Fehlerbehebung bei ASDM-Lizenz-, Upgrade- und Kompatibilitätsproblemen

Inhalt

Einleitung

In diesem Dokument wird der Fehlerbehebungsprozess für ASDM-Lizenz-, Upgrade- und

Kompatibilitätsprobleme beschrieben.

Hintergrund

Das Dokument ist zusammen mit den folgenden Dokumenten Teil der ASDM-Reihe (Adaptive Security Appliance Device Manager) zur Fehlerbehebung:

- Fehlerbehebung bei ASDM-Startproblemen
- Fehlerbehebung bei ASDM-Konfiguration, Authentifizierung und anderen Problemen
- Fehlerbehebung bei ASDM TLS-Sicherheits-, Zertifikat- und Schwachstellenproblemen

ASDM-Upgrade-Probleme

Problem 1. Wie führe ich ein Upgrade von ASA/ASDM von der Quellversion X auf die Zielversion Y durch?

Der Benutzer benötigt Unterstützung bei einem ASA/ASDM-Upgrade von der Quellversion X auf die Zielversion Y.

Fehlerbehebung - empfohlene Maßnahmen

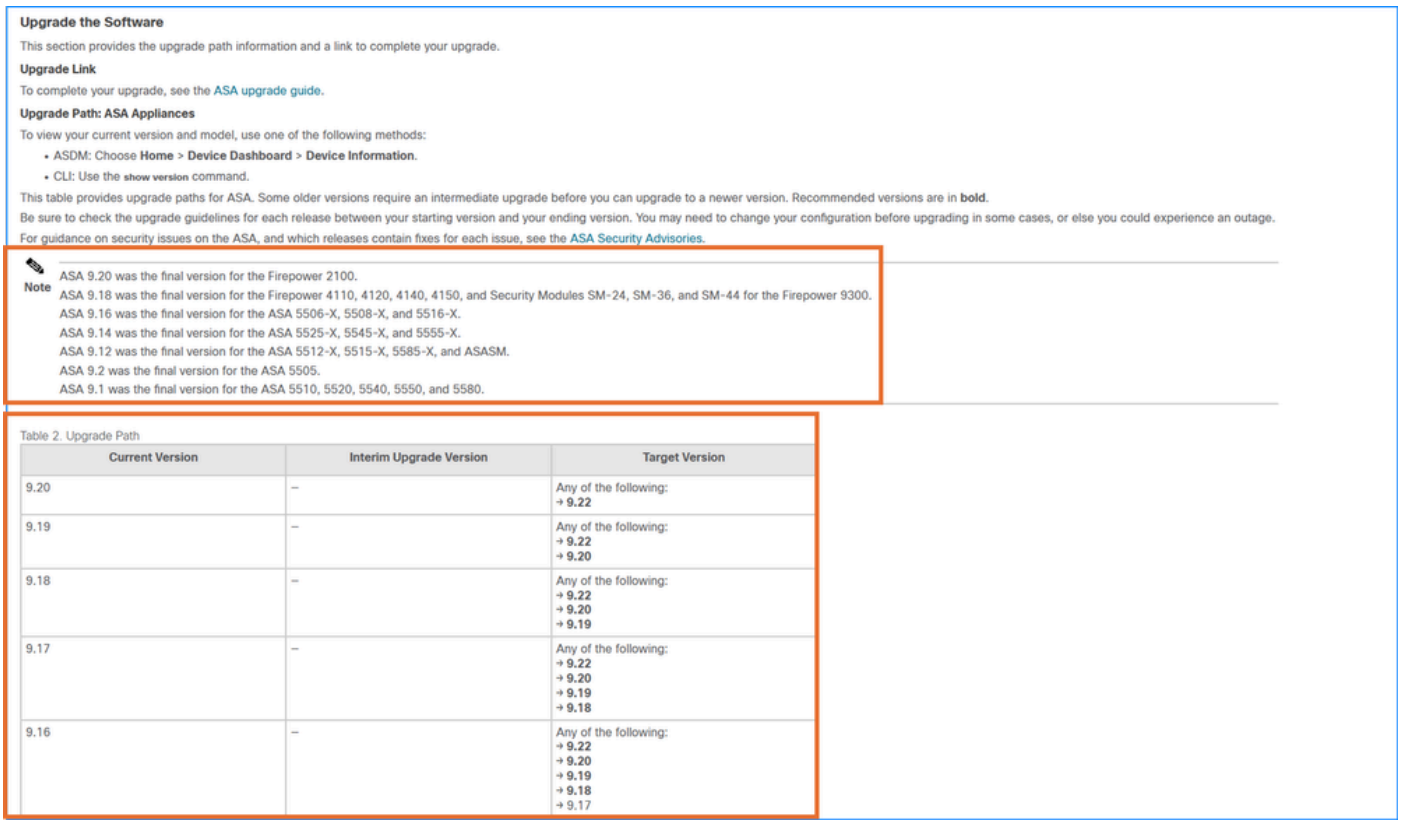
1. Stellen Sie sicher, dass die ASA-, ASDM-, Betriebssystem- und Java-Versionen mit der Zielversion kompatibel sind. Siehe unter Cisco Secure Firewall ASA - Versionshinweise, Cisco Secure Firewall ASDM - Versionshinweise, Cisco Secure Firewall ASA-Kompatibilität.

Die Versionen ASA, ASDM, Betriebssystem und Java müssen kompatibel sein, und die Zielversionen müssen auf bestimmter Hardware unterstützt werden.
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

2. Stellen Sie bei ASA-Geräten mit Firepower 4100/9300 sicher, dass das FXOS (FirePOWER eXtensible Operating System) und die ASA-Softwareversionen kompatibel sind. Weitere Informationen finden Sie unter Cisco FirePOWER 4100/9300 FXOS-Kompatibilität.

3. Machen Sie sich mit den Änderungen in der Zielversion vertraut, indem Sie Cisco Secure Firewall ASA - Versionshinweise, Cisco Secure Firewall ASDM - Versionshinweise. Im Fall von Firepower 4100/9300, machen Sie sich auch mit den Änderungen in FXOS vertraut, indem Sie die FXOS - Versionshinweise.

4. Überprüfen Sie den Upgrade-Pfad in den Versionshinweisen. In diesem Beispiel enthält die Tabelle 2 in den Versionshinweisen für Version 7.22 den Upgrade-Pfad von früheren Versionen auf die Zielversion:



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.

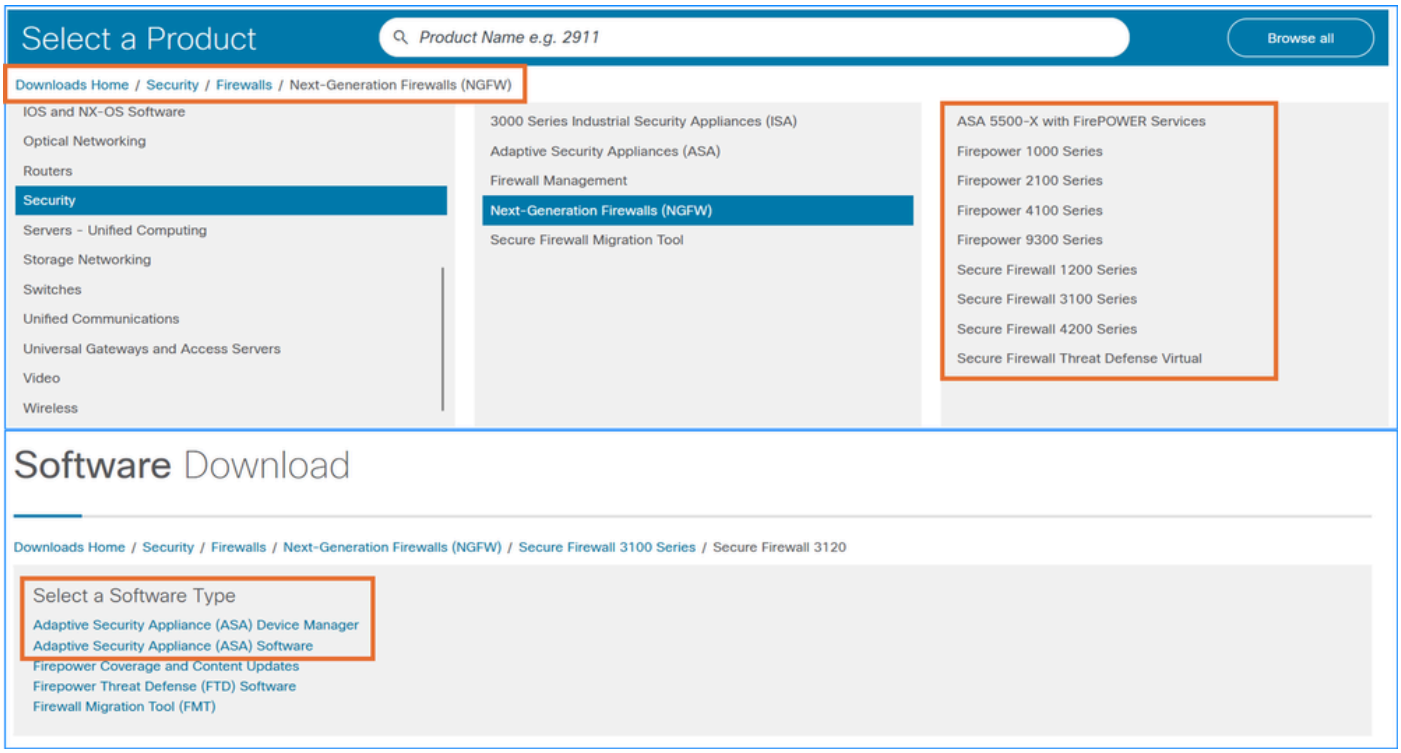
Note

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. Sobald die Kompatibilitätsanforderungen erfüllt sind, laden Sie die Zielversionen ASA/ASDM und FXOS (nur Firepower 4100/9300) von der Seite für den Software-Download herunter. Wählen Sie die in diesem Beispiel gezeigten Hardwaremodelle aus. Die empfohlenen Versionen sind mit einem goldenen Stern gekennzeichnet:



6. Stellen Sie sicher, durch das Kapitel zu gehen: Planen des Upgrades und Kapitel: Aktualisieren Sie die ASA im Cisco Secure Firewall ASA-Upgrade-Leitfaden.

Referenzen

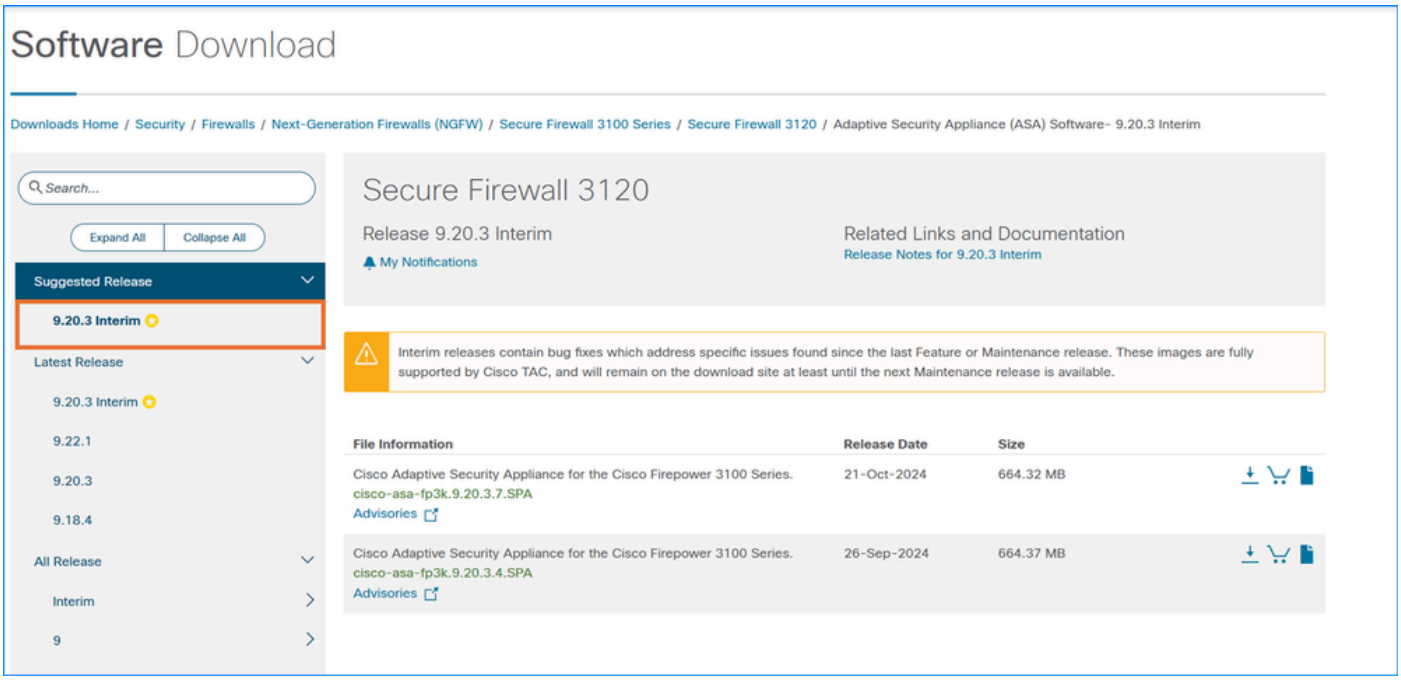
- Cisco Secure Firewall ASA - Versionshinweise
- Cisco Secure Firewall ASDM - Versionshinweise
- Cisco Secure Firewall ASA-Kompatibilität
- Kompatibilität mit Cisco FirePOWER 4100/9300 FXOS
- Cisco Secure Firewall ASA Upgrade-Leitfaden

Problem 2. Welche Versionen werden für ASA/ASDM empfohlen?

Der Benutzer fragt nach den empfohlenen Versionen für ASA/ASDM.

Fehlerbehebung - empfohlene Maßnahmen

Das Cisco TAC gibt keine Empfehlungen zu den Softwareversionen ab. Die von Cisco empfohlene Version basiert auf der Qualität, Stabilität und Langlebigkeit der Software. Die empfohlenen Versionen sind mit einem goldenen Stern markiert, wie unten gezeigt:

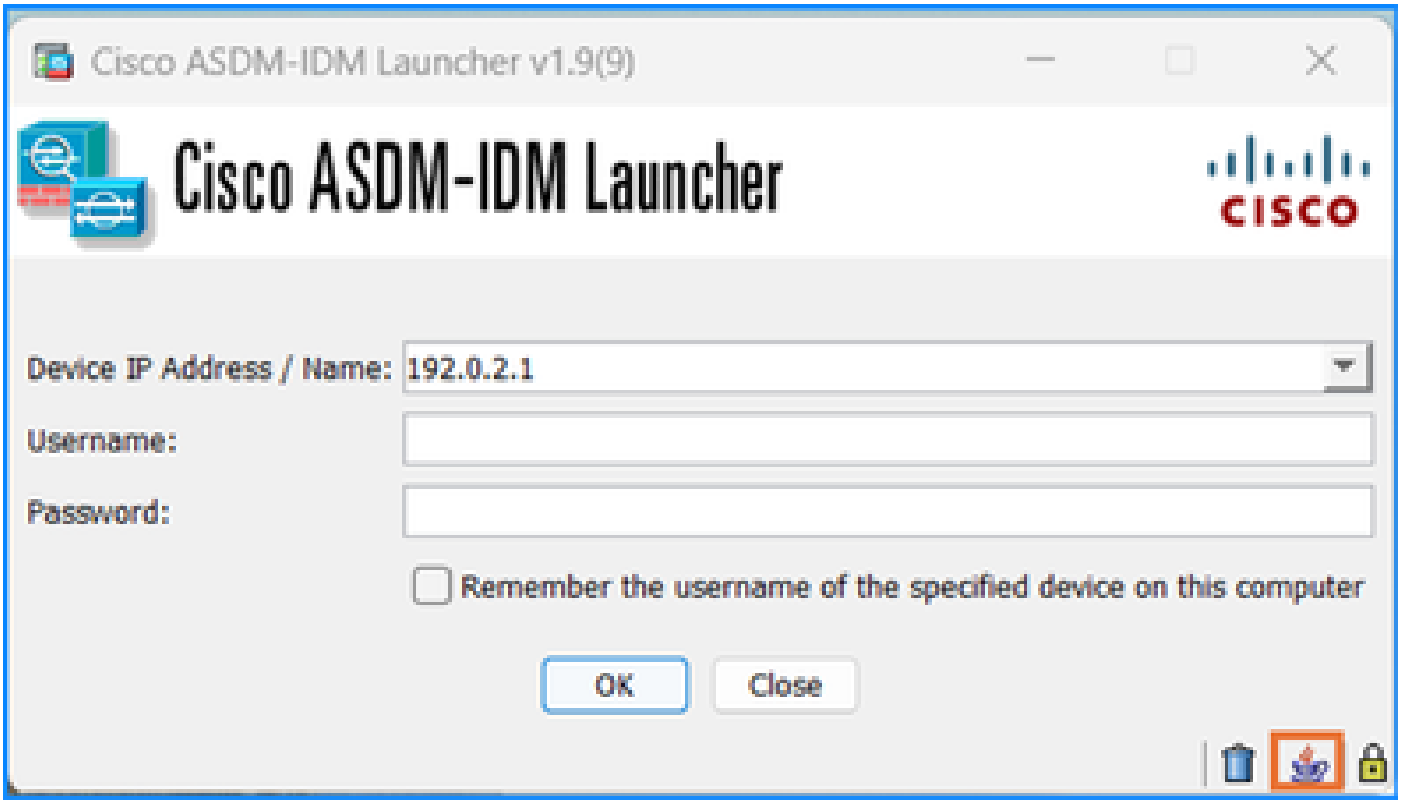


Problem 3: Fehler bei der Prüfung von ASA-/ASDM-Updates im ASDM. Extras > Auf ASA-/ASDM-Updates überprüfen

Die Prüfung auf ASA-/ASDM-Updates im ASDM über Tools > Check for ASA-/ASDM-Updates schlägt fehl. Im Einzelnen werden folgende Symptome beobachtet:

1. Das Fenster Netzwerkkennwort eingeben wird nach dem Klicken auf die Schaltfläche Anmelden erneut angezeigt, auch wenn die richtigen Anmeldeinformationen angegeben wurden.

