Troubleshoot ASDM License, Upgrade and Compatibility Problems

Contents

Introduction

Background

ASDM Upgrade Problems

Problem 1. How to upgrade ASA/ASDM upgrade from the source version X to the target version Y?

Problem 2. What are the recommended versions for ASA/ASDM?

Problem 3. ASA/ASDM update check failure in ASDM via Tools > Check for ASA/ASDM Updates

Problem 4. Which versions contain fixed for specific vulnerabilities?

Problem 5. "% ERROR: ASDM package is not digitally signed. Rejecting configuration." error message

Problem 6. Unable to check for ASA/ASDM Updates in multiple context mode

Problem 7. "Cisco's General Terms form have not been accepted or rejected to continue to download." error message

Problem 8. Unable to download software for specific hardware

Problem 9. "Error occurred in performing File Transfer HTTP Response code -1" error message

ASDM Compatibility Problems

Problem 1. Incompatible Java version

Problem 2. Incompatible ASA and ASDM version

Problem 3. ASDM and OpenJDK Support

Problem 4. ASDM and Java Azul Zulu Compatibility

Problem 5. WARNING: Signature not found in file disk0:/asdm-xxx.bin

Problem 6. "% ERROR: ASDM package is not digitally signed. Rejecting configuration."

Problem 7. "%ERROR: Signature not valid for file disk0:/ "

Problem 8. Secure Firewall Posture (Hostscan) Compatibility

Problem 9. Latest supported version

Problem 10. ASDM support on Linux

Problem 11. ASDM end of support

ASDM License Problems

Problem 1. 3DES/AES Smart License is Missing

Problem 2. Oracle Java JRE Licensing Requirements

Problem 3. ASDM Warning about site-to-site VPN License in Multi-Context Mode

References

Introduction

This document describes the troubleshooting process for ASDM license, upgrade and compatibility problems.

Background

The document is part of the Adaptive Security Appliance Device Manager (ASDM) troubleshoot series along with these documents:

- Troubleshoot ASDM Launch Problems
- Troubleshoot ASDM Configuration, Authentication and Other Problems
- Troubleshoot ASDM TLS Security, Certificate and Vulnerability Problems

ASDM Upgrade Problems

Problem 1. How to upgrade ASA/ASDM upgrade from the source version X to the target version Y?

The user needs assistance with an ASA/ASDM upgrade from the source version X to the target version Y.

Troubleshoot – Recommended Actions

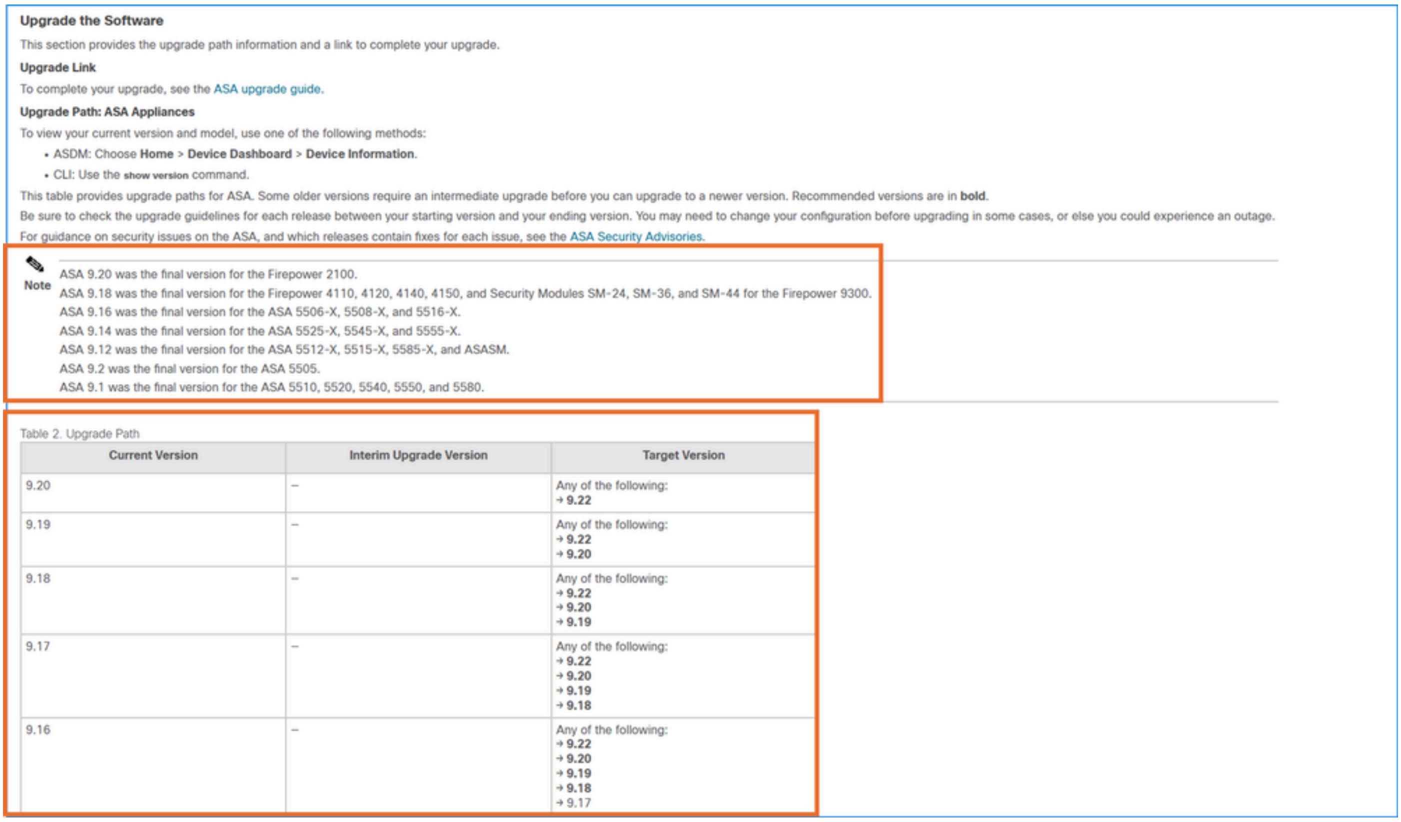
1. Ensure that the ASA, ASDM, operating system and Java versions are compatible with the target version. Refer to the Cisco Secure Firewall ASA Release Notes, Cisco Secure Firewall ASDM Release Notes, Cisco Secure Firewall ASA Compatibility.

The ASA, ASDM, operating system and Java versions **must be compatible,** and the target versions **must be supported** on specific hardware. https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

2. For ASA running on Firepower 4100/9300, ensure that the Firepower eXtensible Operating system (FXOS) and the ASA software versions are compatible. Refer to the Cisco Firepower 4100/9300 FXOS Compatibility.

3. Ensure to familiarize with the changes in the target version by checking the Cisco Secure Firewall ASA Release Notes, Cisco Secure Firewall ASDM Release Notes. In the case of Firepower 4100/9300, also familiarize with the changes in FXOS by checking the FXOS Release Notes.

4. Ensure to check the upgrade path in the release notes. In this example, the Table 2 in the release notes for the version 7.22 contains the upgrade path from previous versions to the target version:



Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Upgrade Path: ASA Appliances

To view your current version and model, use one of the following methods:

- ASDM: Choose **Home** > **Device Dashboard** > **Device Information**.
- CLI: Use the **show version** command.

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

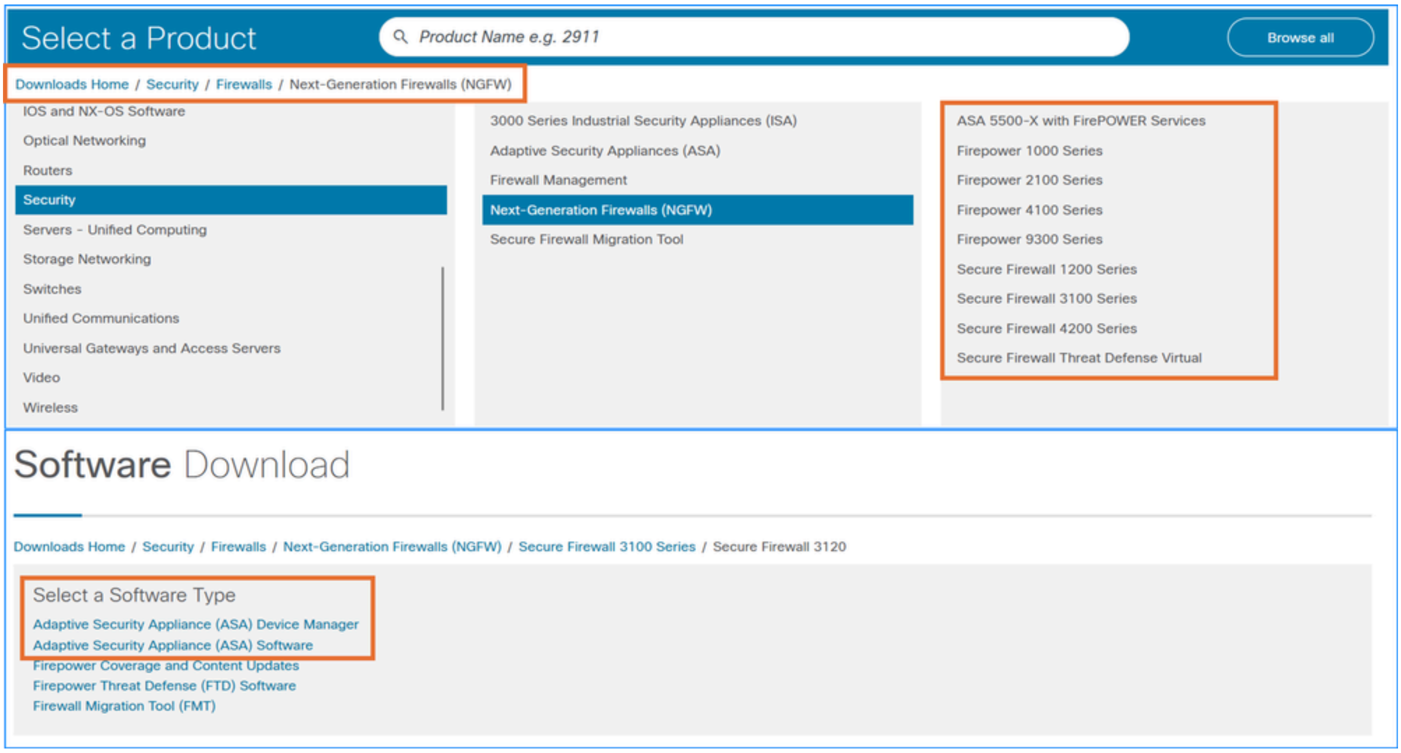
Note

ASA 9.20 was the final version for the Firepower 2100.
ASA 9.18 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.
ASA 9.16 was the final version for the ASA 5506-X, 5508-X, and 5516-X.
ASA 9.14 was the final version for the ASA 5525-X, 5545-X, and 5555-X.
ASA 9.12 was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.
ASA 9.2 was the final version for the ASA 5505.
ASA 9.1 was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Table 2. Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.20	–	Any of the following: → **9.22**
9.19	–	Any of the following: → **9.22** → **9.20**
9.18	–	Any of the following: → **9.22** → **9.20** → **9.19**
9.17	–	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18**
9.16	–	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17

5. Once the compatibility requirements are satisfied, download the target ASA/ASDM and FXOS versions (Firepower 4100/9300 only) from the Software Download page. Ensure to select the specific hardware models as show in this example. The suggested releases are marked with a golden star:



Select a Product
Product Name e.g. 2911
Browse all
Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW)
IOS and NX-OS Software
Optical Networking
Routers
Security
Servers - Unified Computing
Storage Networking
Switches
Unified Communications
Universal Gateways and Access Servers
Video
Wireless
3000 Series Industrial Security Appliances (ISA)
Adaptive Security Appliances (ASA)
Firewall Management
Next-Generation Firewalls (NGFW)
Secure Firewall Migration Tool
ASA 5500-X with FirePOWER Services
Firepower 1000 Series
Firepower 2100 Series
Firepower 4100 Series
Firepower 9300 Series
Secure Firewall 1200 Series
Secure Firewall 3100 Series
Secure Firewall 4200 Series
Secure Firewall Threat Defense Virtual
Software Download
Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall 3100 Series / Secure Firewall 3120
Select a Software Type
Adaptive Security Appliance (ASA) Device Manager
Adaptive Security Appliance (ASA) Software
Firepower Coverage and Content Updates
Firepower Threat Defense (FTD) Software
Firewall Migration Tool (FMT)

6. Ensure to go through the Chapter: Planning Your Upgrade and the Chapter: Upgrade the ASA in the Cisco Secure Firewall ASA Upgrade Guide.

