Release Notes for Cisco ASDM for the FWSM, Version 6.2(x)F

March 2013

This document contains release information for Cisco ASDM Versions 6.2(1)F through 6.2(3)F for the FWSM.

This document includes the following sections:

New Features

Table 1 lists the new features for ASDM Versions 6.2(1)F through 6.2(3)F. These features were introduced in Version 6.2(1)F. There are no new features for Version 6.2(2)F and 6.2(3)F. All features apply to FWSM Version 4.1(1), as well.

Table 1 New Features for FWSM Version 4.1(1)

Feature	Description
Platform Features	
Separate hostnames for primary and secondary blades	This feature lets you configure a separate hostname on the primary and secondary FWSMs. If the secondary hostname is not configured, the primary and secondary hostnames are the same. We modified the following screen: **Configuration** > **Device Setup** > **Device Name/Password**.

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

Table 1 New Features for FWSM Version 4.1(1) (continued)

Feature	Description
Firewall Features	
Creation of UDP sessions with unresolved ARP in the accelerated path	If you configure the FWSM to create the session in the accelerated path even though the ARP lookup fails, then it will drop all further packets to the destination IP address until the ARP lookup succeeds. Without this feature, each subsequent UDP packet goes through the session management path before being dropped by the accelerated path, causing potential overload of the session management path. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **TCP Options**.
DCERPC Enhancement: Remote Create Instance message support	In this release, DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC messages. No screens were modified.
Reset Connection marked for Deletion	You can now disable the sending of a reset (RST) packet for a connection marked for deletion. Starting in this release, reset packets are not sent by default. You can restore the previous behavior, so that when the FWSM receives a SYN packet on the same 5-tuple (source IP and port, destination IP and port, protocol) which was marked for deletion, it will send a reset packet. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **TCP Options**.
PPTP-GRE Timeout	You can now set the timeout for GRE connections that are built as a result of PPTP inspection. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**.
IPv6 support in ASDM	ASDM now supports configuration of IPv6.
Management Features	
Turning on/off names in Syslog messages	This feature enables users to choose whether or not to apply name translation while generating syslogs to the console, syslog server, and FTP syslog server. We modified the following screen: **Configuration** > **Logging** > **Logging Setup**.
Shared Management Interface in Transparent Mode	You can now add a management VLAN that is not part of any bridge group. This VLAN is especially useful in multiple context mode where you can share a single management VLAN across multiple contexts. We modified the following screen: **Configuration** > **Interfaces** > **Add/Edit Interface**.
Teardown Syslog Enhancement	New syslogs were added for when a connection is torn down. We introduced the following syslog messages: 302030 through 33.
SNMP Buffer enhancement	With this enhancement, SNMP requests will be handled more efficiently, so that the allocated blocks for SNMP are freed up quickly, thus leaving enough blocks for other processes. No screens were modified.
Troubleshooting Features	
Crashinfo enhancement	The crashinfo enhancement improves the reliability of generating crash information. No screens were modified.
Packet Capture Wizard	The FWSM uses the Packet Capture Wizard to implement a packet sniffer on the FWSM. Cisco TAC might request captures from you to troubleshoot a problem. These captures may be in PCAP format for download and further analysis on products like TCPDUMP or Ethereal. We modified the following screen: **Wizards** > **Packet Capture Wizard** > **Capture Wizard**.

ASDM Client Operating System and Browser Requirements

Table 2 lists the supported and recommended client operating systems and Java for ASDM.

Table 2 Operating System and Browser Requirements

Operating System	Browser			Sun Java SE Plug-in[1]
	Internet Explorer	Firefox	Safari	
Microsoft Windows (English and Japanese): • 7 • Vista • 2003 Server • XP • 2000 (Service Pack 4 or higher)	6.0 or later	1.5 or later	No support.	• 5.0 (1.5.0) • 6.0
Apple Macintosh OS X: • 10.6 • 10.5 • 10.4	No support.	1.5 or later	2.0 or later	• 5.0 (1.5.0) • 6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • WS	N/A	1.5 or later	N/A	• 5.0 (1.5.0) • 6.0

[1] Obtain Sun Java from java.sun.com.

FWSM and ASDM Release Compatibility

Table 3 shows the ASDM or PDM versions that can be used with each FWSM release.

All ASDM releases are backward-compatible with FWSM 3.1. PDM releases are not backward-compatible.

Table 3 FWSM and ASDM /PDM Release Compatibility

FWSM Release	ASDM/PDM Version
4.1(x)	Requires ASDM 6.2(x)F or higher. Latest version is recommended: 6.2(3)F.
4.0(x)	Requires ASDM 6.1(x)F or higher. Latest version is recommended: 6.1(5)F.
3.2(x)	Requires ASDM 5.2(x)F and higher. Latest version is recommended: 5.2(4)F.
3.1(x)	Requires ASDM 5.0(x)F and higher. Latest version is recommended: 5.0(3)F.
2.3(x)	Requires PDM 4.1(x). Latest version is recommended: 4.1(5).
2.2(x)	Requires PDM 4.1(x). Latest version is recommended: 4.1(5).
1.1(x)	Requires PDM 2.1(1).