2. In den Java-Konsolenprotokollen wird der Fehler "Meta data request failed" (Anforderung von Metadaten fehlgeschlagen) angezeigt:



<#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 fa
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 HT
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.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCvf91260 "ASDM: Das Upgrade von CCO funktioniert aufgrund nicht ignorierbarer Felder nicht. "Anfrage für Metadaten fehlgeschlagen". Die Problemumgehung besteht darin, Bilder direkt von der Download-Seite herunterzuladen und in die Firewall hochzuladen.

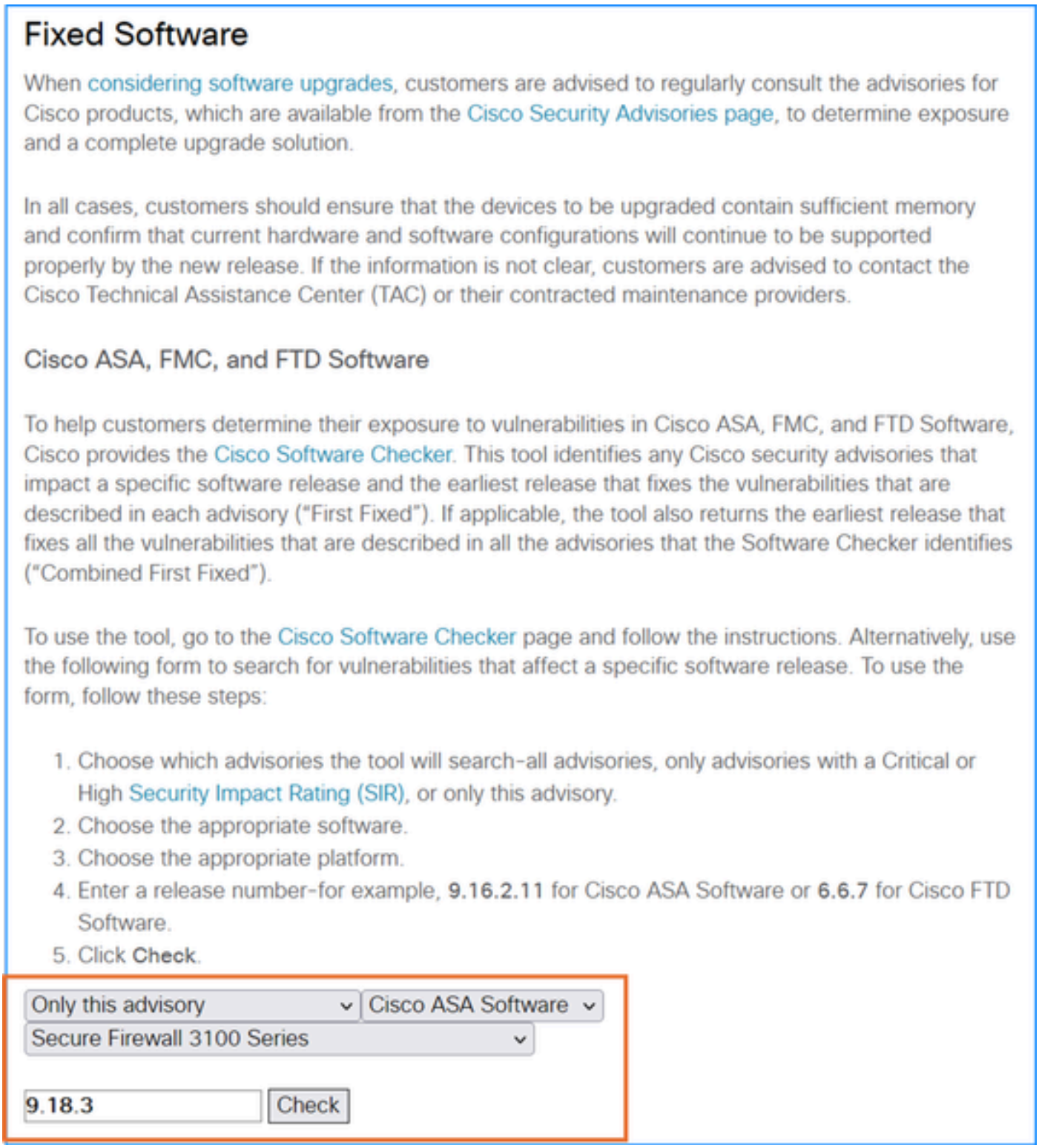
Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 4. Welche Versionen enthalten korrigierte für spezifische Schwachstellen?

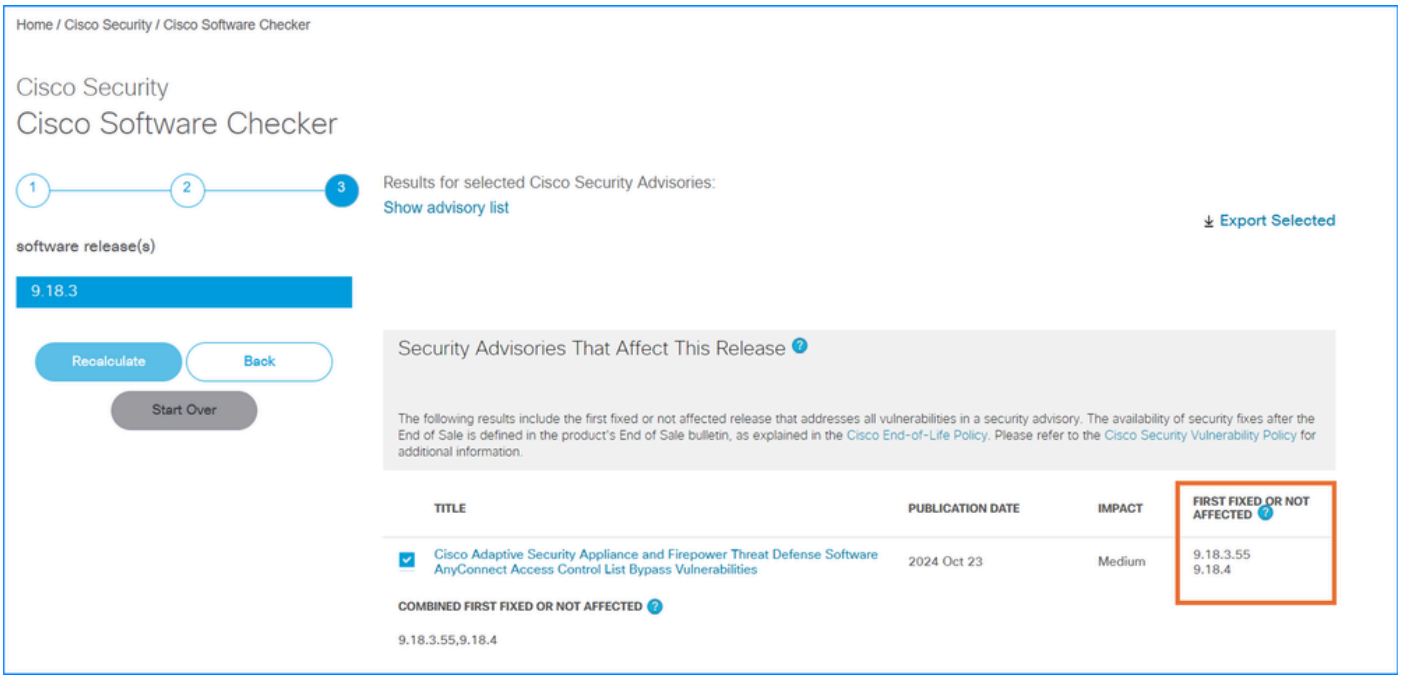
Der Benutzer erkundigt sich nach den korrigierten Versionen spezifischer Schwachstellen.