References

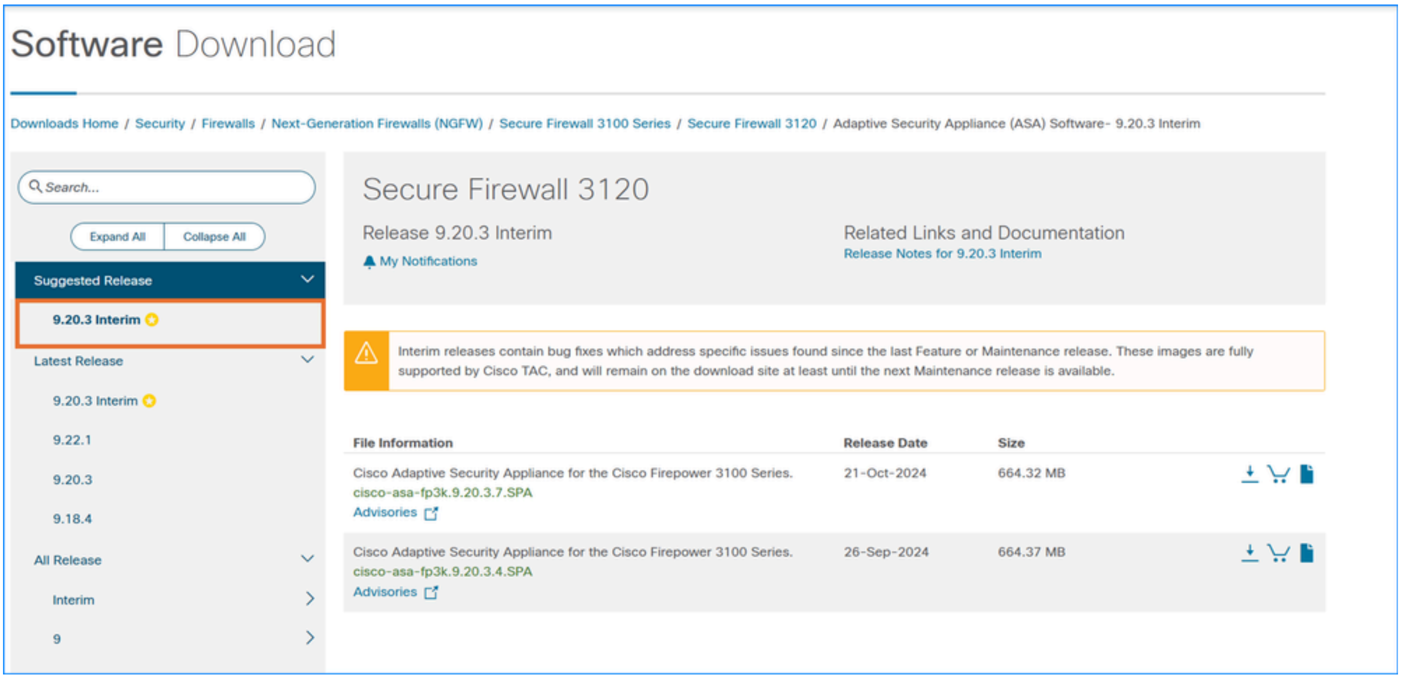
- [Cisco Secure Firewall ASA Release Notes]
- [Cisco Secure Firewall ASDM Release Notes]
- [Cisco Secure Firewall ASA Compatibility]
- [Cisco Firepower 4100/9300 FXOS Compatibility]
- [Cisco Secure Firewall ASA Upgrade Guide]

Problem 2. What are the recommended versions for ASA/ASDM?

The user asks about the recommended versions for ASA/ASDM.

Troubleshoot – Recommended Actions

The Cisco TAC **does not provide** recommendations about the software versions. Users can download the Cisco Suggested release based on software quality, stability and longevity. The suggested releases are marked with a golden star like shown below:



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall 3100 Series / Secure Firewall 3120 / Adaptive Security Appliance (ASA) Software- 9.20.3 Interim

Secure Firewall 3120

Release 9.20.3 Interim

Related Links and Documentation

Release Notes for 9.20.3 Interim

Interim releases contain bug fixes which address specific issues found since the last Feature or Maintenance release. These images are fully supported by Cisco TAC, and will remain on the download site at least until the next Maintenance release is available.

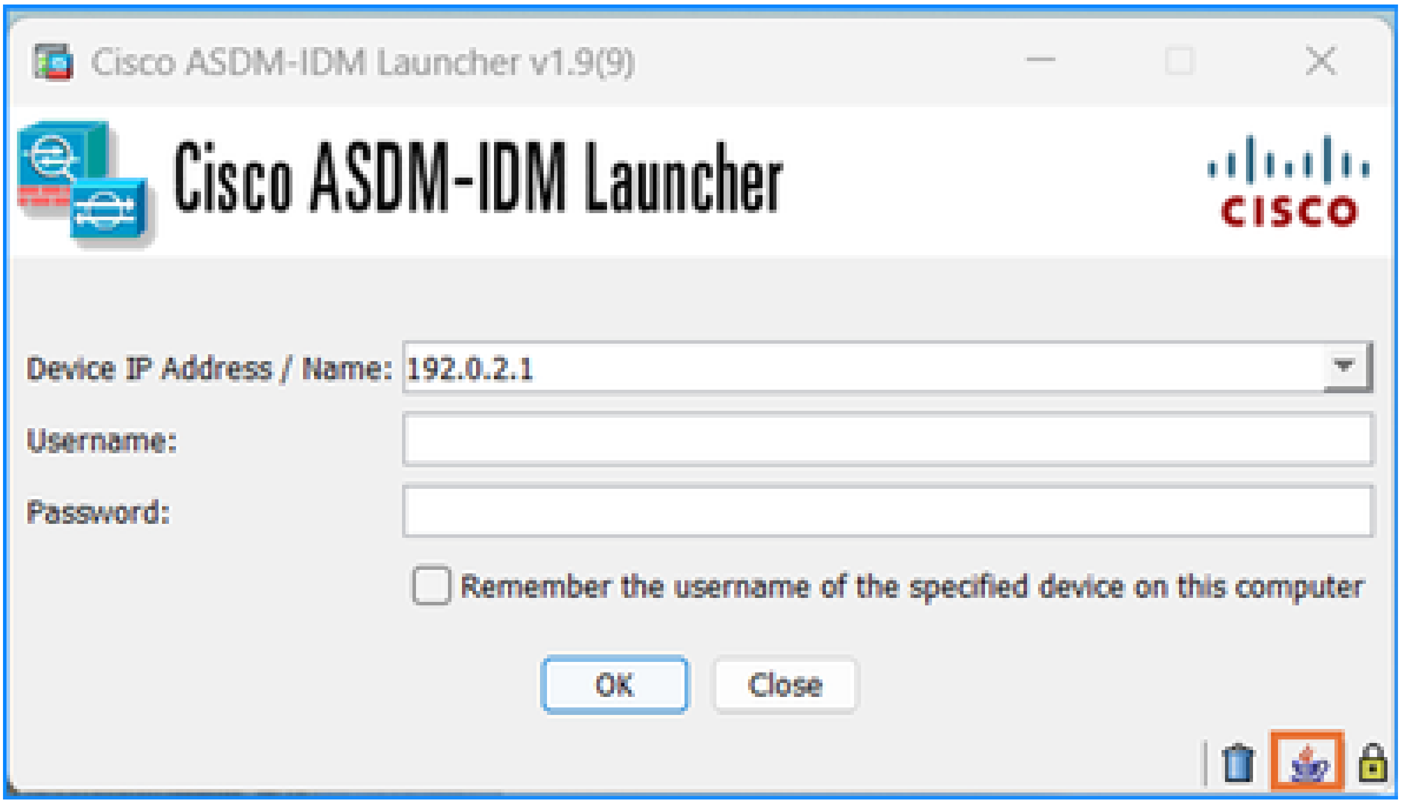
File Information	Release Date	Size
Cisco Adaptive Security Appliance for the Cisco Firepower 3100 Series. cisco-asa-fp3k.9.20.3.7.SPA Advisories	21-Oct-2024	664.32 MB
Cisco Adaptive Security Appliance for the Cisco Firepower 3100 Series. cisco-asa-fp3k.9.20.3.4.SPA Advisories	26-Sep-2024	664.37 MB

Problem 3. ASA/ASDM update check failure in ASDM via Tools > Check for ASA/ASDM Updates

The check for ASA/ASDM updates in ASDM via **Tools** > **Check for ASA/ASDM Updates** fails. Specifically, these symptoms are observed:

1. The Enter Network Password window re-appears after clicking the Login button even if the correct credentials are provided.

2. In the Java console logs the “Meta data request failed” error is shown:


Cisco ASDM-IDM Launcher v1.9(9)

Cisco ASDM-IDM Launcher

Device IP Address / Name: 192.0.2.1

Username:

Password:

□ Remember the username of the specified device on this computer

<#root>

```
2024-06-16 13:00:03,471 [ERROR] Error::Failed : Request processing
88887 [Thread-30] ERROR com.cisco.dmcommon.util.DMCommonEnv  - Error::Failed : Request processing
2024-06-16 13:00:03,472 [ERROR] Error::Access token request processing failed
88888 [Thread-30] ERROR com.cisco.dmcommon.util.DMCommonEnv  - Error::Access token request processing f
2024-06-16 13:00:04,214 [ERROR] getMetaDataResponse :: Server returned HTTP response code: 403 for URL:
89630 [Thread-30] ERROR com.cisco.dmcommon.util.DMCommonEnv  - getMetaDataResponse :: Server returned H
2024-06-16 13:00:04,214 [ERROR] error::Meta data request failed.

89630 [Thread-30] ERROR com.cisco.dmcommon.util.DMCommonEnv  - error::Meta data request failed.
```

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCvf91260 “ASDM: Upgrade from CCO not working due to un-ignorable fields. "Meta data request failed”. The workaround is to download images directly from the download page and upload to the firewall.

Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

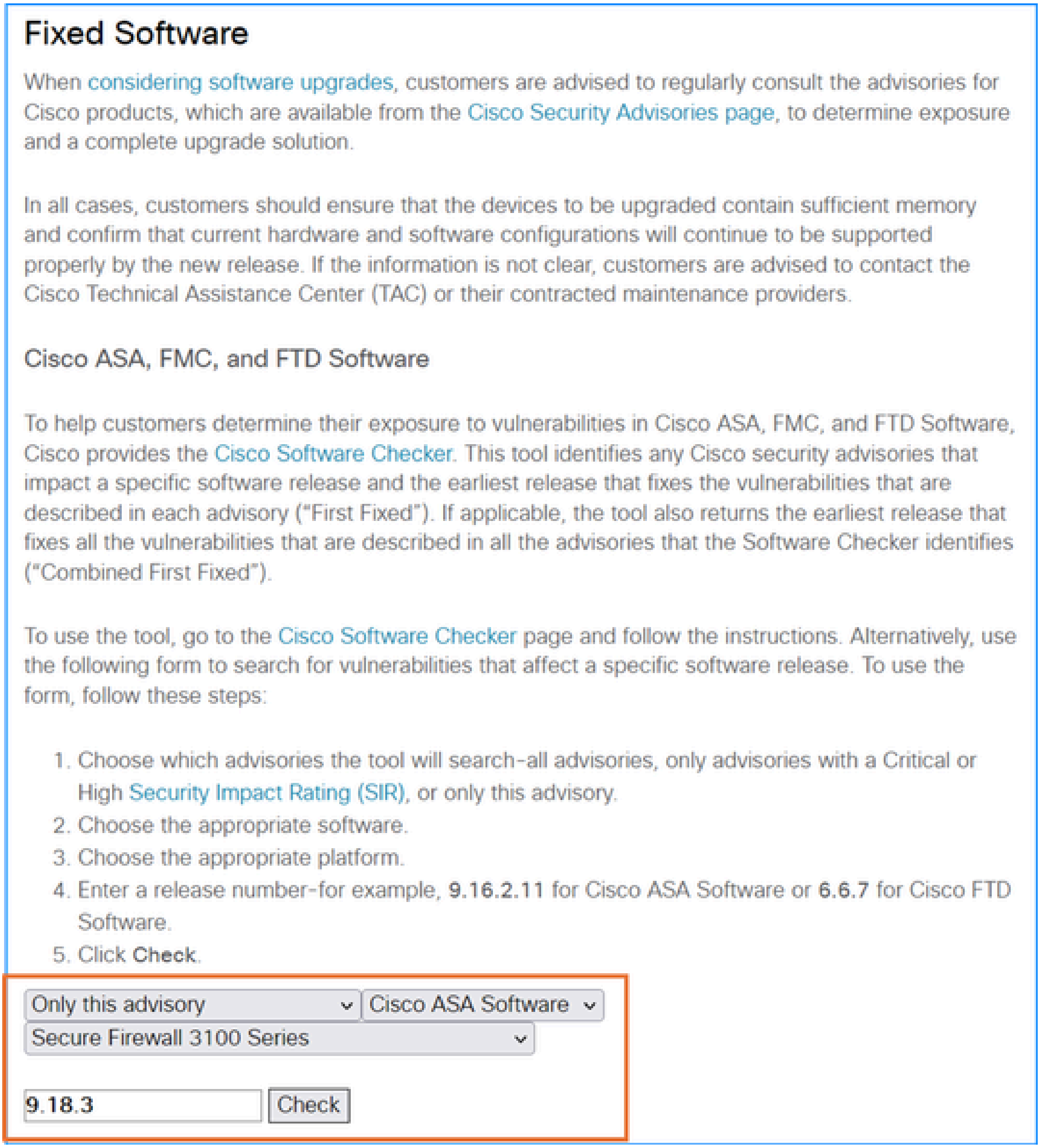
Problem 4. Which versions contain fixed for specific vulnerabilities?

The user asks about the fixed versions of specific vulnerabilities.

Troubleshoot – Recommended Actions

1. Ensure to check the security advisory for the affected products.
2. In the security advisory, provide the existing hardware and software version to the software checker

and click **Check**:



Fixed Software

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Cisco ASA, FMC, and FTD Software

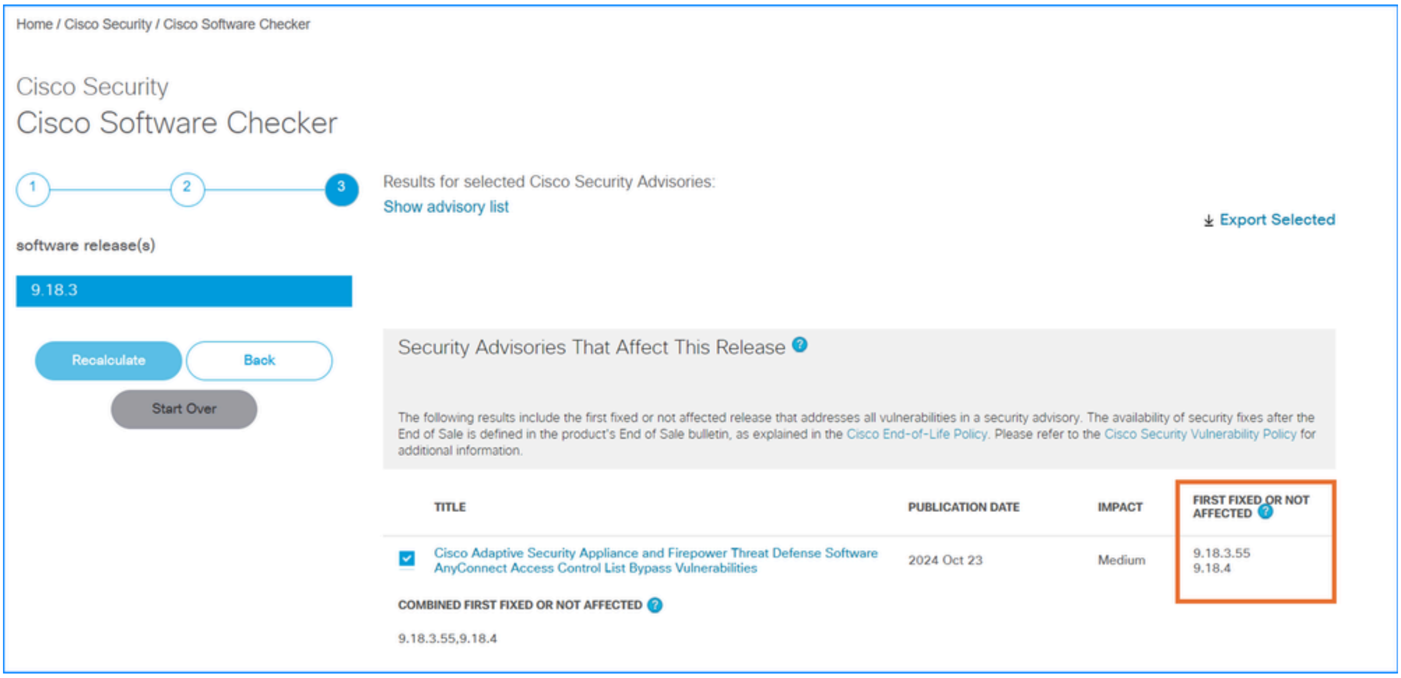
To help customers determine their exposure to vulnerabilities in Cisco ASA, FMC, and FTD Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described in each advisory ("First Fixed"). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities that are described in all the advisories that the Software Checker identifies ("Combined First Fixed").

To use the tool, go to the Cisco Software Checker page and follow the instructions. Alternatively, use the following form to search for vulnerabilities that affect a specific software release. To use the form, follow these steps:

1. Choose which advisories the tool will search-all advisories, only advisories with a Critical or High Security Impact Rating (SIR), or only this advisory.
2. Choose the appropriate software.
3. Choose the appropriate platform.
4. Enter a release number-for example, **9.16.2.11** for Cisco ASA Software or **6.6.7** for Cisco FTD Software.
5. Click **Check**.

Only this advisory
Cisco ASA Software
Secure Firewall 3100 Series
9.18.3

3. If the fixed version is available, note the versions in the **FIRST FIXED OR NOT AFFECTED** column:



Home / Cisco Security / Cisco Software Checker

Cisco Security

Cisco Software Checker

Results for selected Cisco Security Advisories:

Show advisory list

software release(s)

9.18.3

Security Advisories That Affect This Release

The following results include the first fixed or not affected release that addresses all vulnerabilities in a security advisory. The availability of security fixes after the End of Sale is defined in the product's End of Sale bulletin, as explained in the Cisco End-of-Life Policy. Please refer to the Cisco Security Vulnerability Policy for additional information.

	TITLE	PUBLICATION DATE	IMPACT	FIRST FIXED OR NOT AFFECTED
☑	Cisco Adaptive Security Appliance and Firepower Threat Defense Software AnyConnect Access Control List Bypass Vulnerabilities	2024 Oct 23	Medium	9.18.3.55 9.18.4

COMBINED FIRST FIXED OR NOT AFFECTED

9.18.3.55,9.18.4

4. Go through the steps from the “Problem 1. How to upgrade ASA/ASDM upgrade from the source version X to the target version Y?” section to upgrade the software.

Problem 5. “% ERROR: ASDM package is not digitally signed. Rejecting configuration.” error message

The “% ERROR: ASDM package is not digitally signed. Rejecting configuration.” error message when a new ASDM image is set using the **asdm image <image path>** command.

Troubleshoot – Recommended Actions

1. The ASA validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM is blocked and the message “%ERROR: Signature not valid for file disk0:/<filename>” is displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. Refer to the **Important Notes** section in Release Notes for Cisco ASDM, 7.17(x).

2. For ASA running on the Secure Firewall 3100, check the software Cisco bug ID CSCwc12322 “Digitally signed ASDM image verification error on FPR3100 platforms”.

