



Release Notes for Cisco ASDM, Version 6.5(x) for ASASM

Released: July 7, 2011

Updated: June 28, 2013

This document contains release information for Cisco ASDM Version 6.5(x) for the ASA Services Module (ASASM).

This document includes the following sections:

- [Important Notes, page 1](#)
- [ASDM Client Operating System and Browser Requirements, page 2](#)
- [New Features, page 3](#)
- [Upgrading the Software, page 7](#)
- [Unsupported Commands, page 12](#)
- [Open Caveats, page 14](#)
- [Resolved Caveats in Version 6.5\(1.110\), page 15](#)
- [Resolved Caveats in Version 6.5\(1.101\), page 15](#)
- [End-User License Agreement, page 16](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation and Submitting a Service Request, page 16](#)

Important Notes

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.



Americas Headquarters:

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

© 2011 Cisco Systems, Inc. All rights reserved.

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): <ul style="list-style-type: none"> 7 Vista 2008 Server XP 	6.0 or later ²	1.5 or later	No support	6.0
Apple Macintosh OS X: <ul style="list-style-type: none"> 10.7³ 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): <ul style="list-style-type: none"> Desktop Desktop with Workstation 	N/A	1.5 or later	N/A	6.0

- Support for Java 5.0 was removed in ASDM 6.4. Obtain Sun Java updates from java.sun.com.
- ASDM requires an SSL connection from the browser to the ASDM. 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 ASDM 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.
- 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.

New Features

- [New Features in Version 6.5\(1.101\)/ASA 8.5\(1.7\), page 3](#)
- [New Features in Version 6.5\(1\)/ASA 8.5\(1.6\), page 4](#)
- [New Features in Version 6.5\(1\)/8.5\(1\), page 5](#)

New Features in Version 6.5(1.101)/ASA 8.5(1.7)

Released: March 5, 2012

[Table 2](#) lists the new features for ASA interim Version 8.5(1.7)/ASDM Version 6.5(1.101).



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 2 ***New Features for ASA Interim Version 8.5(1.7)/ASDM Version 6.5(1.101)***

Feature	Description
Hardware Features	
Support for the Catalyst 6500 Supervisor 2T	<p>The ASASM now interoperates with the Catalyst 6500 Supervisor 2T. For hardware and software compatibility, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html.</p> <p>Note You may have to upgrade the FPD image on the ASASM. See the Upgrading procedure in the release notes.</p>
Multiple Context Features	
ASDM support for Automatic generation of a MAC address prefix	<p>ASDM now shows that an autogenerated prefix will be used if you do not specify one.</p> <p>We modified the following screen: Configuration > Context Management > Security Contexts</p>

Table 2 ***New Features for ASA Interim Version 8.5(1.7)/ASDM Version 6.5(1.101) (continued)***

Feature	Description
Failover Features	
Configure the connection replication rate during a bulk sync	<p>You can now configure the rate at which the ASASM replicates connections to the standby unit when using stateful failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASASM is 8 million; replicating 8 million connections in 15 seconds means creating 533K connections per second. However, the maximum connections allowed per second is 300K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced.</p> <p>We modified the following screen: Configuration > Device Management > High Availability > Failover.</p>

New Features in Version 6.5(1)/ASA 8.5(1.6)

Released: January 27, 2012

[Table 2](#) lists the new features for ASA interim Version 8.5(1.6)/ASDM Version 6.5(1).



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 3 **New Features for ASA Interim Version 8.5(1.6)/ASDM Version 6.5(1)**

Feature	Description
Multiple Context Features	
Automatic generation of a MAC address prefix	<p>In multiple context mode, the ASASM now converts the automatic MAC address generation configuration to use a default prefix. The ASASM auto-generates the prefix based on the last two bytes of the backplane MAC address. This conversion happens automatically when you reload, or if you reenables MAC address generation. The prefix method of generation provides many benefits, including a better guarantee of unique MAC addresses on a segment. 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.</p> <p>Note To maintain hitless upgrade for failover pairs, the ASASM does <i>not</i> 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 when using failover. Without the prefix method, ASASMs installed in different slot numbers experience a MAC address change upon failover, and can experience traffic interruption. After upgrading, to use the prefix method of MAC address generation, reenables MAC address generation to use the default prefix.</p> <p>ASDM was not changed.</p>

New Features in Version 6.5(1)/8.5(1)

Released: July 8, 2011

[Table 4](#) lists the new features for ASA Version 8.5(1)/ASDM Version 6.5(1). This ASA and ASDM software version is only supported on the ASASM.



