Release Notes for Cisco ASDM, Version 6.6(x)

Released: February 28, 2012
Updated: July 5, 2012

This document contains release information for Cisco ASDM Version 6.6(1) for the Cisco ASA 5500-X series, which includes the Cisco 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.

This document includes the following sections:

Important Notes

Default Shipping Configuration Might Not Allow Access to ASDM

For ASA version 8.6 and ASDM version 6.6, you might have to correct the SSL encryption settings in the ASA's SSL settings to enable access to ASDM.

Note The factory default configuration that you can restore with the **configure factory-default** command is not affected. Only the initial shipping configuration might be affected.

To change SSL encryption settings:

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

```
asa> enable
asa# show running-config ssl
asa# ssl encryption des-sha1
asa# conf t
asa(config)# no ssl encryption des-sha1
asa(config)# ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
```

ASDM Launcher

A change to the ASDM launcher might disrupt ASDM launch capabilities for some users; however, you may use the following workarounds.

In general, we expect that you have the proper file association between JAR files and the Java Runtime Environment. This association is usually created by default when you install the JRE, but there may be scenarios in which you change this association or in which the association does not exist. In these scenarios, the launcher will not launch, or an attempt to launch ASDM may result in another application being launched. If you encounter one of these problems launching, you can choose one of the following three methods to rectify the problem:

- (Recommended) Re-install or upgrade the Java Runtime Environment (JRE).
- Change the application type to open JAR files.
  a. Open the Windows Explorer, and choose **Tools > Folder Options**.
  b. Click the File Types tab, scroll down, and choose **JAR File type**.
  c. Click **Advanced**.
  d. From the Edit File Type dialog box, choose **Open** in the Actions dialog box, and click **Edit**.
  e. Click **Browse**, and navigate to the location of the Java interpreter "javaw.exe"file (typically, C:\Program Files\Java\).
  f. In the Application used to perform action field, modify the field with the following parameters to point to the current JRE installation directory: C:\Program Files\Java\jre6\bin\javaw.exe" -jar "%1" %*
  g. Click **OK** until all dialogs are closed.
- Modify the shortcut target. Right-click the shortcut used to launch the ASDM-IDM launcher, modify the Target field, and prepend the path to the JRE with the -jar parameter.

  For example, change:

  ```
  C:\Program Files (x86)\Cisco Systems\ASDM\asdm-launcher.jar" -Xms64m -Xmx512m
  -Dsun.swing.enableImprovedDragGesture=true -classpath
  lzma.jar;jploader.jar;asdm-launcher.jar;retroweaver-rt-2.0.jar
  ```

  to:

  ```
  C:\Program Files\Java\jre6\bin\javaw.exe" -jar "C:\Program Files (x86)\Cisco
  Systems\ASDM\asdm-launcher.jar" -Xms64m -Xmx512m
  -Dsun.swing.enableImprovedDragGesture=true -classpath
  lzma.jar;jploader.jar;asdm-launcher.jar;retroweaver-rt-2.0.jar
  ```

Maximum Configuration Size

ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory.

To increase the ASDM heap memory size, modify the launcher shortcut by performing the following procedure:

Step 1 Right-click the shortcut for the ASDM-IDM Launcher, and choose **Properties**.

Step 2 Choose the Shortcut tab.

Step 3 In the Target field, change the argument prefixed with "-Xmx" to specify your desired heap size. For example, change it to -Xmx768m for 768 MB or -Xmx1g for 1 GB. For more information about this parameter, see the Oracle document in the following location:
http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/java.html

ASDM Client Operating System and Browser Requirements

Table 1 lists the supported and recommended client operating systems and Java for ASDM.