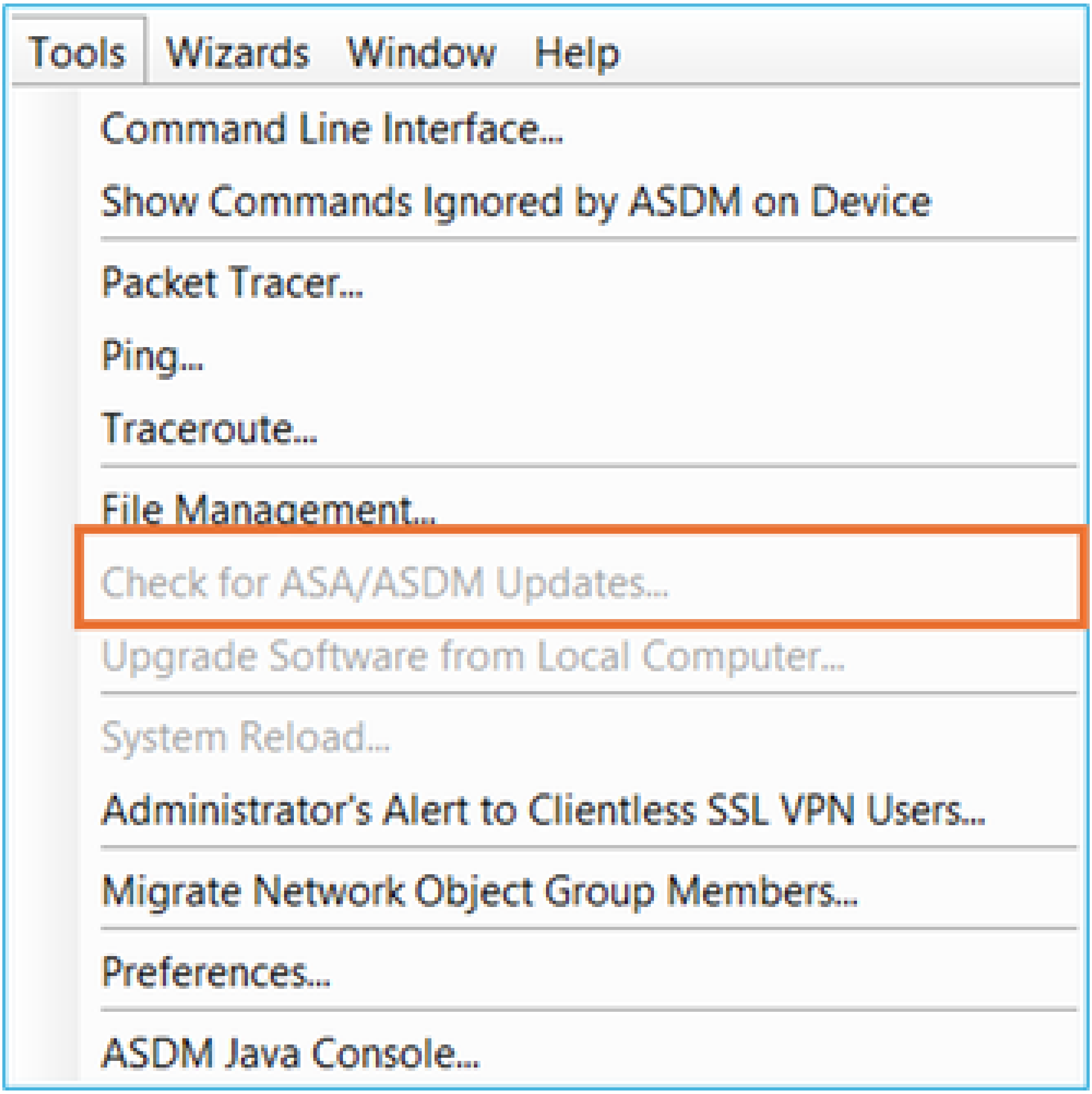
Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

References

- Release Notes for Cisco ASDM, 7.17(x)

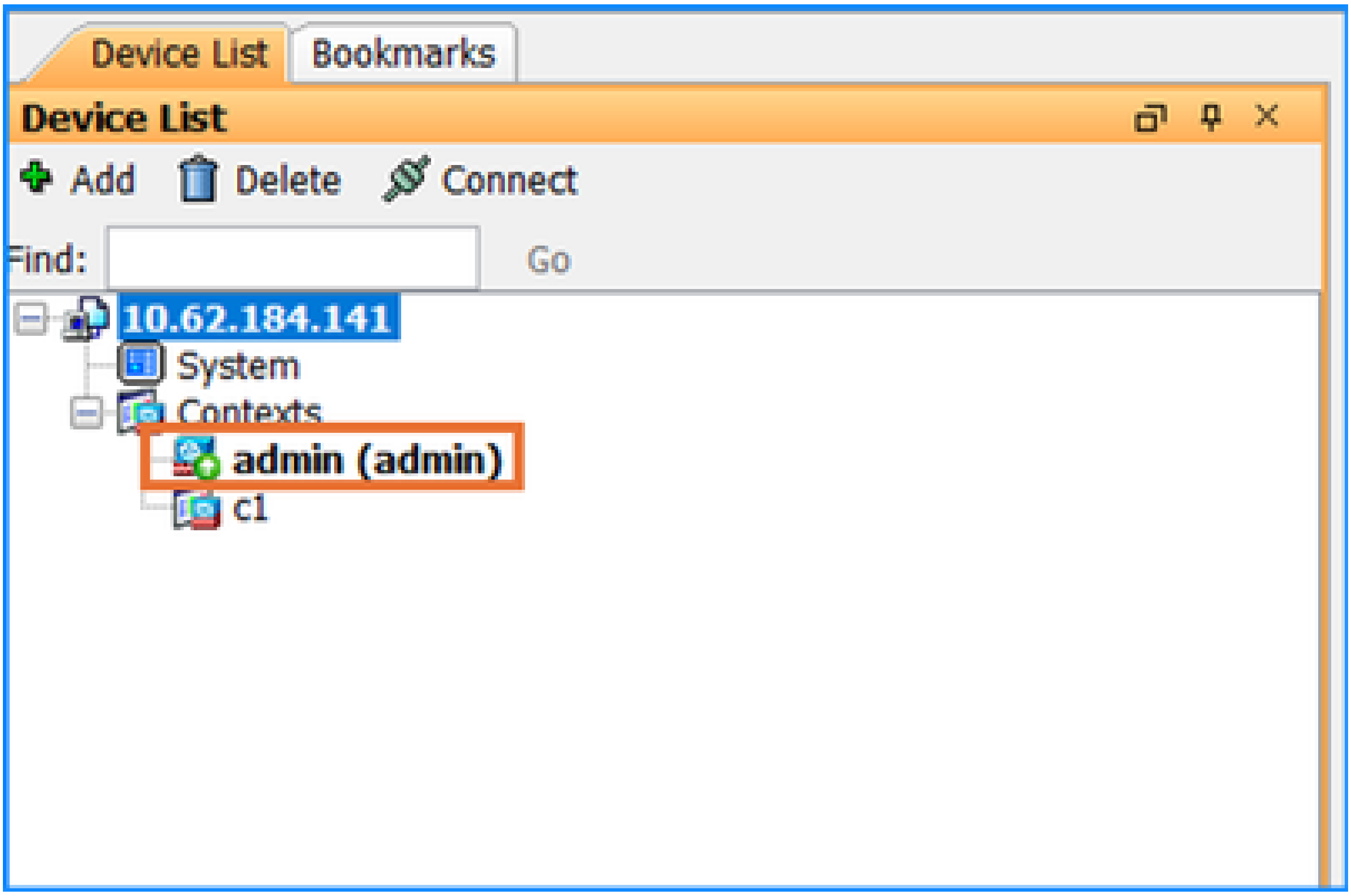
Problem 6. Unable to check for ASA/ASDM Updates in multiple context mode

The **Tools** > **Check for ASA/ASDM Updates** option is greyed out in multiple context mode:

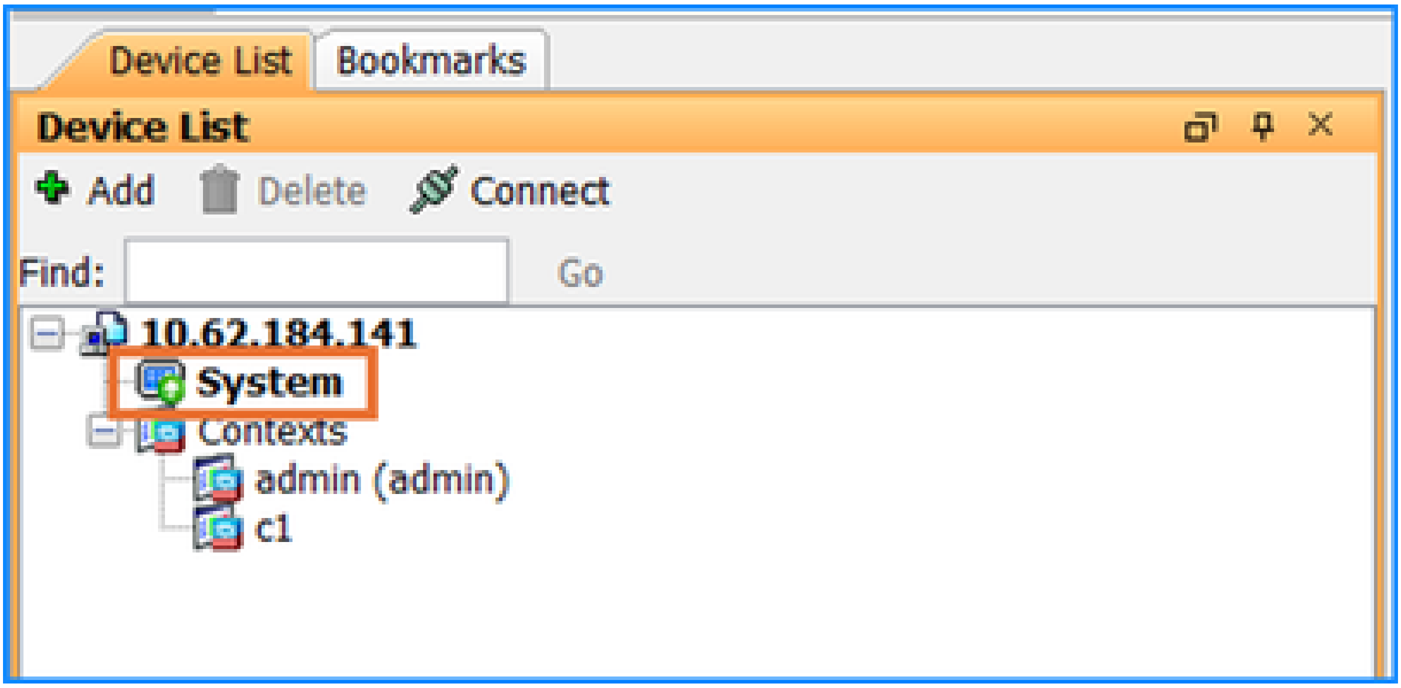

Tools
Wizards
Window
Help
Command Line Interface...
Show Commands Ignored by ASDM on Device
Packet Tracer...
Ping...
Traceroute...
File Management...
Check for ASA/ASDM Updates...
Upgrade Software from Local Computer...
System Reload...
Administrator's Alert to Clientless SSL VPN Users...
Migrate Network Object Group Members...
Preferences...
ASDM Java Console...

Troubleshoot – Recommended Actions

Usually, this option is greyed out because in the **Device List** tab the current select context is the **admin** context:



In this case, ensure to switch to the system context by double clicking on the **System** icon:



Problem 7. “Cisco's General Terms form have not been accepted or rejected to continue to download.” error message

The "Cisco's General Terms form have not been accepted or rejected to continue to download." error message is shown when the user tries to update the ASA/ASDM images via the **Tools** > **Check for**

ASA/ASDM Updates menu.

Troubleshoot – Recommended Actions

This error message is shown if the end-user license agreement (EULA) is not accepted by the user. To continue, ensure to accept the EULA.

References

- End-user license agreement (EULA)

Problem 8. Unable to download software for specific hardware

The Software Download page does not show some ASA/ASDM software versions for specific hardware.

