Release Notes for Cisco ASDM, Version 6.7(x)

Updated: October 16, 2012
Released: August 20, 2012

This document contains release information for Cisco ASDM Version 6.7(1) for the Cisco ASA 1000V and includes the following sections:

Important Notes

Complete Solution Installation

- Neither the ASA 1000V nor VSG supports non-ASCII characters. To support localization, all components (that is, Cisco VNMC, Cisco VSG, and ASA 1000V) must meet this requirement.
- The ASA 1000V and Cisco VNMC require that the VMware vCenter installation, including keyboard and password or shared key settings, be set to American English.

ASA 1000V Installation

- You can use only one management mode (either VNMC or ASDM) on the ASA 1000V. They are mutually exclusive, and you need to decide on the mode before installation. If you want to switch management modes, you must reinstall the ASA 1000V.
- ASDM is used to monitor traffic on the ASA 1000V in both VNMC and ASDM modes.

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

- Routes through the management interface can only be configured using the CLI in VNMC mode.

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 box 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 system heap memory size, modify the launcher shortcut by performing the following steps:

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 at the following URL:
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

	Browser				**Sun Java SE Plug-in**
Operating System	**Internet Explorer**	**Firefox**[1]	**Safari**	**Chrome**[2]	
Microsoft Windows (English and Japanese): • 7 • Vista • 2008 Server • XP	6.0 or later[1]	1.5 or later	No support	18.0 or later	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	18.0 or later	6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	18.0 or later	6.0

[1] ASDM requires an SSL connection from the browser to the ASA 1000V. 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 1000V 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.

[2] If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome “SSL false start” feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome wusing the **--disable-ssl-false-start** flag according to http://www.chromium.org/developers/how-tos/run-chromium-with-flags.

[3] 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.

ASA 1000V and ASDM Compatibility

Table 2 lists information about the ASA 1000V and ASDM compatibility.

Table 2 ASA 1000V and ASDM Compatibility

Application	Description
ASDM	ASA Version 8.7(1.1) requires ASDM Version 6.7(1). For information about ASDM requirements for other releases, see *Cisco ASA Compatibility,* at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

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

Released: October 16, 2012

Table 3 lists the new features for ASA Version 8.7(1.1)/ASDM Version 6.7(1).

Note Version 8.7(1) was removed from Cisco.com due to build issues; please upgrade to Version 8.7(1.1) or later.

Table 3 New Features for ASA Version 8.7(1.1)/ASDM Version 6.7(1)

Feature	Description
Platform Features	
Support for the ASA 1000V	We introduced support for the ASA 1000V for the Nexus 1000V switch.
Cloning the ASA 1000V	You can add one or multiple instances of the ASA 1000V to your deployment using the method of cloning VMs.
Management Features	
ASDM mode	You can configure, manage, and monitor the ASA 1000V using the Adaptive Security Device Manager (ASDM), which is the single GUI-based device manager for the ASA.
VNMC mode	You can configure and manage the ASA 1000V using the Cisco Virtual Network Management Center (VNMC), which is a GUI-based multi-device manager for multiple tenants.
XML APIs	You can configure and manage the ASA 1000V using XML APIs, which are application programmatic interfaces provided through the Cisco VNMC. This feature is only available in VNMC mode.
Firewall Features	
Cisco VNMC access and configuration	Cisco VNMC access and configuration are required to create security profiles. You can configure access to the Cisco VNMC through the Configuration > Device Setup > Interfaces pane in ASDM. Enter the login username and password, hostname, and shared secret to access the Cisco VNMC. Then you can configure security profiles and security profile interfaces. In VNMC mode, use the CLI to configure security profiles.
Security profiles and security profile interfaces	Security profiles are interfaces that correspond to an edge security profile that has been configured in the Cisco VNMC and assigned in the Cisco Nexus 1000V VSM. Policies for through-traffic are assigned to these interfaces and the outside interface. You can add security profiles through the Configuration > Device Setup > Interfaces pane. You create the security profile by adding its name and selecting the service interface. ASDM then generates the security profile through the Cisco VNMC, assigns the security profile ID, and automatically generates a unique interface name. The interface name is used in the security policy configuration. We introduced or modified the following screens: Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add Security Profile Monitoring > Interfaces > Security Profiles

Table 3 New Features for ASA Version 8.7(1.1)/ASDM Version 6.7(1) (continued)

Feature	Description
Service interface	The service interface is the Ethernet interface associated with security profile interfaces. You can only configure one service interface, which must be the inside interface. We modified the following screen: Configuration > Device Setup > Interfaces.
VNMC policy agent	The VNMC policy agent enables policy configuration through both the ASDM and VNMC modes. It includes a web server that receives XML-based requests from Cisco VNMC over HTTPS and converts it to the ASA 1000V configuration. We modified the following screen: Configuration > Device Setup > Interfaces.

Upgrading the ASAand ASDM Software

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

- Viewing Your Current Version, page 6
- Upgrading the ASA and ASDM Images, page 6

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 ASA and ASDM Images

This section describes how to install the ASDM and ASA images.

We recommend that you upgrade the ASDM image before the ASA image. You must upgrade the ASA by copying files through the ASA CLI. You must use the 6.7(1) version of the ASDM image; you cannot use another older version of the ASDM image with the ASA.

Note The VNMC does not support ASA image upgrade.

Upgrading Using ASDM 6.7(1)

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**.

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 then restart the ASDM.

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

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, page 7
- Effects of Unsupported Commands, page 8
- Discontinuous Subnet Masks Not Supported, page 8
- Interactive User Commands Not Supported by the ASDM CLI Tool, page 8

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.
pager	Ignored.

Table 4 List of Unsupported Commands **(continued)**

Unsupported Commands	ASDM Behavior

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`

sysopt nodnsalias	Ignored.
sysopt uauth allow-http-cache	Ignored.
terminal	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

There are no open caveats in the ASDM 6.7(1) release.

Licensing for the ASA 1000V

The ASA 1000V is licensed per each CPU socket that it is protecting. The Cisco Nexus 1000V switch provisions and enforces licenses for the ASA 1000V. Licenses are installed on the Virtual Supervisor Module (VSM) in the Cisco Nexus 1000V switch.

For more information, see the most recent version of the *Cisco Nexus 1000V License Configuration Guidelines* document at the following URL:
http://www.cisco.com/en/US/products/ps9902/products_licensing_information_listing.html

Related Documentation

For more information about the individual components that comprise the ASA 1000V, see the following documentation:

- Cisco Nexus 1000V
  Cisco http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
- Cisco VNMC and Cisco VSG
  http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html
- VMware
  http://www.vmware.com/support/pubs/
- ASA 1000V
  http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html
- ASDM
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.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.

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.