Note

Version 8.5(1) includes all features in 8.4(1), plus the features listed in this table. The following features, however, are not supported in No Payload Encryption software, and this release is only available as a No Payload Encryption release:

- VPN
- Unified Communications

Features added in 8.4(2) are not included in 8.5(1) unless they are explicitly listed in this table.

Table 4 **New Features for ASA Version 8.5(1)/ASDM Version 6.5(1)**

Feature	Description
Hardware Features	
Support for the ASA Services Module	We introduced support for the ASASM for the Cisco Catalyst 6500 E switch.
Firewall Features	

Table 4 **New Features for ASA Version 8.5(1)/ASDM Version 6.5(1) (continued)**

Feature	Description
Mixed firewall mode support in multiple context mode	<p>You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode.</p> <p>We modified the following command: firewall transparent.</p> <p>You cannot set the firewall mode in ASDM; you must use the command line interface.</p>
Interface Features	
Automatic MAC address generation is now enabled by default in multiple context mode	<p>Automatic generation of MAC addresses is now enabled by default in multiple context mode.</p> <p>We modified the following screen: System > Configuration > Context Management > Security Contexts.</p>
NAT Features	
Identity NAT configurable proxy ARP and route lookup	<p>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.</p> <p>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.</p> <p>We modified the following screens:</p> <p>Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced NAT Settings Configuration > Firewall > NAT Rules > Add/Edit NAT Rule</p> <p><i>Also available in Version 8.4(2).</i></p>
PAT pool and round robin address assignment	<p>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.</p> <p>Note Currently in 8.5(1), 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).</p> <p>We modified the following screens:</p> <p>Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > Firewall > NAT Rules > Add/Edit NAT Rule</p> <p><i>Also available in Version 8.4(2).</i></p>
Switch Integration Features	

Table 4 **New Features for ASA Version 8.5(1)/ASDM Version 6.5(1) (continued)**

Feature	Description
Autostate	<p>The switch supervisor engine can send autostate messages to the ASASM about the status of physical interfaces associated with ASASM VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASASM that the VLAN is down. This information lets the ASASM declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASASM takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).</p> <p>Note The switch supports autostate messaging only if you install a single ASASM in the chassis.</p> <p>See the following Cisco IOS command: firewall autostate.</p>
Virtual Switching System	The ASASM supports VSS when configured on the switches. No ASASM configuration is required.

Upgrading the Software

**Note**

For users migrating from the FWSM, see *Migrating to the Cisco ASA Services Module from the FWSM*.

This section describes how to upgrade to the latest version of the ASA image or the Field-Programmable Device (FPD) image and includes the following topics:

- [Upgrading the ASA Image, page 7](#)
- [Upgrading the FPD Image, page 8](#)
- [Upgrading the ASASM from the Supervisor 720 to the Supervisor 2T, page 11](#)

**Note**

For CLI procedures, see the ASA release notes.

Upgrading the ASA Image

- [Viewing Your Current Version, page 7](#)
- [Upgrading the Operating System and ASDM Images, page 7](#)

Viewing Your Current Version

The software version appears on the ASDM home page; view the home page to verify the software version of your ASASM.

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.

Detailed Steps

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

Upgrading the FPD Image

The ASASM includes a separate FPD image that you can upgrade using Cisco IOS software on the switch.

- [Determining if an FPD Upgrade is Required, page 8](#)
- [Upgrading the Cisco IOS and FPD Image, page 9](#)
- [Upgrading the FPD Image Only, page 9](#)

Determining if an FPD Upgrade is Required

Determine if an FPD upgrade is required using the **show hw-module all fpd** IOS command on the switch.

If the ASASM has the minimum required version, no further action is necessary. If an FPD image package needs an upgrade, proceed to the next step.


The following sample output indicates that the ASASM does not meet the minimum version requirements.

```
Router# show hw-module all fpd
=====
Slot Card Type          H/W   Field Programmable   Current   Min. Required
Ver.    Device: "ID-Name"   Version   Version
=====
   1  WS-SVC-ASA-SM1    1.0    1-TRISUL FPGA        1.8       1.10
=====
```


Upgrading the Cisco IOS and FPD Image

If you need to upgrade the Cisco IOS image, you can also load a new FPD image on local flash memory (disk0: or bootdisk:) to automatically install the FPD on the ASASM when you reload the switch.