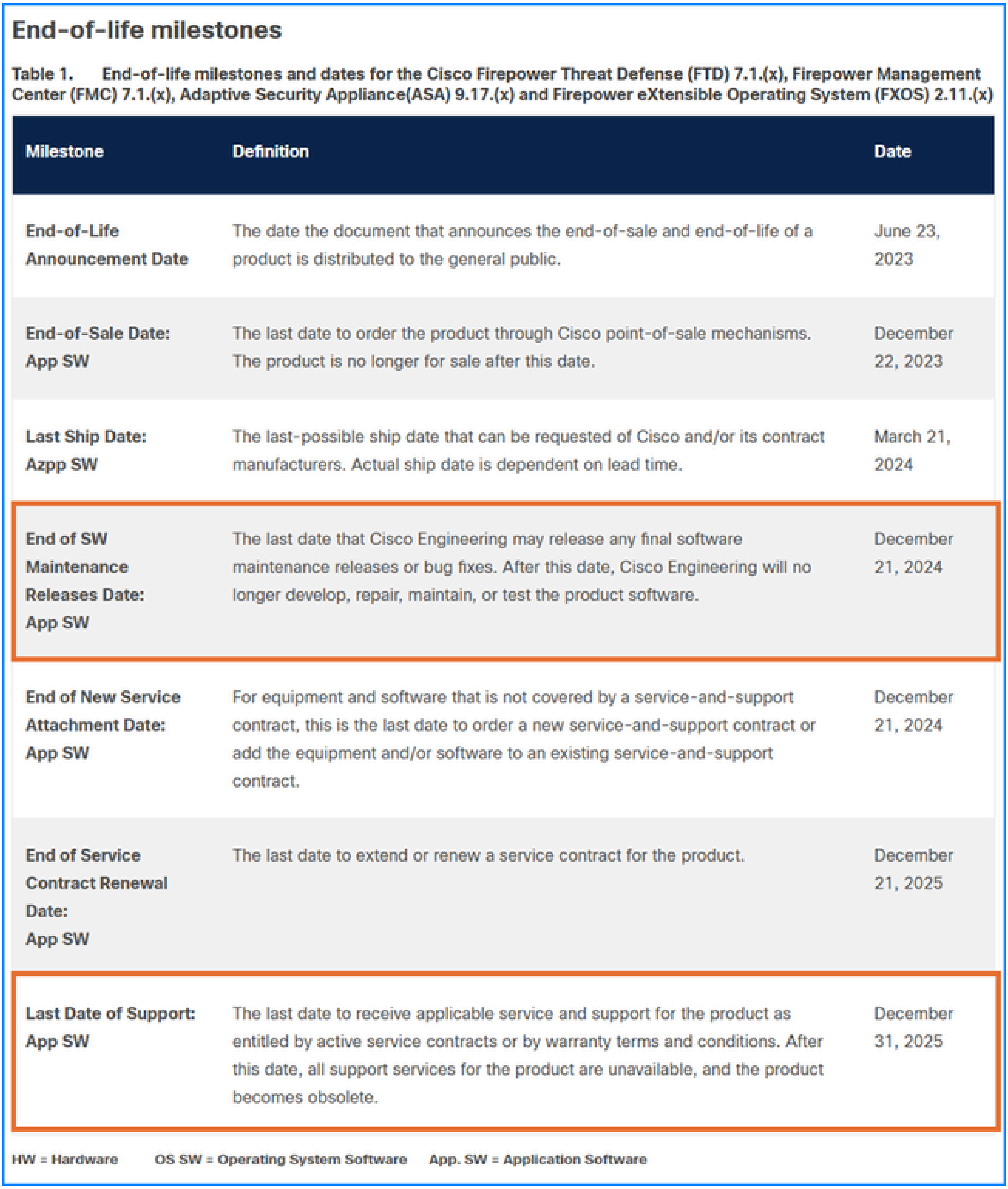
Troubleshoot – Recommended Actions

The availability of software for specific hardware mainly depends on the compatibility and the End-of-Life (EoL) milestones. In the case of incompatibility, EoL products or release deferrals, the software versions are usually not available for download.

Ensure to go through these steps to verify the compatibility and supported versions:

1. Check the compatibility between software and hardware versions. Refer to the Cisco Secure Firewall ASA Compatibility.
2. Check the End of SW Maintenance Releases Date and the Last Date of Support in the End-of-Life and End-of-Sale Notices

- **End of SW Maintenance Releases Date** - The last date that Cisco Engineering can release any final software maintenance releases or bug fixes. After this date, Cisco Engineering no longer develops, repairs, maintains, or tests the product software.
- **Last Date of Support** - The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.



End-of-life milestones

Table 1. End-of-life milestones and dates for the Cisco Firepower Threat Defense (FTD) 7.1.(x), Firepower Management Center (FMC) 7.1.(x), Adaptive Security Appliance(ASA) 9.17.(x) and Firepower eXtensible Operating System (FXOS) 2.11.(x)

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	June 23, 2023
End-of-Sale Date: App SW	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	December 22, 2023
Last Ship Date: Azpp SW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	March 21, 2024
End of SW Maintenance Releases Date: App SW	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.	December 21, 2024
End of New Service Attachment Date: App SW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	December 21, 2024
End of Service Contract Renewal Date: App SW	The last date to extend or renew a service contract for the product.	December 21, 2025
Last Date of Support: App SW	The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.	December 31, 2025

HW = Hardware OS SW = Operating System Software App. SW = Application Software

3. Check Cisco Secure Firewall ASA Release Notes and Cisco Secure Firewall ASDM Release Notes for deferral or removal of release.

References

- Cisco Secure Firewall ASA Compatibility
- End-of-Life and End-of-Sale Notices
- Cisco Secure Firewall ASA Release Notes

- Cisco Secure Firewall ASDM Release Notes

Problem 9. “Error occurred in performing File Transfer HTTP Response code -1” error message

The “Error occurred in performing File Transfer HTTP Response code -1” error message is shown when the user uploads a file to the firewall using the ASDM **Tools** > **File Management** option.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCvf85831 “ASDM error "Error occurred in performing File Transfer HTTP Response code -1" during image upload”.

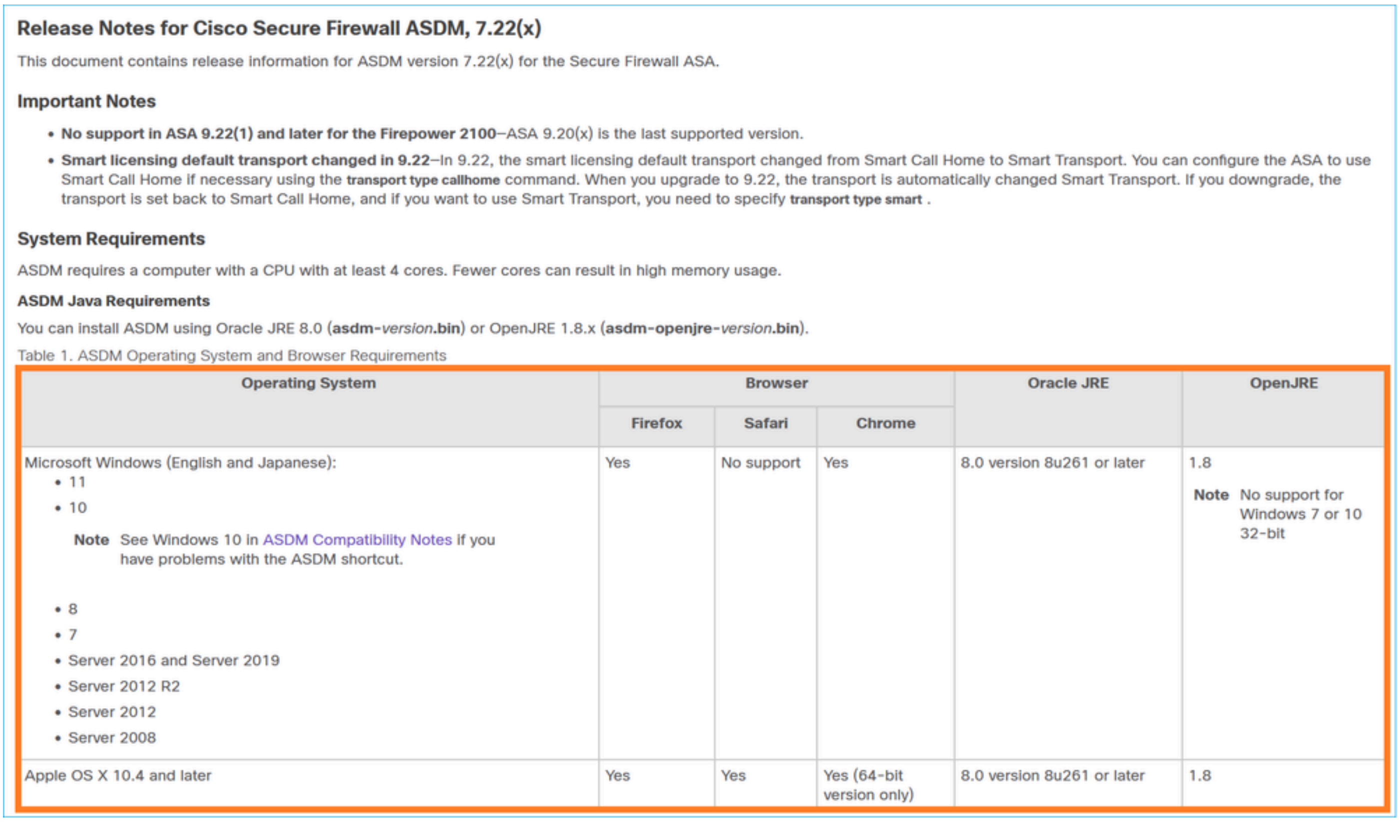
ASDM Compatibility Problems

This section covers the most common ASDM compatibility-related problems.

In general, ASDM must be compatible with these components:

- ASA
- Java
- Operating System (OS)
- Browser
- SFR module (if it is used)

Thus, before installing or upgrading ASDM, it is highly recommended to always check first this table:



Release Notes for Cisco Secure Firewall ASDM, 7.22(x)

This document contains release information for ASDM version 7.22(x) for the Secure Firewall ASA.

Important Notes

- **No support in ASA 9.22(1) and later for the Firepower 2100**—ASA 9.20(x) is the last supported version.
- **Smart licensing default transport changed in 9.22**—In 9.22, the smart licensing default transport changed from Smart Call Home to Smart Transport. You can configure the ASA to use Smart Call Home if necessary using the **transport type callhome** command. When you upgrade to 9.22, the transport is automatically changed Smart Transport. If you downgrade, the transport is set back to Smart Call Home, and if you want to use Smart Transport, you need to specify **transport type smart** .

System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0 (**asdm-*version*.bin**) or OpenJRE 1.8.x (**asdm-openjre-*version*.bin**).