Fehlerbehebung - empfohlene Maßnahmen

1. Überprüfen Sie die Sicherheitsankündigung für die betroffenen Produkte.
2. Geben Sie in der Sicherheitsempfehlung die vorhandene Hardware- und Softwareversion an die Softwareprüfung an, und klicken Sie auf Prüfen:



3. Wenn die feste Version verfügbar ist, beachten Sie die Versionen in der Spalte ERSTE FESTE ODER NICHT BETROFFENE:



4. Gehen Sie durch die Schritte unter "Problem 1. Wie kann ich ein Upgrade von ASA/ASDM von der Quellversion X auf die Zielversion Y durchführen?" , um die Software zu aktualisieren.

Problem 5. "% FEHLER: Das ASDM-Paket ist nicht digital signiert. Konfiguration wird abgelehnt." fehl

"% FEHLER: Das ASDM-Paket ist nicht digital signiert. Konfiguration wird abgelehnt." Wenn ein neues ASDM-Image mit dem Befehl asdm image <image path> festgelegt wird, wird eine Fehlermeldung angezeigt.

Fehlerbehebung - empfohlene Maßnahmen

1. Die ASA validiert, ob es sich bei dem ASDM-Image um ein digital signiertes Cisco Image handelt. Wenn Sie versuchen, ein älteres ASDM-Image mit einer ASA-Version mit diesem Fix auszuführen, wird ASDM blockiert und die Meldung "%ERROR: Die Signatur für die Datei disk0:/<filename>" ist ungültig und wird in der ASA CLI angezeigt. ASDM Release 7.18(1.152) und höher sind abwärtskompatibel mit allen ASA-Versionen, auch ohne dieses Fix. Weitere Informationen finden Sie im Abschnitt Wichtige Hinweise in Release Notes for Cisco ASDM, 7.17(x).

2. Bei ASA-Geräten, die auf der sicheren Firewall 3100 ausgeführt werden, überprüfen Sie die Cisco Bug-ID CSCwc12322 "Digital signed ASDM image verify error on FPR3100 platform" (digital signierter ASDM-Image-Verifizierungsfehler auf FPR3100-Plattformen).

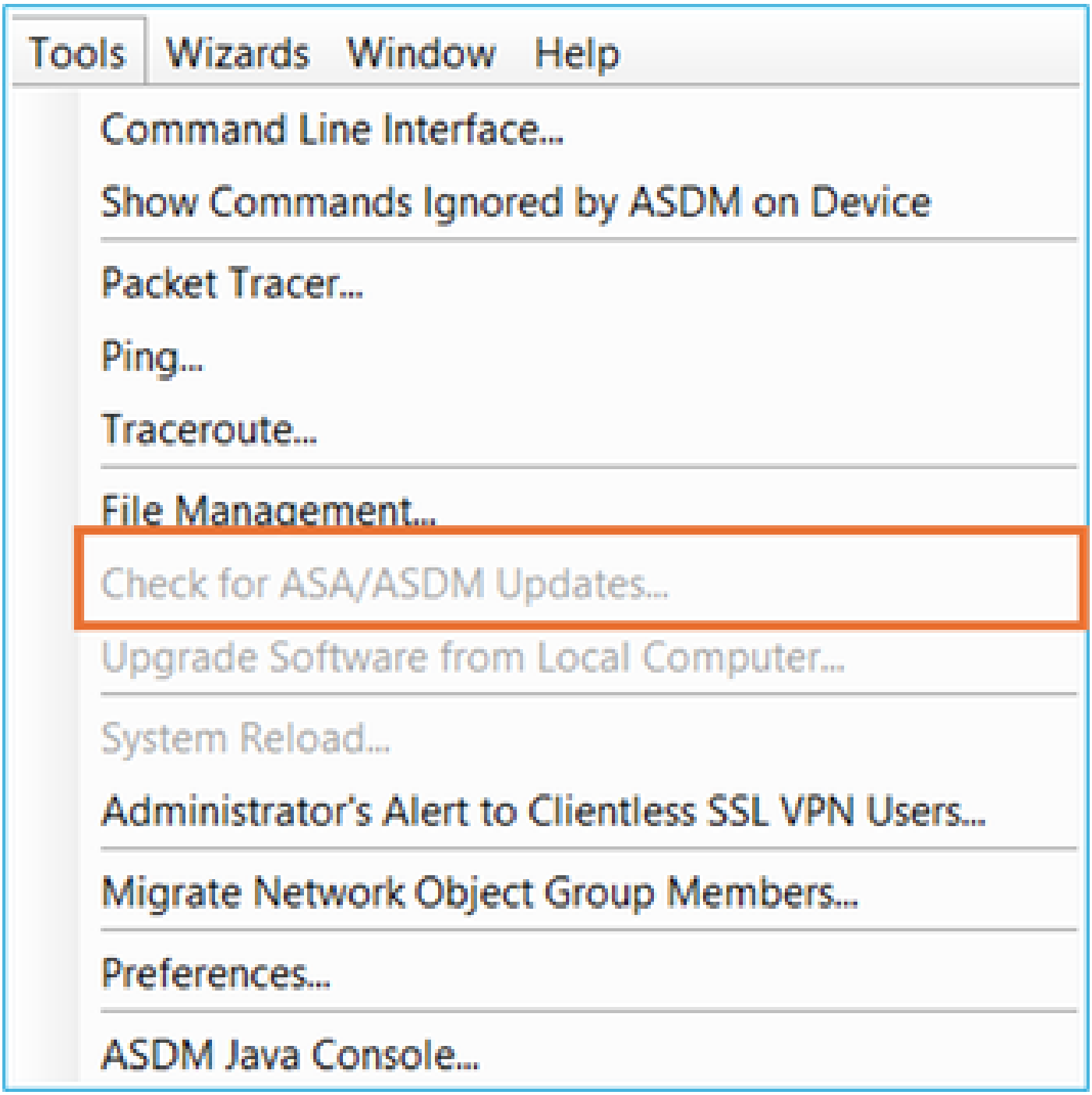
Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Referenzen

- Versionshinweise für Cisco ASDM, 7.17(x)

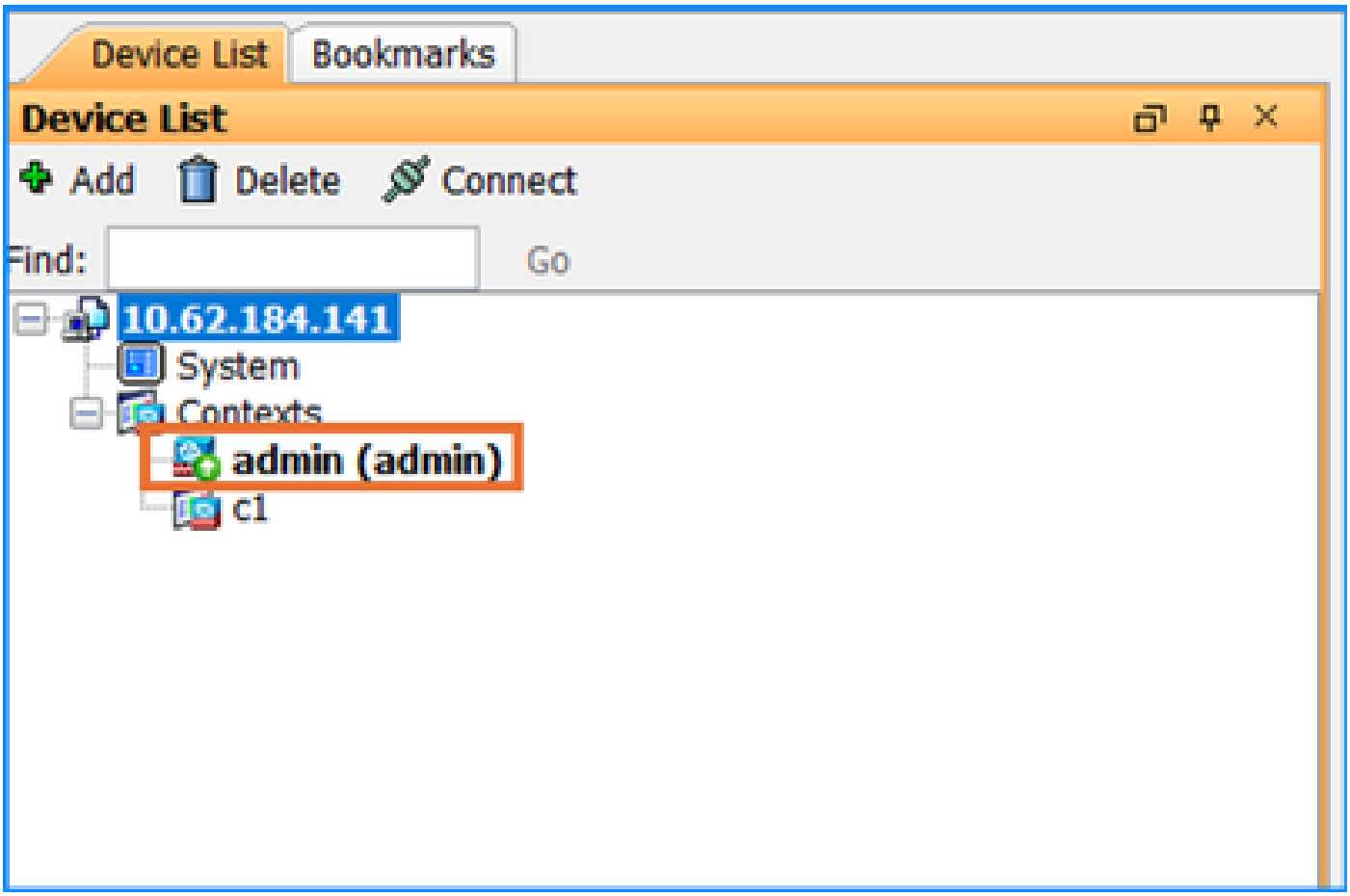
Problem 6. Im Multiple-Context-Modus kann nicht nach ASA/ASDM-Updates gesucht werden.