Upgrading or Downgrading the Software

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

- Viewing Your Current Version, page 4
- Upgrading from 2.x or 3.x, page 4
- Upgrading the Operating System and ASDM Images, page 4
- Downgrading from 4.1, page 5

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 FWSM.

Upgrading from 2.x or 3.x

Starting in Release 4.0(1), many commands are migrated to new commands (for example, the **http-map** commands are converted to **policy-map type inspect http** commands).

If you upgrade from 2.x or 3.x, the configuration is converted. This converted configuration is not saved to memory until you save the configuration by clicking **Save** at the top of the window.

If you try to downgrade to 2.x or 3.x using a converted configuration, many commands will be rejected. Moreover, if you add access lists to the 4.x configuration to take advantage of larger access list memory space, then downgrading could result in an inability to load all the new access lists.

If you want to downgrade, be sure to copy a saved 2.x or 3.x configuration to the starting configuration before you reload with the 2.x or 3.x image.

Upgrading the Operating System and ASDM Images

This section describes how to install the ASDM and operating system (OS) images to the current application partition.

Note If the FWSM is running Version 4.0 or later, then you can upgrade to the latest version of ASDM (and disconnect and reconnect to start running it) before upgrading the OS.

If the FWSM is running a version earlier than 4.0, then use the already installed version of ASDM to upgrade both the OS and ASDM to the latest versions, and then reload.

To install and start using the new images, perform the following steps:

Detailed Steps

Step 1 From the Tools menu, choose **Tools > Upgrade Software from Cisco.com**.

In multiple context mode, access this menu from the System. For 6.2F, this menu item is located under Tools > Software Updates.

The Upgrade Software from Cisco.com Wizard appears.

Note If you are running ASDM Version 5.2 or lower, then the Upgrade Software from Cisco.com Wizard is not available. You can download the software from the following URL:

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

Then use **Tools > Upgrade Software**.

Step 2 Click **Next**.

The Authentication screen appears.

Step 3 Enter your Cisco.com username and password, and click **Next**.

The Image Selection screen appears.

Step 4 Check the **Upgrade the FWSM version** check box and the **Upgrade the ASDM version** check box to specify the most current images to which you want to upgrade, and click **Next**.

The Selected Images screen appears.

Step 5 Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.

The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.

The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the FWSM.

If you upgraded the FWSM version and the upgrade succeeded, an option to save the configuration and reload the FWSM appears.

Step 6 Click **Yes**.

For the upgrade versions to take effect, you must save the configuration, reload the FWSM, and restart ASDM.

Step 7 Click **Finish** to exit the wizard when the upgrade is finished.

Downgrading from 4.1

This section describes how to downgrade from 4.1, and includes the following topics:

- Important Notes, page 6
- Downgrading, page 6

Important Notes

If you configure the shared management VLAN feature that was introduced in 4.1(1), this feature is not supported when you downgrade to a pre-4.1(1) release.

See the following issues when you use this feature, and then downgrade:

- The interface configuration for the shared VLAN is accepted in the first context configuration in which it appears, but is rejected in subsequent transparent mode contexts.
- For these subsequent contexts, if the startup-config has the management VLAN configuration defined directly *after* another VLAN configuration for through traffic, then the name and security level associated with the (rejected) shared management VLAN is erroneously applied to the immediately preceding VLAN.

Workaround: Remove the interface configuration for the shared VLAN from all contexts before you downgrade.

For example, you have the following configuration in 4.1:

```
interface Vlan100
 nameif outside
 bridge-group 5
 security-level 0

interface Vlan101
 nameif dmz
 security-level 100
 management-only
 ip address 10.90.90.4 255.255.255.0 standby 10.90.90.5
```

After downgrading, the shared management **interface vlan101** command is rejected if it was already used in another context; so the **nameif dmz** and **security-level 100** commands are applied to VLAN 100, overwriting the original **nameif** and **security-level** commands. (The VLAN 101 **management-only** and **ip address** commands are rejected because they are not allowed for the **interface vlan** command pre-4.1). The resulting VLAN 100 configuration is the following:

```
interface Vlan100
 nameif dmz
 bridge-group 5
 security-level 100
```

Downgrading

This section describes how to downgrade the ASDM and operating system (OS) images to the current application partition.