Table 1. ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): • 11 • 10 **Note** See Windows 10 in ASDM Compatibility Notes if you have problems with the ASDM shortcut. • 8 • 7 • Server 2016 and Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	Yes	No support	Yes	8.0 version 8u261 or later	1.8 **Note** No support for Windows 7 or 10 32-bit
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0 version 8u261 or later	1.8

And then the ASA and ASDM Compatibility Per Model table, for example:

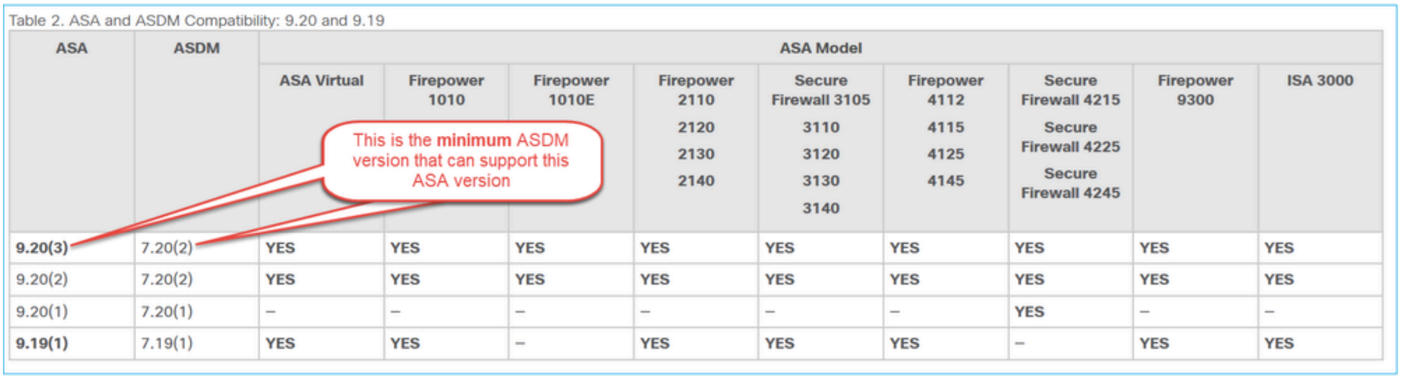


Table 2. ASA and ASDM Compatibility: 9.20 and 9.19

ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010	Firepower 1010E	Firepower 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Firepower 9300	ISA 3000
9.20(3)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(2)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(1)	7.20(1)	–	–	–	–	–	–	YES	–	–
9.19(1)	7.19(1)	YES	YES	–	YES	YES	YES	–	YES	YES

This is the minimum ASDM version that can support this ASA version

Notes:

New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA.

Example 1

You cannot use ASDM 7.17 with ASA 9.18. For ASA interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.22(1.2) with ASDM 7.22(1).

Example 2

You have ASAS 9.8(4)32. You can use ASDM 7.19(1) to manage it since ASDM is backward compatible unless otherwise mentioned in the ASDM release notes.

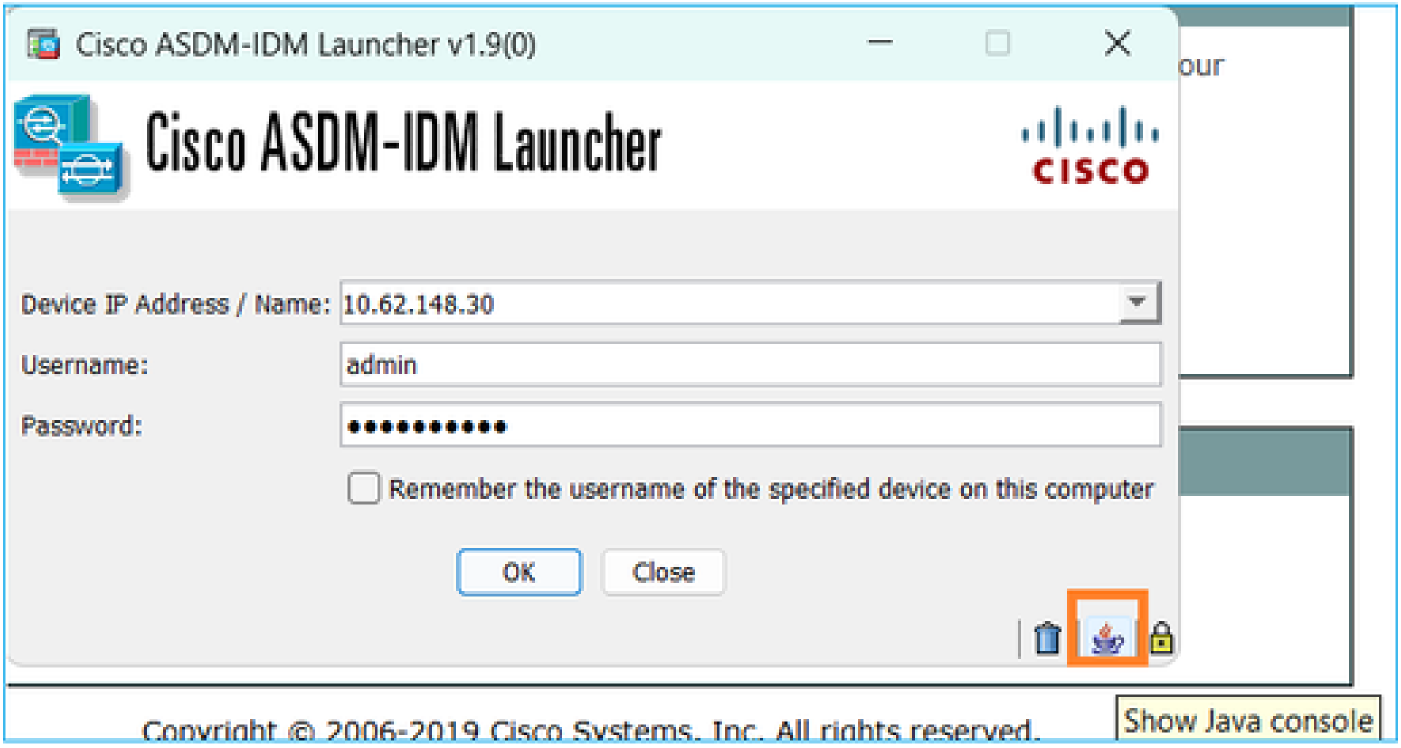
References

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25469
- https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#id_65776

Problem 1. Incompatible Java version

Troubleshoot – Recommended Steps

Check the Java console logs:



Cisco ASDM-IDM Launcher v1.9(0)

Cisco ASDM-IDM Launcher

Device IP Address / Name: 10.62.148.30

Username: admin

Password: ●●●●●●●●●●●

□ Remember the username of the specified device on this computer

OK
Close
Show Java console
Copyright © 2006-2019 Cisco Systems, Inc. All rights reserved.

Then check the Java and ASA compatibility guides:

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25469
- https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#id_65776

Problem 2. Incompatible ASA and ASDM version

If you run into incompatible ASA and ASDM versions you can lose access to ASDM UI.

Troubleshoot – Recommended Steps

You need to install the ASDM version from the CLI of the device, copy the image into the flash of the ASA via TFTP, and set the ASDM image using the command "**asdm image**" as explained in the guide below:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/ar-az-commands.html#wp3551901007

Example

<#root>

```
asa#
```

```
copy tftp flash



Address or name of remote host []? 10.62.146.125
Source filename []? asdm-7221.bin
Destination filename [asdm-7221.bin]?

Verifying file disk0:/asdm-7221.bin...
Writing file disk0:/asdm-7221.bin...
INFO: No digital signature found
126659176 bytes copied in 70.590 secs (1809416 bytes/sec)
```

<#root>

```
asa#

config terminal


asa(config)#

asdm image disk0:/asdm-7151-150.bin


asa(config)#

copy run start


Source filename [running-config]?
Cryptochecksum: afae0454 bf24b2ac 1126e026 b1a26a2c

4303 bytes copied in 0.210 secs
```

Problem 3. ASDM and OpenJDK Support

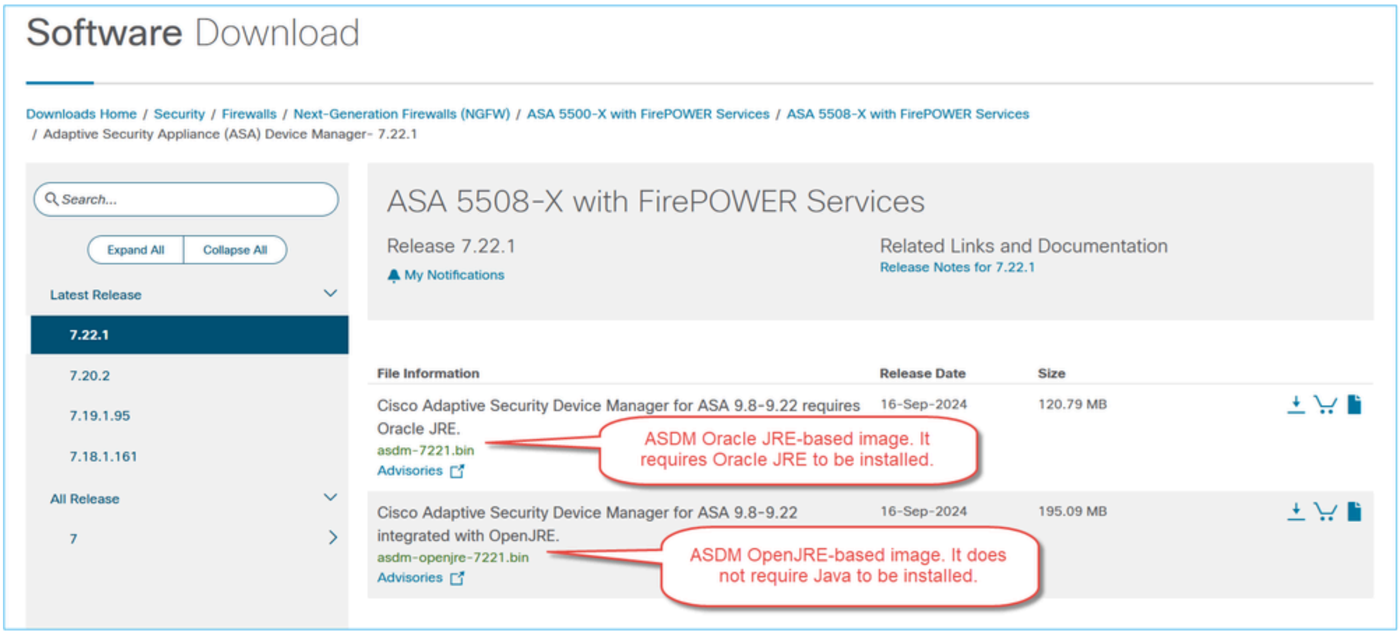
Cisco ASDM image does not support OpenJDK officially. Thus, there are 2 available options:

- Oracle JRE: Contains the Java Web Start runtime to launch ASDM on the host PC. To use this method you need the 64-bit Oracle JRE to be installed on the local PC. You can download this at the official website of Java.
- OpenJRE: The open JRE image is the same as the Oracle one, but the difference is that you don’t need to install the 64-bit Oracle JRE on the local PC since the image itself has the Java Web Start feature to launch the ASDM. This is the reason why the size of the OpenJRE image is greater than the Oracle JRE. Note that it is expected to see the OpenJRE using a bit older Java release, as they are compiled with the latest stable version available at the beginning of the ASDM openJRE development cycle.