Die Option Tools > Check for ASA/ASDM Updates (Extras > Nach ASA/ASDM-Updates suchen) ist im Multiple-Context-Modus abgeblendet:

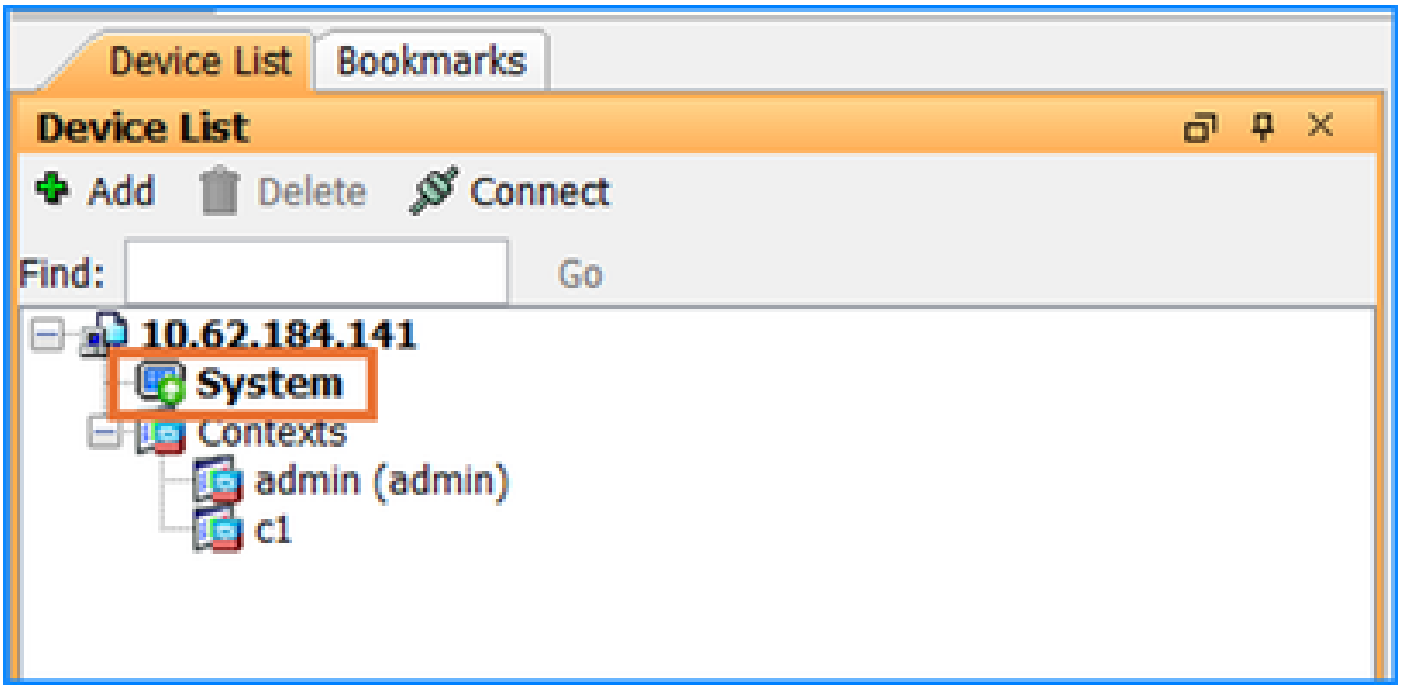


Fehlerbehebung - empfohlene Maßnahmen

Diese Option ist in der Regel abgeblendet, da der aktuelle Auswahlkontext auf der Registerkarte Geräteliste der Admin-Kontext ist:



Stellen Sie in diesem Fall sicher, dass Sie zum Systemkontext wechseln, indem Sie auf das Symbol System doppelklicken:



Problem 7. "Das Formular für die Allgemeinen Geschäftsbedingungen von Cisco

wurde nicht akzeptiert oder für den weiteren Download abgelehnt." fehl

Das Formular "Allgemeine Geschäftsbedingungen von Cisco wurden nicht akzeptiert oder abgelehnt, um den Download fortzusetzen." wird eine Fehlermeldung angezeigt, wenn der Benutzer versucht, die ASA/ASDM-Images über das Menü Tools > Check for ASA/ASDM Updates (Extras > Auf ASA/ASDM-Updates überprüfen) zu aktualisieren.

Fehlerbehebung - empfohlene Maßnahmen

Diese Fehlermeldung wird angezeigt, wenn die Endbenutzer-Lizenzvereinbarung (EULA) vom Benutzer nicht akzeptiert wird. Akzeptieren Sie die EULA, um fortzufahren.

Referenzen

- Endbenutzer-Lizenzvereinbarung (EULA)

Problem 8: Software für bestimmte Hardware kann nicht heruntergeladen werden

Auf der Seite für den Software-Download werden einige ASA-/ASDM-Softwareversionen für bestimmte Hardware nicht angezeigt.

Fehlerbehebung - empfohlene Maßnahmen

Die Verfügbarkeit von Software für bestimmte Hardware hängt hauptsächlich von der Kompatibilität und den End-of-Life (EoL) Meilensteinen ab. Bei Inkompatibilität, EoL-Produkten oder Zurückstellungen stehen die Softwareversionen in der Regel nicht zum Download zur Verfügung.

Überprüfen Sie anhand der folgenden Schritte die Kompatibilität und die unterstützten Versionen:

1. Prüfen Sie die Kompatibilität zwischen Software- und Hardwareversionen. Weitere Informationen finden Sie unter Cisco Secure Firewall ASA-Kompatibilität.
2. Prüfen Sie in den End-of-Life- und End-of-Sale-Hinweisen das Datum für die Einstellung der Softwarewartungsversionen und das Datum für die Einstellung des Supports.

- Enddatum der Softwarewartungsversionen - Das letzte Datum, an dem Cisco Engineering letzte Softwarewartungsversionen oder Bugfixes veröffentlichen kann. Nach diesem Datum entwickelt, repariert, wartet oder testet Cisco Engineering die Produktsoftware nicht mehr.
- Letztes Datum für den Support - Das letzte Datum, an dem der entsprechende Service und Support für das Produkt gemäß aktiver Serviceverträge oder den Garantiebedingungen verfügbar ist. Nach diesem Datum sind keine Support-Services mehr für das Produkt verfügbar, und das Produkt ist veraltet.

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. Informieren Sie sich in den Cisco Secure Firewall ASA Versionshinweisen und in den Cisco Secure Firewall ASDM Versionshinweisen über den Aufschub oder das Entfernen der Version.

Referenzen

- Cisco Secure Firewall ASA-Kompatibilität
- End-of-Life- und End-of-Sale-Hinweise

- Cisco Secure Firewall ASA - Versionshinweise
- Cisco Secure Firewall ASDM - Versionshinweise

Problem 9. Fehlermeldung "Fehler beim Ausführen des HTTP-Antwortcodes für die Dateiübertragung -1"

Die Fehlermeldung "Fehler beim Durchführen des HTTP-Antwortcodes für die Dateiübertragung -1" wird angezeigt, wenn der Benutzer eine Datei mithilfe der Option ASDM-Tools > Dateiverwaltung in die Firewall hochlädt.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCvf85831 "ASDM error PERR PERFORMANCE PERFORMANCE PERFORMANCE IN PERFORMANCE File Transfer HTTP Response code -1" during image upload".