Table 1 Operating System and Browser Requirements

Operating System	Browser			Sun Java SE Plug-in[1]
	Internet Explorer	Firefox[2]	Safari	
Microsoft Windows (English and Japanese): • 7 • Vista • 2008 Server • XP	6.0 or later[2]	1.5 or later	No support	6.0
Apple Macintosh OS X: • 10.7[3] • 10.6 • 10.5 • 10.4	No support	1.5 or later	2.0 or later	6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	6.0

1. Support for Java 5.0 was removed in ASDM 6.4. Obtain Sun Java updates from java.sun.com.
2. ASDM requires an SSL connection from the browser to the ASA. By default, Internet Explorer on Windows Vista and later and Firefox on all operating systems do not support base encryption (DES) for SSL, and therefore require the ASA to have a strong encryption (3DES/AES) license. For Windows Internet Explorer, you can enable DES as a workaround. See http://support.microsoft.com/kb/929708 for details. For Firefox on any operating system, you can enable the security.ssl3.dhe_dss_des_sha setting as a workaround. See http://kb.mozillazine.org/About:config to learn how to change hidden configuration preferences.
3. 6.4(7) and later. You may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.

ASDM Compatibility

Table 2 lists information about ASDM, module, and VPN compatibility with the ASA 5500-X series.

Table 2 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA Version 8.6(1) requires ASDM Version 6.6. 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

Note ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Similarly, if a feature was added into a maintenance release for an older major or minor version, then the ASDM documentation includes the new feature even though that feature might not be available in all later ASA releases. Please refer to the new features tables to determine when features were added. For the minimum supported version of ASDM for each ASA version, see *Cisco ASA Compatibility*.

New Features in Version 6.6(1)

Note New, changed, and deprecated syslog messages are listed in *Cisco ASA 5500 Series System Log Messages*.

Table 3 lists the new features for ASA Version 8.6(1)/ASDM Version 6.6(1). This ASA software version is only supported on the ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, and ASA 5585-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 3 New Features forASA Version 8.6(1)/ASDM Version 6.6(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 did not modify any screens.
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 8.4(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 modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression. *Also available in Version 8.4(3).*
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 screens: Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Customizations > Add/Edit > Timeout Alerts Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > Add/Edit General *Also available in Version 8.4(3).*
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). ASDM does not support this command; enter the command using the Command Line Tool. *Also available in Version 8.4(3).*

Table 3 New Features forASA Version 8.6(1)/ASDM Version 6.6(1) (continued)

Feature	Description
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*. ASDM does not support this command; enter the command using the Command Line Tool. *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:

Note For CLI procedures, see the ASA release notes.

Viewing Your Current Version

The software version appears on the ASDM home page; view the home page 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.

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.

Step 1 Back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the File > Save Running Configuration options.

Step 2 Choose **Tools > Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The Cisco.com Authentication dialog box appears.

Step 3 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

The Cisco.com Upgrade Wizard appears.

Step 4 Complete the upgrade wizard.

Step 5 For the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA and restart ASDM.

Step 6 Click **Finish** to exit the wizard and save the configuration changes that you made.

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, choose **Tools > File Management**.

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 your computer, and then on the File Management dialog box, choose **File Transfer > Between Local PC and Flash**.

Step 3 Choose **Tools > Command Line Interface**.

Step 4 To identify the IPS module software location in disk0, enter the following command and then click **Send**:

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

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

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

Step 5 To install and load the IPS module software, enter the following command and then click **Send**:

```
sw-module module ips recover boot
```

Step 6 To check the progress of the image transfer and module restart process, enter the following command and then click **Send**:

```
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.

These instructions provide the CLI commands needed to install Secure Desktop. You may, however, prefer to use ASDM. To do so, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup** and click **Help**.

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
```

Unsupported Commands

ASDM supports almost all commands available for the adaptive ASA, but ASDM ignores some commands in an existing configuration. Most of these commands can remain in your configuration; see Tools > Show Commands Ignored by ASDM on Device for more information.

This section includes the following topics:

Ignored and View-Only Commands

Table 4 lists commands that ASDM supports in the configuration when added through the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Table 4 List of Unsupported Commands

Unsupported Commands	ASDM Behavior
capture	Ignored.
coredump	Ignored. This can be configured only using the CLI.
crypto engine large-mod-accel	Ignored.
dhcp-server (tunnel-group name general-attributes)	ASDM only allows one setting for all DHCP servers.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
fips	Ignored.
nat-assigned-to-public-ip	Ignored.
pager	Ignored.
pim accept-register route-map	Ignored. You can configure only the **list** option using ASDM.
prefix-list (supported in 6.4(7) and later)	Ignored if not used in an OSPF area.

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	Ignored.
sysopt nodnsalias	Ignored.