Oracle JRE vs OpenJRE

	Oracle JRE	**OpenJRE**
Requires Java to be installed on the	Yes	No (it has its own Java integrated)

end host		
Proprietary	Yes	No (open source)
Image size	Medium	Bigger since it also has Java integrated
Image name	asdm-xxxx.bin	asdm-openjre-xxxx.bin



Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / ASA 5500-X with FirePOWER Services / ASA 5508-X with FirePOWER Services / Adaptive Security Appliance (ASA) Device Manager- 7.22.1

ASA 5508-X with FirePOWER Services

Release 7.22.1

Related Links and Documentation
Release Notes for 7.22.1

File Information	Release Date	Size
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 requires Oracle JRE. asdm-7221.bin	16-Sep-2024	120.79 MB
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin	16-Sep-2024	195.09 MB

ASDM Oracle JRE-based image. It requires Oracle JRE to be installed.

ASDM OpenJRE-based image. It does not require Java to be installed.

Tip: If you decide to change the ASDM launcher version, first uninstall the existing ASDM launcher and then install the new by connecting to the ASA via HTTPS.

References

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- OpenJDK: Full development and runtime environment, open-source, GPL license.
- Oracle JRE: Runtime environment only, proprietary license, requires a commercial license for production use.
- OpenJRE: Runtime environment only, open-source, GPL license.
- https://www.oracle.com/java/technologies/javase/jre8-readme.html

Problem 4. ASDM and Java Azul Zulu Compatibility

Oracle JRE-based ASDM images do not support Java Azul Zulu. On the other hand, ASDM OpenJRE-based images come Azul Zulu integration. Check 'Problem 3' recommendations for the available options.

Problem 5. WARNING: Signature not found in file disk0:/asdm-xxx.bin

Example:

<#root>

```
asa#

copy tftp flash:


Address or name of remote host [192.0.2.5]?
Source filename []? asdm-7171.bin
Destination filename [asdm-7171.bin]?

Accessing ftp://192.0.2.5/asdm-7171.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/asdm-7171.bin...

%WARNING: Signature not found in file disk0:/asdm-7171.bin.
```

Troubleshoot – Recommended Steps

This is typically an ASA vs ASDM compatibility problem. Check the ASDM compatibility guide and ensure your ASDM is compatible with the ASA image. You can find the ASA and ASDM compatibility matrix at:

https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#id_65776

Problem 6. “% ERROR: ASDM package is not digitally signed. Rejecting configuration.”

This error message can be shown when a new ASDM image is set using the **asdm image <image path>** command.

Troubleshoot – Recommended Actions

1. The ASA validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM is blocked and the message “%ERROR: Signature not valid for file disk0:/<filename>” is displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. Refer to the **Important Notes** section in Release Notes for Cisco ASDM, 7.17(x).

2. Update the Java version on your host PC.

3. For ASA running on the Secure Firewall 3100, check the software Cisco bug ID CSCwc12322 “Digitally signed ASDM image verification error on FPR3100 platforms”

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc12322

Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 7. “%ERROR: Signature not valid for file disk0:/<filename>”

The error is shown during the file copy, for example:

<#root>

```
asa#

copy tftp://cisco:cisco@192.0.2.1/cisco-asa-fp2k.9.20.3.7.SPA



Address or name of remote host [192.0.2.1]?
Source filename [cisco-asa-fp2k.9.20.3.7.SPA]?
Destination filename [cisco-asa-fp2k.9.20.3.7.SPA]?

Accessing tftp://cisco:<password>@192.0.2.1/cisco-asa-fp2k.9.20.3.7.SPA...
!!!!!!!!!!!!!!!!!!!...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying file disk0:/cisco-asa-fp2k.9.20.3.7.SPA...

%ERROR: Signature not valid for file disk0:/cisco-asa-fp2k.9.20.3.7.SPA.
```

Troubleshoot – Recommended Actions

ASA 9.14(4.14) and later requires ASDM 7.18(1.152) or later. The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image than 7.18(1.152) with an ASA version with this fix, ASDM is blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" is displayed at the ASA CLI.

This change was introduced due to Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability (CVE ID CVE-2022-20829)

- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb05291
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb05264

In case the device operates in Platform Mode go through the instructions from this document to upload the image: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_zp4_dzj_cjb

References

- ASDM release notes: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3_ngz_vhb
- ASA upgrade guide: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task_E9EE51964590499999B1D976F66E2771

Problem 8. Secure Firewall Posture (Hostscan) Compatibility

Hostscan version depends more on AnyConnect version than ASA version. You can find both the versions here: Software Download - Cisco Systems:

https://software.cisco.com/download/home/283000185

Problem 9. Latest supported version

Troubleshoot – Recommended Actions

If you want to know the latest supported ASDM version for your firewall there are mainly two documents to check:

- ASDM release notes: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3_ngz_vhb

Specifically, the ASA Model table

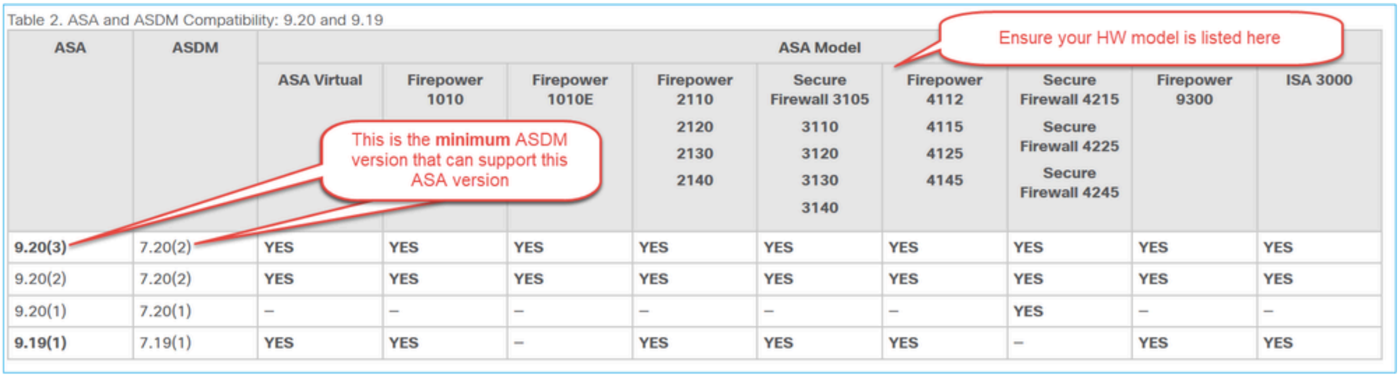


Table 2. ASA and ASDM Compatibility: 9.20 and 9.19

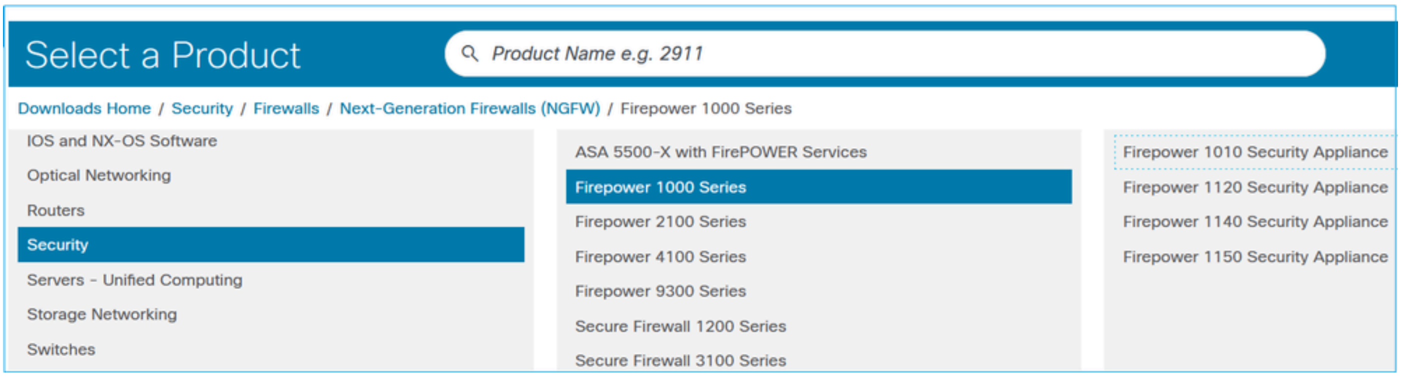
ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010	Firepower 1010E	Firepower 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Firepower 9300	ISA 3000
9.20(3)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(2)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(1)	7.20(1)	–	–	–	–	–	–	YES	–	–
9.19(1)	7.19(1)	YES	YES	–	YES	YES	YES	–	YES	YES

Ensure your HW model is listed here

This is the **minimum** ASDM version that can support this ASA version

The second document is the SW download page:

https://software.cisco.com/download/home/286291275



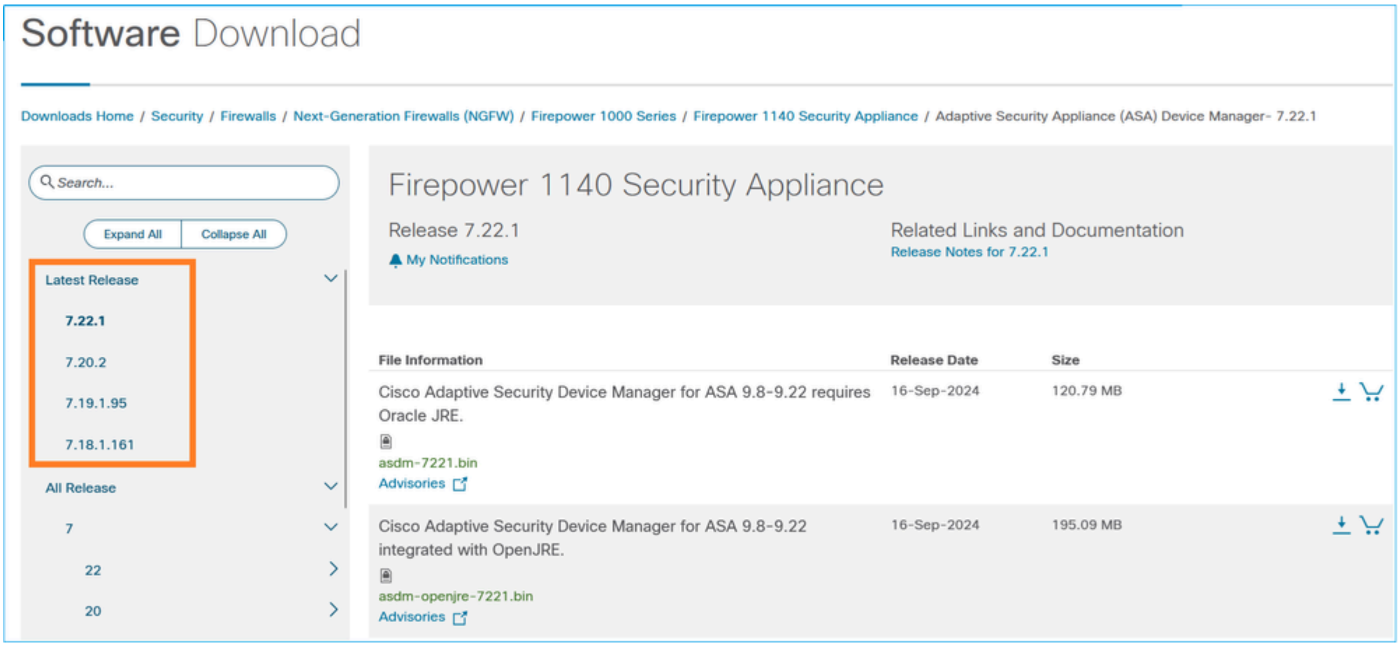
Select a Product

Product Name e.g. 2911

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower 1000 Series

IOS and NX-OS Software	ASA 5500-X with FirePOWER Services	Firepower 1010 Security Appliance
Optical Networking	**Firepower 1000 Series**	Firepower 1120 Security Appliance
Routers	Firepower 2100 Series	Firepower 1140 Security Appliance
Security	Firepower 4100 Series	Firepower 1150 Security Appliance
Servers - Unified Computing	Firepower 9300 Series	
Storage Networking	Secure Firewall 1200 Series	
Switches	Secure Firewall 3100 Series	

You can find the latest ASDM versions per SW train supported by your HW, for example:



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower 1000 Series / Firepower 1140 Security Appliance / Adaptive Security Appliance (ASA) Device Manager- 7.22.1

Firepower 1140 Security Appliance

Release 7.22.1

My Notifications

Related Links and Documentation

Release Notes for 7.22.1

File Information	Release Date	Size
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 requires Oracle JRE. asdm-7221.bin Advisories	16-Sep-2024	120.79 MB
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin Advisories	16-Sep-2024	195.09 MB

Problem 10. ASDM support on Linux

Troubleshoot – Recommended Actions

Linux is not officially supported.