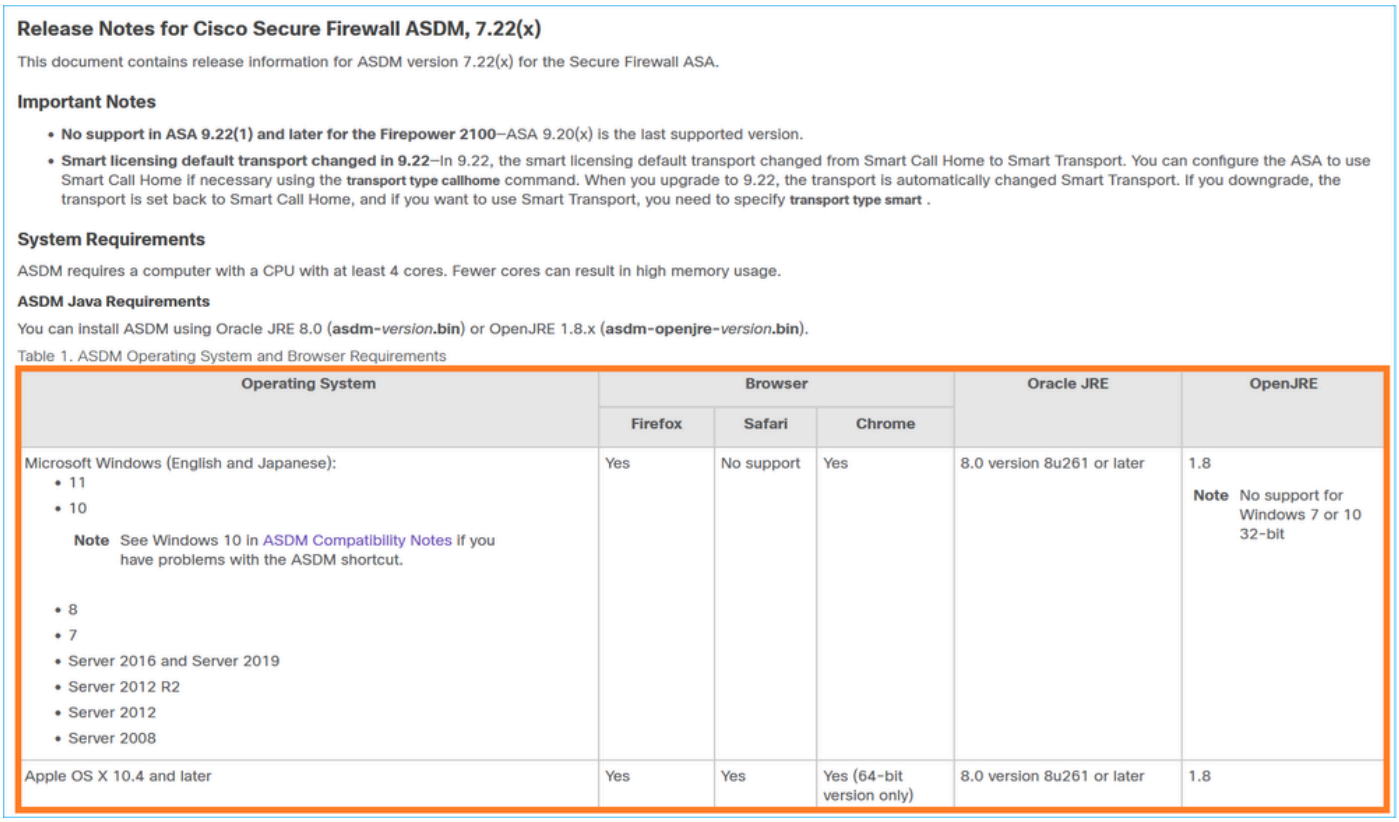
ASDM-Kompatibilitätsprobleme

In diesem Abschnitt werden die häufigsten Probleme im Zusammenhang mit der ASDM-Kompatibilität behandelt.

Im Allgemeinen muss ASDM mit den folgenden Komponenten kompatibel sein:

- ASA
- Java
- Betriebssystem (BS)
- Browser
- SFR-Modul (falls verwendet)

Daher wird dringend empfohlen, vor der Installation oder dem Upgrade von ASDM immer zuerst diese Tabelle zu überprüfen:



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

Anschließend werden die ASA- und ASDM-Kompatibilitätstabellen pro Modell angezeigt. Beispiel:

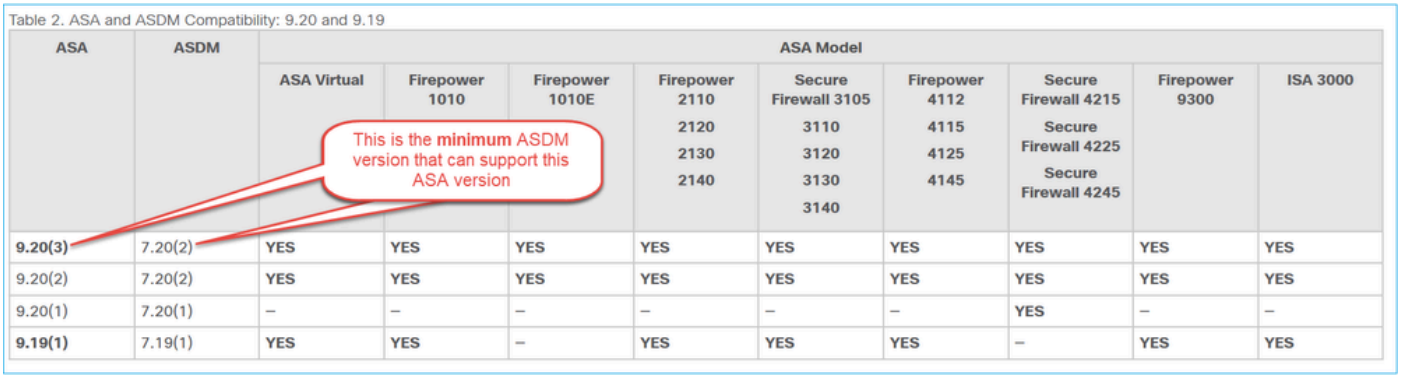


Table 2. ASA and ASDM Compatibility: 9.20 and 9.19

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

Hinweise:

Neue ASA-Versionen erfordern eine koordinierende ASDM-Version oder eine neuere Version. Sie können eine alte Version von ASDM nicht mit einer neuen ASA-Version verwenden.

Beispiel 1

Sie können ASDM 7.17 nicht mit ASA 9.18 verwenden. Für ASA-Interims können Sie die aktuelle ASDM-Version verwenden, sofern nicht anders angegeben. Beispielsweise können Sie ASA 9.22(1.2) mit ASDM 7.22(1) verwenden.

Beispiel 2

Sie verwenden ASAS 9.8(4)32. Sie können ASDM 7.19(1) für die Verwaltung verwenden, da ASDM abwärtskompatibel ist, sofern in den ASDM-Versionshinweisen nichts anderes angegeben ist.

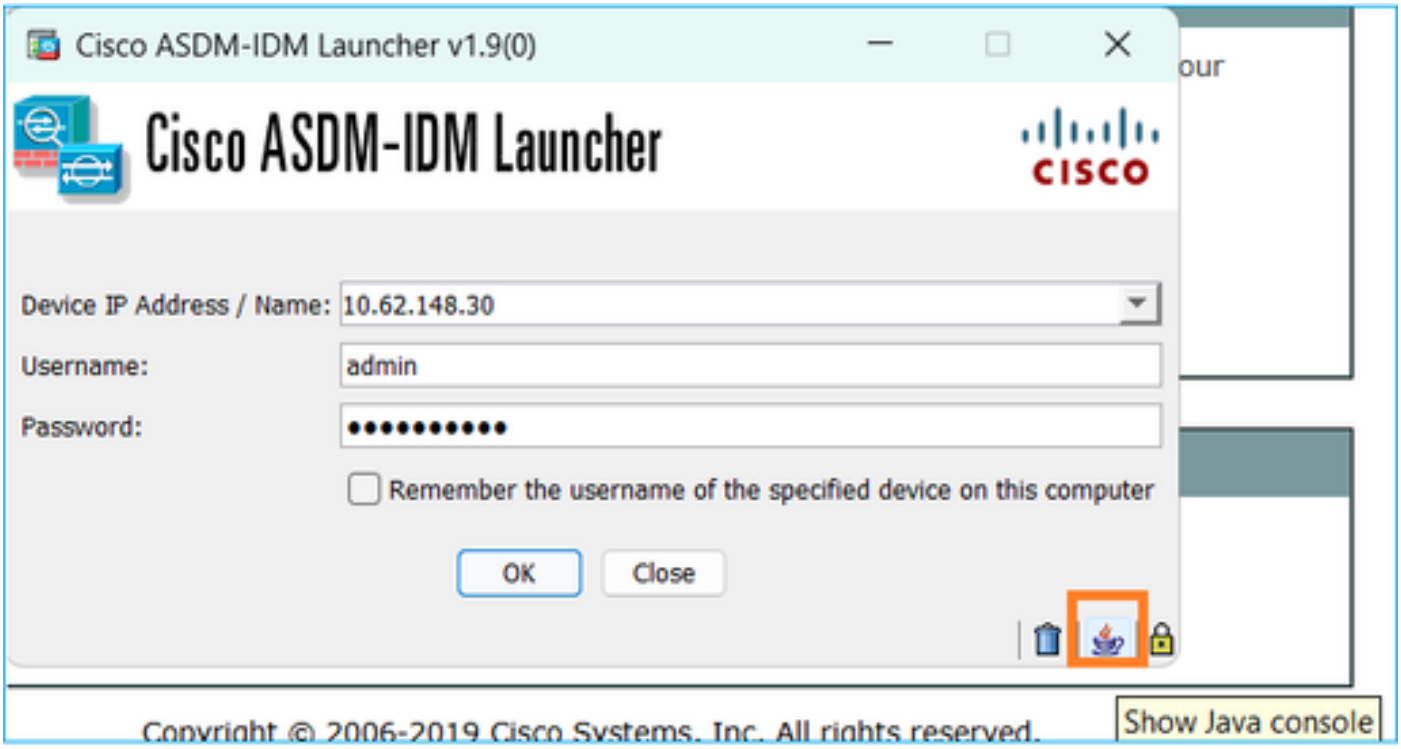
Referenzen

- 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: Inkompatible Java-Version