Table 4 List of Unsupported Commands (continued)

Unsupported Commands	ASDM Behavior
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
threat-detection rate	Ignored.

Effects of Unsupported Commands

If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.

Discontinuous Subnet Masks Not Supported

ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Interactive User Commands Not Supported by the ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter "[yes/no]" but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. Choose **Tools > Command Line Interface**.
2. Enter the **crypto key generate rsa** command.

   ASDM generates the default 1024-bit RSA key.
3. Enter the **crypto key generate rsa** command again.

   Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM panes.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

Open Caveats

Table 5 contains open caveats in ASDM software BETA Version 6.6(1).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

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

Table 5 Open Caveats in BETA Version 6.6(1)

Caveat	Description
CSCte75929	ASDM: Upgrade from Cisco.com wizard experiences ghosting on a Macintosh
CSCtq69054	Management Inteface panel should not be listed on ASA NPE -K7 models
CSCtq76917	IPS Home window freezes after trying to get to Details in Sensor Health
CSCtq78816	ASDM IPSec IKEv1 Wizard fails with split-tunnel option
CSCtq84939	Remove redundant Unified Communication panels
CSCtq87726	IDFW: Cannot easily remove primary AD Agent from server group
CSCtq88352	Translation table files are created under disk0 after restore with ASDM
CSCtq95042	FQDN: Cannot configure "expire-entry-timer" and "poll-timer" on ASDM
CSCtr00700	Implement Scripting in AC for CP detection.
CSCtr29271	ASDM doc:VPN monitoring option to easily identify user
CSCtr37439	Newly Created n/w objects and objectgroups not listed in n/w to shun win
CSCtr49362	AC profile saved to flash before config is saved and completed in ASDM
CSCtr54025	Interface flow control CLI is not generated for non-10GE interfaces
CSCtr62524	ASDM forces user to apply changes when switching between sections
CSCtr68540	ASDM-ClientlessVPN-Customization-Applications-All plugins shown to edit
CSCtr80669	Inapplicable fields are shown for EC interfaces
CSCts09430	ASDM: Commands ignored by ASDM
CSCts19466	Saleen platform: Startup wizard & IPS configuration on standby unit
CSCts24145	ASDM Group Policies have duplicate options caused user confusion
CSCts24777	OWA 2010&2007 fail auto sign on using template bookmark
CSCts31190	ASDM does not backup SNMP Community string in startup-config
CSCts40044	ACL remark - inconsistency between packet tracer and ASDM
CSCts79696	No SCEP forwarding url none
CSCts86675	ASDM Startup Wizard does not cleanly exit when resetting config
CSCts96100	ASDM downgrade error: can't delete external portal page post parameters
CSCts96156	ASDM navigation panels missing
CSCtt15676	Navigation to IDM panel can lock up ASDM
CSCtt19636	ASDM on missing the warning for multiple crypto peer

Table 5 Open Caveats in BETA Version 6.6(1) (continued)

Caveat	Description
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCtt44483	Saleen: Unable to edit existing traffic allocation in IPS startup wizard
CSCtt45459	HostScan config is not restored by ASDM.
CSCtt97015	ASDM-IDM launcher cannot connect to DES-only device with Java 7
CSCtu53621	SDM DAP Symantec needs to add both SymantecAV and NortonAV
CSCtw47962	ASDM online help index is incomplete
CSCtw47975	ASDM online help contains duplicate/multiple entries
CSCtw52336	Online help on ASDM for NAT CCB is not available
CSCtw58877	ASDM crypto map view is not showing peer with it's name
CSCtw60293	Apply button is not enabled in Filter Rules & Default Information screen
CSCtw73611	Manage CA server on TLS proxy
CSCtx01016	ASDM: Home screen graphs may show ghost images on Windows and Macintosh
CSCtx10581	ASDM real time logs do not refresh automatically after clearing filter
CSCtx12851	ASDM CRL check in trustpoint does not reflect CLI configuration
CSCtx19886	ASDM-ASA upgrade wizard misleading 6.4.5(206)

End-User License Agreement

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

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

Related Documentation

For additional information about ASDM or its platforms, see *Navigating the Cisco ASA 5500 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.