Detailed Steps

-
- Step 1** Verify that the FPD automatic upgrade feature is enabled by examining the output of the **show running-config** IOS command on the switch.
- Look for the “upgrade fpd auto” line in the output. If there are no **upgrade** commands in the output, **upgrade fpd auto** is enabled because it is the default setting. If automatic upgrades are disabled, use the **upgrade fpd auto** command to enable automatic FPD upgrades.
- Step 2** If you have a Cisco.com login, you can obtain the FPD image from the following website:
<http://www.cisco.com/cisco/software/release.html?mdfid=283933147&flowid=29364&softwareid=280805682&release=15.0.1-SY1&reind=AVAILABLE&rellifecycle=ED&reltype=latest>
- Step 3** Download the FPD image package to local flash memory on the switch.
- See the switch documentation for more information about downloading files to flash memory.
-
-  **Note** Do not change any FPD-related settings on your system. If the default settings for the **upgrade fpd path** command have been changed, change the settings back to their default settings using the **no** form of this command.
-
- Step 4** Obtain the Cisco IOS image from the following website:
<http://www.cisco.com/cisco/software/release.html?mdfid=283933147&flowid=29364&dvdid=282804709&softwareid=280805685&release=15.0.1-SY1&reind=AVAILABLE&rellifecycle=ED&reltype=latest>
- See the switch documentation for information about loading the new IOS image.
- Step 5** Reload the switch using the new IOS image.
- When Cisco IOS boots, it searches for the FPD image package in flash. The switch updates the FPD images automatically as part of the Cisco IOS boot process.
-

Upgrading the FPD Image Only

If you do not need to upgrade the Cisco IOS image, you can upgrade the FPD image separately.

Restrictions

The FPD image must be in local flash memory. Remote upgrading from FTP or TFTP is not supported.

Detailed Steps

-
- Step 1** If you have a Cisco.com login, you can obtain the FPD image from the following website:
<http://www.cisco.com/cisco/software/release.html?mdfid=283933147&flowid=29364&softwareid=280805682&release=15.0.1-SY1&reind=AVAILABLE&rellifecycle=ED&reltype=latest>

- Step 2** Download the FPD image package to the switch flash memory. We recommend the local flash disk (disk0: or bootdisk:).

See the switch documentation for more information about downloading files to flash memory.

- Step 3** Verify the contents of the FPD image package using the following command:

```
Router# show upgrade fpd file file-url
```

The *file-url* argument is the location and name of the FPD image package file. For example, the following command successfully verifies the image (see the TRIFECTA card type for the ASASM):

```
Router# show upgrade fpd file disk0:c6500-fpd-pkg.1.10.pkg
Cisco Field Programmable Device Image Package for IOS
C6500 Family FPD Image Package (c6500-fpd-pkg.1.10.pkg), Version 15.0(0)SY99.41
Copyright (c) 2004-2012 by cisco Systems, Inc.
Built Thu 12-Jan-2012 14:46 by integ
```

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	1.4	0.0
	4	T3E3 SPA T3 FPGA	1.4	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	1.4	0.0
	4	T3E3 SPA T3 FPGA	1.4	0.0
...				
TRIFECTA	1	Trifecta DPFPGA	1.10	0.0

- Step 4** Upgrade the FPD using the following command:

```
Router# upgrade hw-module slot slot-number fpd file file-url
```

The *slot-number* argument indicates the chassis slot location of the ASASM. The *file-url* argument is the location and name of the FPD image package file. For example, to upgrade the ASASM in slot 2, enter the following command:

```
Router# upgrade hw-module slot 2 fpd file disk0:c6500-fpd-pkg.1.10.pkg
```

% The following FPD will be upgraded for WS-SVC-ASA-SM1 (H/W ver = 1.0) in slot 2:

Field Programmable Device: "ID-Name"	Current Version	Upgrade Version	Estimated Upgrade Time
1-TRISUL FPGA	1.8	1.10	00:06:30

% NOTES:

- Use 'show upgrade fpd progress' command to view the progress of the FPD upgrade.
- Since the target card is currently in disabled state, it will be automatically reloaded after the upgrade operation for the changes to take effect.

```
WARNING: The target card will be reloaded in order to start FPD image
         upgrade. This action will interrupt normal operation of the card.
         If necessary, ensure that appropriate actions have been taken to
         redirect card traffic before starting the upgrade operation.
```

```
% Are you sure that you want to perform this operation? [no]: yes
% Reloading the target card for FPD image upgrade ... Done!
% Upgrade operation will start in the background once the target card gets
  initialized after the reload operation. Please wait ...
  (Use "show upgrade fpd progress" command to see upgrade progress)
```

Step 5 Verify that the FPD upgrade is complete using the following command:

```
Router# show upgrade fpd progress
```

The following example shows that the FPD upgrade is updating:

```
Router# show upgrade fpd progress
```

FPD Image Upgrade Progress Table:

```
==== =====
Slot Card Type          Field Programmable      Approx.
                        Device : "ID-Name"      Time      Elapsed
                        =====
2 WS-SVC-ASA-SM1        1-TRISUL FPGA          00:06:30   00:00:24   Updating...
=====
```