Fehlerbehebung - Empfohlene Schritte

Prüfen Sie die Java-Konsolenprotokolle:



Lesen Sie anschließend die Java- und ASA-Kompatibilitätsleitfäden:

- 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: Inkompatible ASA- und ASDM-Version

Bei inkompatiblen ASA- und ASDM-Versionen kann der Zugriff auf die ASDM-Benutzeroberfläche unterbrochen werden.

Fehlerbehebung - Empfohlene Schritte

Sie müssen die ASDM-Version über die CLI des Geräts installieren, das Image über TFTP in den Flash-Speicher der ASA kopieren und das ASDM-Image mithilfe des Befehls "asdm image" festlegen, wie im unten stehenden Handbuch beschrieben:

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

Beispiel

<#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. Support für ASDM und OpenJDK

Das Cisco ASDM-Image unterstützt offiziell kein OpenJDK. Es stehen daher zwei Optionen zur Verfügung:

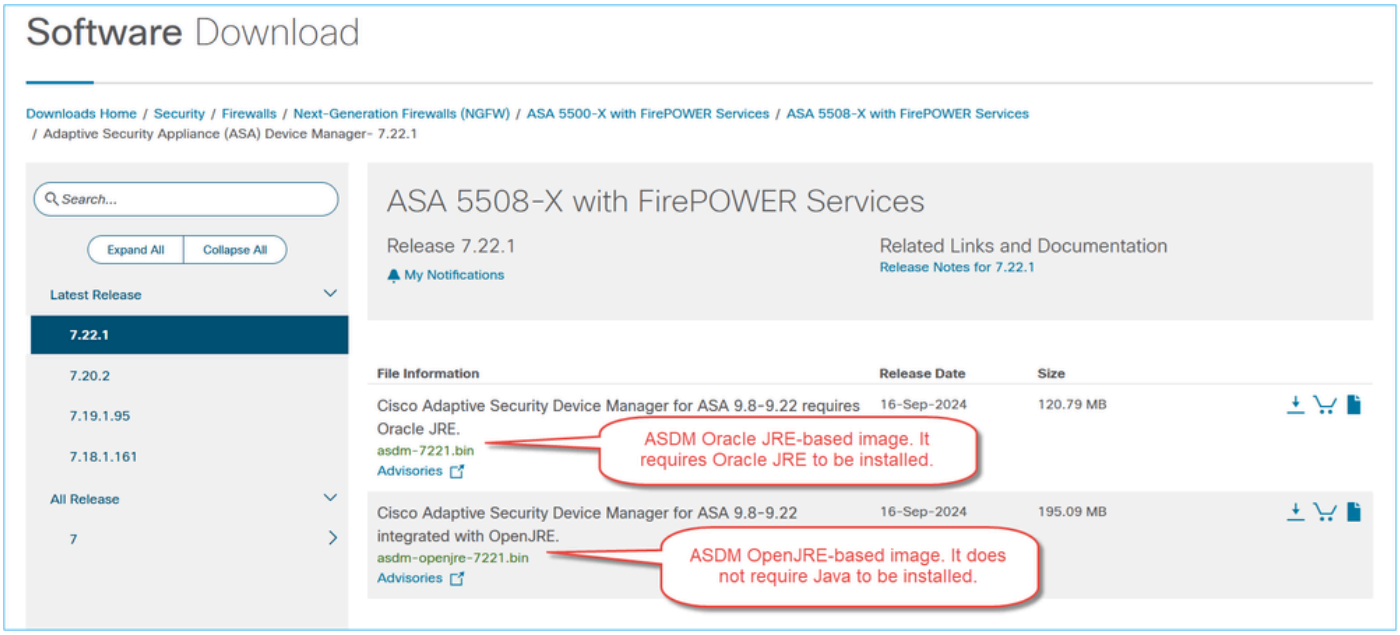
- Oracle JRE: Enthält die Java Web Start-Laufzeit zum Starten von ASDM auf dem Host-PC. Um diese Methode verwenden zu können, muss die 64-Bit-Version von Oracle JRE auf dem lokalen PC installiert sein. Sie können diese auf der offiziellen Website von Java

herunterladen.

- OpenJRE: Das offene JRE-Image ist mit dem Oracle-Image identisch, der Unterschied besteht jedoch darin, dass Sie das 64-Bit-Oracle JRE nicht auf dem lokalen PC installieren müssen, da das Image selbst über die Java Web Start-Funktion verfügt, um den ASDM zu starten. Aus diesem Grund ist die Größe des OpenJRE-Images größer als die von Oracle JRE. Beachten Sie, dass es erwartet wird, dass OpenJRE eine etwas ältere Java-Version verwendet, da sie mit der neuesten stabilen Version kompiliert werden, die zu Beginn des ASDM openJRE-Entwicklungszyklus verfügbar ist.

Oracle JRE und OpenJRE

	Oracle JRE	OpenJRE
Erfordert die Installation von Java auf dem Endhost	Ja	Nein (eigene Java-Lösung integriert)
Proprietär	Ja	Nein (Open Source)
Bildgröße	Mittel	Größer, da auch Java integriert ist
Bildname	asdm-xxxx.bin	asdm-openjre-xxxx.bin



Tipp: Wenn Sie die Version des ASDM-Launchers ändern möchten, deinstallieren Sie zuerst den vorhandenen ASDM-Launcher, und installieren Sie dann den neuen, indem Sie über HTTPS eine Verbindung mit der ASA herstellen.

Referenzen

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- OpenJDK: Vollständige Entwicklungs- und Laufzeitumgebung, Open-Source, GPL-Lizenz.
- Oracle JRE: Nur die Laufzeitumgebung, eine proprietäre Lizenz, erfordert eine kommerzielle Lizenz für den Produktionsgebrauch.
- OpenJRE: Nur Laufzeitumgebung, Open-Source, GPL-Lizenz.
- https://www.oracle.com/java/technologies/javase/jre8-readme.html

Problem 4: Kompatibilität von ASDM und Java Azul Zulu

Oracle JRE-basierte ASDM-Images unterstützen Java Azul Zulu nicht. Auf der anderen Seite, ASDM OpenJRE-basierte Bilder kommen Azul Zulu Integration. Überprüfen Sie die Empfehlungen für "Problem 3" hinsichtlich der verfügbaren Optionen.

Problem 5. WARNUNG: Die Signatur wurde in der Datei disk0:/asdm-xxx.bin nicht gefunden

Beispiel:

<#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.
```

Fehlerbehebung - Empfohlene Schritte

In der Regel handelt es sich hierbei um ein ASA- oder ASDM-Kompatibilitätsproblem. Lesen Sie den ASDM-Kompatibilitätsleitfaden, und stellen Sie sicher, dass Ihr ASDM mit dem ASA-Image kompatibel ist. Die ASA- und ASDM-Kompatibilitätsmatrix finden Sie unter:

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

Problem 6. "% FEHLER: Das ASDM-Paket ist nicht digital signiert. Konfiguration wird abgelehnt."

Diese Fehlermeldung kann angezeigt werden, wenn ein neues ASDM-Image mithilfe des asdm image <Bildpfad> aus.

Fehlerbehebung - empfohlene Maßnahmen

1. Die ASA validiert, ob es sich bei dem ASDM-Image um ein digital signiertes Cisco Image handelt. Wenn Sie versuchen, ein älteres ASDM-Image mit einer ASA-Version mit diesem Fix auszuführen, wird ASDM blockiert und die Meldung "%ERROR: Die Signatur für die Datei disk0:/<filename>" ist ungültig und wird in der ASA CLI angezeigt. ASDM Release 7.18(1.152) und höher sind abwärtskompatibel mit allen ASA-Versionen, auch ohne dieses Fix. Weitere Informationen finden Sie im Abschnitt Wichtige Hinweise in Versionshinweise für Cisco ASDM, 7.17(x).

2. Aktualisieren Sie die Java-Version auf Ihrem Host-PC.

3. Wenn die ASA auf der sicheren Firewall 3100 ausgeführt wird, überprüfen Sie die Software-Bug-ID von Cisco. CSCwc12322 "Digital signierter ASDM Image Verification Error on FPR3100 platform"

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

Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 7. "%FEHLER: Signatur ungültig für Datei disk0:/<Dateiname>"

Der Fehler wird beim Kopieren der Datei angezeigt. Beispiel:

<#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.
```

Fehlerbehebung - empfohlene Maßnahmen

ASA 9.14(4.14) und neuere Versionen erfordern ASDM 7.18(1.152) oder neuere Versionen. Die ASA validiert nun, ob es sich bei dem ASDM-Image um ein digital signiertes Cisco Image handelt. Wenn Sie versuchen, ein älteres ASDM-Image als 7.18(1.152) mit einer ASA-Version mit diesem Fix auszuführen, wird ASDM blockiert und die Meldung "%ERROR: Die Signatur für die Datei disk0:/<filename>" ist ungültig und wird in der ASA CLI angezeigt.

