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

Step 4 To install and load the IPS module software, enter the following command:

```
hostname# sw-module module ips recover boot
```

Step 5 To check the progress of the image transfer and module restart process, enter the following command:

```
hostname# show module ips details
```

The Status field in the output indicates the operational status of the module. A module operating normally shows a status of "Up." While the ASA transfers an application image to the module, the Status field in the output reads "Recover." When the ASA completes the image transfer and restarts the module, the newly transferred image is running.

Installing or Upgrading Cisco Secure Desktop

ASA Version 8.6.(1) requires Cisco Secure Desktop Release 3.2 or later. You do not need to restart the ASA after you install or upgrade Cisco Secure Desktop.

To install or upgrade the Cisco Secure Desktop software, perform the following steps:

Step 1 Download the latest Cisco Secure Desktop package file from the following website:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Install the new image using TFTP:

```
hostname# copy tftp://server[/path]/filename disk0:/[path/]filename
```

Step 3 Enter the following command to access webvpn configuration mode (from global confguration mode):

```
hostname(config)# webvpn
hostname(config-webvpn)#
```

Step 4 To validate the Cisco Secure Desktop distribution package and add it to the running configuration, enter the following command:

```
hostname(config-webvpn)# csd image disk0:/securedesktop_asa_3_2_0_build.pkg
```

Step 5 To enable Cisco Secure Desktop for management and remote user access, use the following command.

```
hostname(config-webvpn)# csd enable
```

Open Caveats

Table 3 contains the open caveats in Version 8.6(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 3 Open Caveats in ASA Version 8.6(1)

DDTS Number	Caveats
CSCtr71193	reload not performed when IPS software module in recover state
CSCts89380	Saleen: ASDM Handler does not support envmon psu power input sensor
CSCtt98015	Saleen: crypto engine archives continuous after license upgrade
CSCtu59747	Saleen: need to wait for 1 minutes before issue show inventory
CSCtv22976	Saleen crashed after negative test against tunnel limit
CSCtv27382	RDP and ICA plug-in issues with Saleen

End-User License Agreement

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

https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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

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