The following example shows that the FPD upgrade is complete, because the upgrade is no longer in progress:

```
Router# show upgrade fpd progress
```

```
% There is no FPD image upgrade in progress.
```

Step 6 Verify that the FPD upgrade was successful using the following command:

```
Router# show hw-module all fpd
```

Upgrading the ASASM from the Supervisor 720 to the Supervisor 2T

To upgrade the ASASM from the Supervisor 720 to the Supervisor 2T, perform the following steps:

Step 1 Upgrade the ASASM with the Supervisor 2T image while the Supervisor 720 image is still loaded on the Catalyst 65000 Series E Switch.



Note If you replace the supervisor card on the Catalyst 65000 Series E Switch before you upgrade the ASASM, then the interfaces on the ASASM will not be recognized, and you will not be able to load a new image.

Step 2 Change the supervisor card from the Supervisor 720 to the Supervisor 2T on the Catalyst 65000 Series E Switch.

Step 3 Upgrade the Catalyst 65000 Series E Switch with the Supervisor 2T image.

Unsupported Commands

ASDM supports almost all commands available for the adaptive ASASM, 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, page 12](#)
- [Effects of Unsupported Commands, page 13](#)
- [Discontinuous Subnet Masks Not Supported, page 13](#)
- [Interactive User Commands Not Supported by the ASDM CLI Tool, page 13](#)

Ignored and View-Only Commands

Table 5 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 5 *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.

Table 5 **List of Unsupported Commands (continued)**

Unsupported Commands	ASDM Behavior
service-policy global	Ignored if it uses a match access-list class. For example: <pre>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</pre>
set metric	Ignored.
sysopt nodnsalias	Ignored.
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
ke00000000000000$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

- [Open Caveats in Version 6.5\(1.101\), page 14](#)
- [Open Caveats in Version 6.5\(1\), page 15](#)

Open Caveats in Version 6.5(1.101)

[Table 6](#) contains open caveats in ASDM software Version 6.5(1.101).

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 6 *Open Caveats in ASDM Version 6.5(1.101)*

Caveat	Description
CSCtq69054	Management Interface panel should not be listed on ASA NPE -K7 models
CSCtq87726	IDFW: Cannot easily remove primary AD Agent from server group
CSCtq95042	FQDN: Cannot configure "expire-entry-timer" and "poll-timer" on ASDM
CSCtr37439	Newly Created n/w objects and objectgroups not listed in n/w to shun win
CSCtr62524	ASDM forces user to apply changes when switching between sections
CSCtr80669	Inapplicable fields are shown for EC interfaces
CSCts13394	Startup wizard generates incorrect clock set CLI
CSCts31190	ASDM does not backup SNMP Community string in startup-config
CSCts79696	No SCEP forwarding url none
CSCts86675	ASDM Startup Wizard does not cleanly exit when resetting config
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCtw47962	ASDM online help index is incomplete
CSCtw47975	ASDM online help contains duplicate/multiple entries
CSCtw60293	Apply button is not enabled in Filter Rules & Default Information screen

Open Caveats in Version 6.5(1)

Table 7 contains open caveats in ASDM software Version 6.5(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 7 *Open Caveats in ASDM Version 6.5(1)*

Caveat	Description
CSCto34624	Refreshing ASDM connection table causes Monitoring tab to freeze
CSCto69856	IPv6: Changes to the IPv6 inspect map

Resolved Caveats in Version 6.5(1.110)

Table 8 contains the resolved caveats in ASDM software Version 6.5(1.110).

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 8 *Resolved Caveats in ASDM Version 6.5(1.110)*

Caveat	Description
CSCtn88072	Access rule description replication issue
CSCty30364	ASDM show none selected for failover command link
CSCua97321	ASDM: add inspect ipsec-pass-thru panel for ASASM
CSCuh65051	ACL remarks applied in ASDM 6.5.1.101 cause remarks to shift

Resolved Caveats in Version 6.5(1.101)

Table 9 contains the resolved caveats in ASDM software Version 6.5(1.101).

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 9 *Resolved Caveats in ASDM Version 6.5(1.101)*

Caveat	Description
CSCtr38862	SNMP ignored commands
CSCtx46042	ACL order in ASDM is not matching CLI
CSCtx55679	Support failover replication rate
CSCtx87609	MAC Address Auto: New auto-generated prefix

End-User License Agreement

For information on 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 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 *What's New in Cisco Product Documentation* at:

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

©2011-2013 Cisco Systems, Inc. All rights reserved