To install and start using the old images, perform the following steps:

Detailed Steps

Step 1 If you have a Cisco.com login, you can obtain the old OS and ASDM images from the following website:

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

Step 2 If you configured shared management VLANs for transparent mode contexts, see the "Important Notes" section on page 6 to remove the configuration for each context.

Step 3 From the Tools menu, choose **Tools > Software Updates > Upgrade Software from Local Computer**.

The Upgrade Software from Local Computer dialog box appears.

Step 4 (Optional) To downgrade ASDM, from the Image to Upload drop-down list, choose **ASDM**.

ASDM Version 6.2F is backwards compatible with previous versions, so you do not need to downgrade ASDM.

Step 5 Enter the local path to the file on your PC or click **Browse Local Files** to find the file on your PC.

Step 6 Click **Upload Image**. The uploading process might take a few minutes; make sure you wait until it is finished.

Step 7 To downgrade your FWSM image, repeat Step 3 through Step 6, except choose **FWSM** from the Image to Upload drop-down list.

Step 8 You are prompted to reload. Click **OK**.

Unsupported Commands

ASDM supports almost all commands available for the adaptive FWSM, 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 9
- Interactive User Commands Not Supported by the ASDM CLI Tool, page 9

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.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
ipv6 nd prefix	Unsupported.
match-metric	Ignored. This is a command of route-map.
match-interface	Ignored. This is a command of route-map.

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

Unsupported Commands	ASDM Behavior
match route-type	Ignored. This is a command of route-map.
pager	Ignored.
pim accept-register route-map	Ignored. You can configure only the **list** option using ASDM.
prefix-list	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 line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

set metric	Ignored.
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**.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

  Monitor-only mode allows access to the following functions:

  - The Monitoring area
  - The CLI tool (Tools > Command Line Interface), which lets you use the CLI commands

  To exit Monitor-only mode, use the CLI tool or access the FWSM console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information.

Note You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose **Configuration** > **Device Management** > **Users/AAA** > **User Accounts and Configuration** > **Device Management** > **Users/AAA** > **AAA Access**.

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. From the ASDM Tools menu, click **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

This section lists the open caveats in software Versions 6.2(2)F and 6.2(3)F.

If you are running an older release and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from your release moving forward. For example, if you are running Release 6.2(1), then you need to add the caveats in that section to the resolved caveats from 6.2(2) to determine the complete list of open caveats for your release.

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 5 Open Caveats Version 6.2(2)F

Caveat ID	Description
CSCsy68911	FWSM: ASDM may report an error about incorrect version number
CSCsy98391	Incorrect configurable parameters shown on changing context mode
CSCtf53475	Switch from management-only to bridge-group or vice versa doesn't work
CSCtf66005	Launching ASDM from browser prompts for login 3 times

Table 6 Open Caveats Version 6.2(3)F

Caveat ID	Description
CSCud68382	Java Web Start may not work on MacOS

Resolved Caveats

This section lists the open caveats in software Versions 6.2(2)F and 6.2(3)F.

Table 7 Resolved Caveats in Version 6.2(2)F

Caveat ID	Description
CSCsu00870	ASDM webpage does not load and produces a 404
CSCsy47137	ASDM shows wrong n/w objects while filtering, which is not part of config
CSCta40669	Captures not saved from ASDM Packet Capture Wizard
CSCte97635	Description for service RST conn marked for deletion not clear
CSCtf34586	Unable to download PCAP directly from a context for device in multi-mode
CSCtf38829	Capture Wizard: capture file not saved in multiple mode
CSCtf58007	Enforcing EUI-64 option gives an ERROR
CSCtf66222	No support for **service reset no-connection** command
CSCtf71056	“Name” disappears when modify Network Object Netmask in ASDM
CSCtf99691	Src and Dst IP/ports not correct in real-time viewer for syslog 302015

Table 7 Resolved Caveats (continued) in Version 6.2(2)F

Caveat ID	Description
CSCtg75843	Reverse access-rule addition fails for a user with privilege < 15
CSCtg98056	ASDM: “This syslog message has an invalid format” Error

Table 8 Resolved Caveats in Version 6.2(3)F

Caveat ID	Description
CSCsy68911	FWSM: ASDM may report an error about incorrect version number
CSCtk46281	ASDM for FWSM: tcp-udp object-group can be removed even if applied
CSCtx73665	Java exception for read-only user priv 5 - Access rules panel hangs
CSCty12281	configured description is ignored when adding Access Rule via ASDM
CSCtz47688	Merge dmlauncher 1.5.55 into ASDM-FWSM branch to add Java 7 support
CSCub56905	ASDM allows the dns keyword when configuring dynamic & static policy nat
CSCud17119	ASDM launcher not working on Linux redhat6
CSCud37686	ASDM for FWSM: Delete button on Network Objects/Group window is disabled
CSCud40817	ACL hit count stayed 0 with FWSM 4.1(6)

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.

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.