Related enhancement:

Cisco bug ID CSCwk67345
ENH: Include Linux in the list of supported OSs

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwk67345

Problem 11. ASDM end of support

Troubleshoot – Recommended Actions

Consult the ASA/ASDM End-of-Life and End-of-Sale Notices:

https://www.cisco.com/c/en/us/products/security/asa-firepower-services/eos-eol-notice-listing.html

ASDM License Problems

This section covers the most common ASDM license-related problems.

Smart Licensing model is used by:

- Firepower 4100/9300 chassis registration: License Management for the ASA
- ASAv, Firepower 1000, Firepower 2100, Firepower 9300, and Firepower 4100: Licenses: Smart Software Licensing (ASAv, ASA on Firepower)

All other models use Product Authorization Key (PAK) Licensing

References

- Cisco Secure Firewall ASA Series Feature Licenses - Model Guidelines

https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/licenseroadmap.html

Problem 1. 3DES/AES Smart License is Missing

ASDM requires Strong Encryption license (3DES/AES) on ASA unless you access it using the management interface. In order to enable ASDM access over a data interface you need to get the 3DES/AES license.

To request a 3DES/AES license from Cisco:

1. Go to https://www.cisco.com/go/license
2. Click **Continue to Product License Registration.**
3. In the Licensing Portal, click **Get Other Licenses** next to the text field.
4. Choose **IPS, Crypto, Other**... from the drop-down list.
5. Type **ASA** in to the **Search by Keyword** field.
6. Select **Cisco ASA 3DES/AES License** in the **Product** list, and click **Next**.
7. Enter the serial number of the ASA, and go through the prompts to request a 3DES/AES license for the ASA.

Troubleshoot – Recommended Actions

To enable the license and register to the Cisco Smart Licensing portal, ensure that these items are in place:

- The ASA clock shows the correct time. The recommendation is to use an NTP server.
- Routing towards the Cisco Smart Licensing portal.
- HTTPS traffic is not blocked from the firewall to the licensing portal. A capture collection on the firewall can confirm this.
- If there is a need to use an HTTP proxy server include the necessary command, for example:

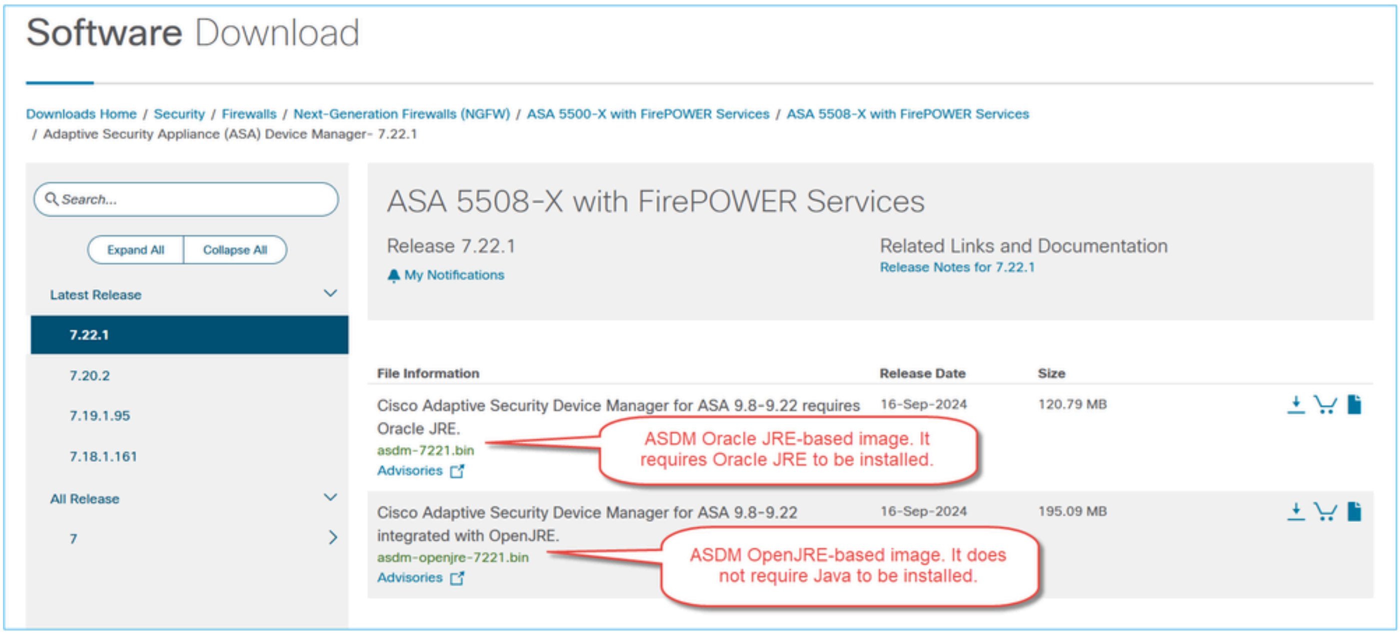
```
<#root>

ciscoasa(config)#

call-home


ciscoasa(cfg-call-home)#

http-proxy 10.1.1.1 port 443
```

Problem 2. Oracle Java JRE Licensing Requirements

Troubleshoot – Recommended Actions

ASDM .bin image file comes in two flavors:

- Oracle JRE: Contains the Java Web Start runtime to launch ASDM on the host PC. To use this method you need the 64-bit Oracle JRE to be installed on the local PC. You can download this at the official website of Java.
- OpenJRE: The open JRE image is the same as the Oracle one, but the difference is that you don't need to install the 64-bit Oracle JRE on the local PC since the image itself has the Java Web Start feature to launch the ASDM.



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / ASA 5500-X with FirePOWER Services / ASA 5508-X with FirePOWER Services / Adaptive Security Appliance (ASA) Device Manager- 7.22.1

ASA 5508-X with FirePOWER Services

Release 7.22.1

Related Links and Documentation

Release Notes for 7.22.1

File Information	Release Date	Size
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 requires Oracle JRE. asdm-7221.bin Advisories	16-Sep-2024	120.79 MB
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin Advisories	16-Sep-2024	195.09 MB

ASDM Oracle JRE-based image. It requires Oracle JRE to be installed.

ASDM OpenJRE-based image. It does not require Java to be installed.

In case you decide to use the Oracle-based ASDM image, you need to have a Java license when you use it for non-Personal uses. Per Oracle Java SE Licensing FAQ:

Personal use is using Java on a desktop or laptop computer to do things such as to play games or run other personal applications. If you are using Java on a desktop or laptop computer as part of any business operations, that is not personal use. For example, you could use a Java productivity application to do your own homework or your personal taxes, but you could not use it to do your business accounting.

If you don't want to apply any Java licenses you can use the OpenJRE-based ASDM image.

References

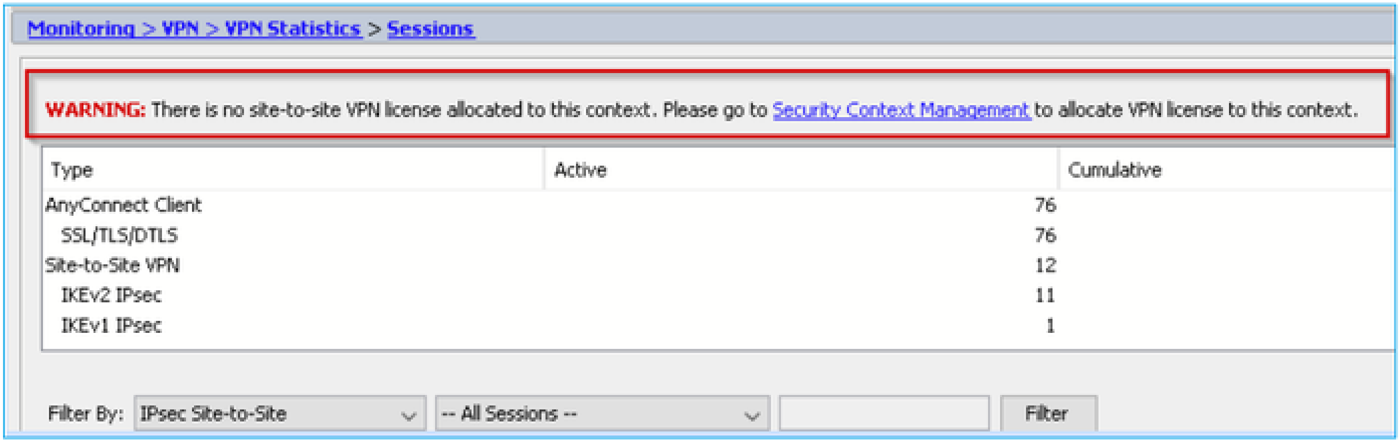
- https://www.oracle.com/java/technologies/javase/jdk-faqs.html
- ASDM Java Requirements for ASDM 7.22: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- ASDM Compatibility Notes for ASDM 7.22: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476

Note: Check the release notes for the ASDM version you use.

Problem 3. ASDM Warning about site-to-site VPN License in Multi-Context Mode

The ASDM displays this:

WARNING: There is no site-to-site VPN license allocated to this context. Please go to Security Context Management to allocate VPN license to this context.



Monitoring > VPN > VPN Statistics > Sessions

WARNING: There is no site-to-site VPN license allocated to this context. Please go to Security Context Management to allocate VPN license to this context.

Type	Active	Cumulative
AnyConnect Client	76	
SSL/TLS/DTLS	76	
Site-to-Site VPN	12	
IKEv2 IPsec	11	
IKEv1 IPsec	1	

Filter By: IPsec Site-to-Site; -- All Sessions --

Troubleshoot – Recommended Actions

This is a cosmetic software defect tracked by:

Cisco bug ID CSCvj66962

ASDM 7.9(2) ASA 9.6(4)8 multi context L2L persistent error

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj66962

You can subscribe to the defect, so you receive a notification on defect updates.

References

- ASDM Configuration Guides
- Cisco ASA and ASDM Compatibility per Model