Diese Änderung wurde aufgrund von Cisco ASDM und ASA Software Client-side Arbitrary Code Execution Vulnerability (CVE ID CVE-2022-20829) eingeführt.

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

Falls das Gerät im Plattformmodus betrieben wird, gehen Sie durch die Anweisungen in diesem Dokument, um das Bild hochzuladen: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_zp4_dzj_cjb

Referenzen

- ASDM-Versionshinweise: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3
- ASA-Upgrade-Leitfaden: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task_E9EE51964590499999B1D976F66E2771

Problem 8: Kompatibilität mit sicherem Firewall-Status (Hostscan)

Die Hostscan-Version hängt mehr von der AnyConnect-Version ab als von der ASA-Version. Beide Versionen finden Sie hier: Software-Download - Cisco Systems:

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

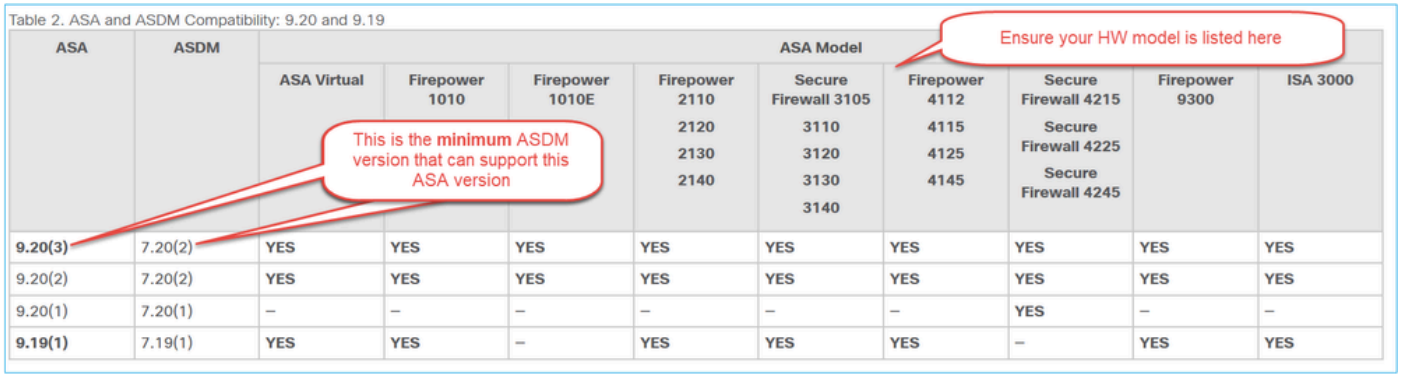
Problem 9. Zuletzt unterstützte Version

Fehlerbehebung - empfohlene Maßnahmen

Wenn Sie die neueste unterstützte ASDM-Version für Ihre Firewall kennen möchten, müssen Sie vor allem zwei Dokumente überprüfen:

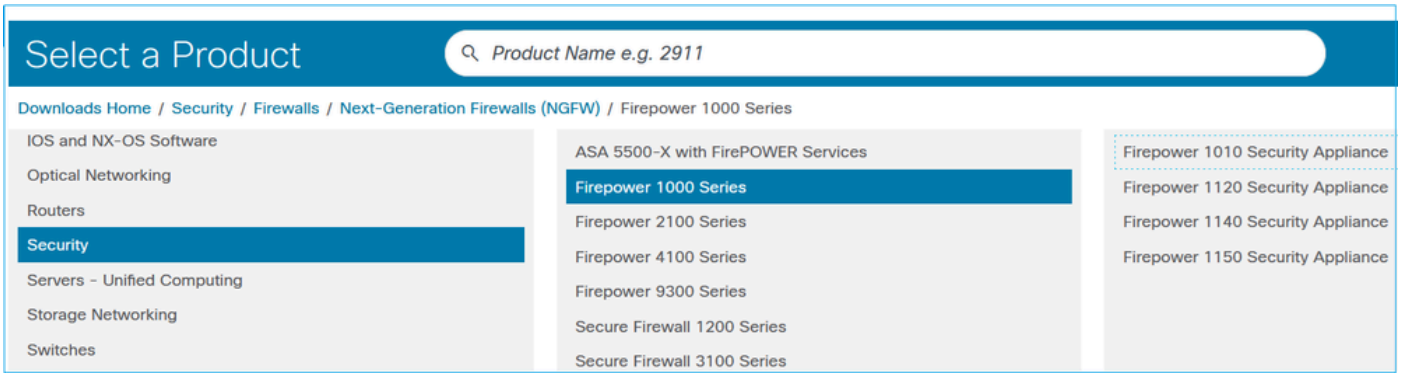
- ASDM-Versionshinweise: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3

Insbesondere die ASA-Modelltabelle

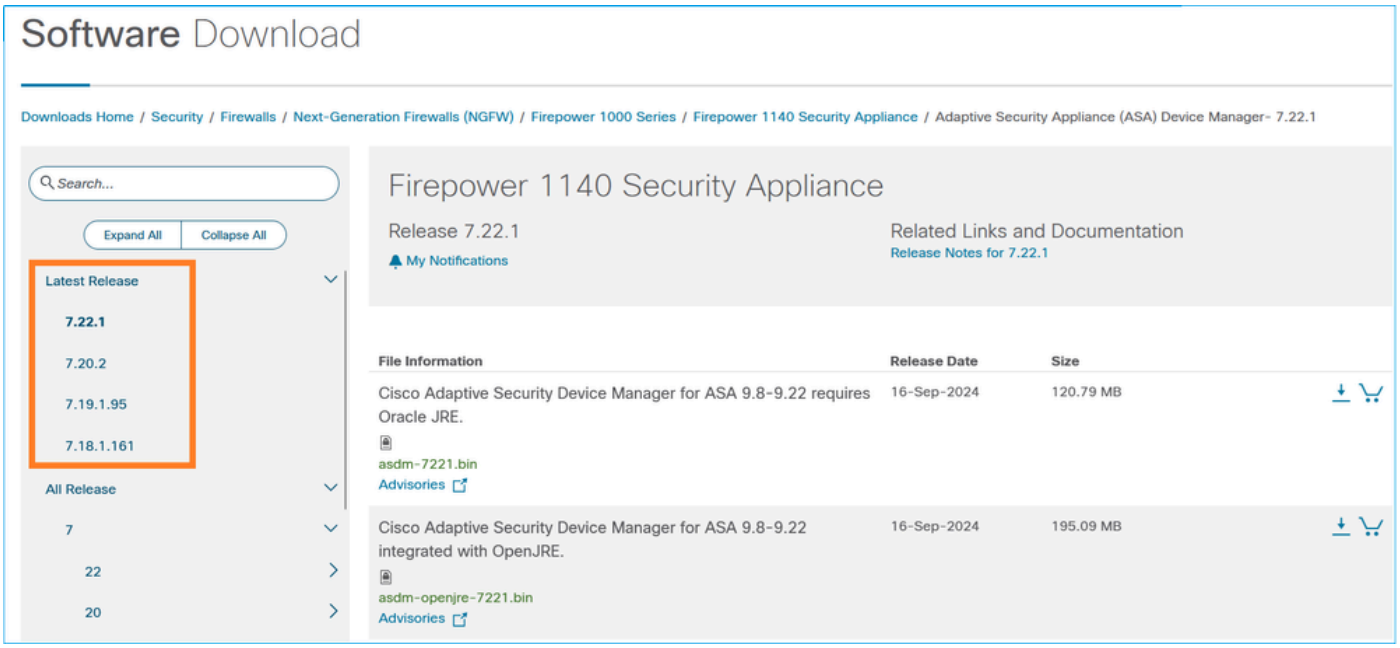


Das zweite Dokument ist die Software-Download-Seite:

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



Aktuelle ASDM-Versionen pro SW-Zug, die von Ihrer HW unterstützt werden, finden Sie z. B.:

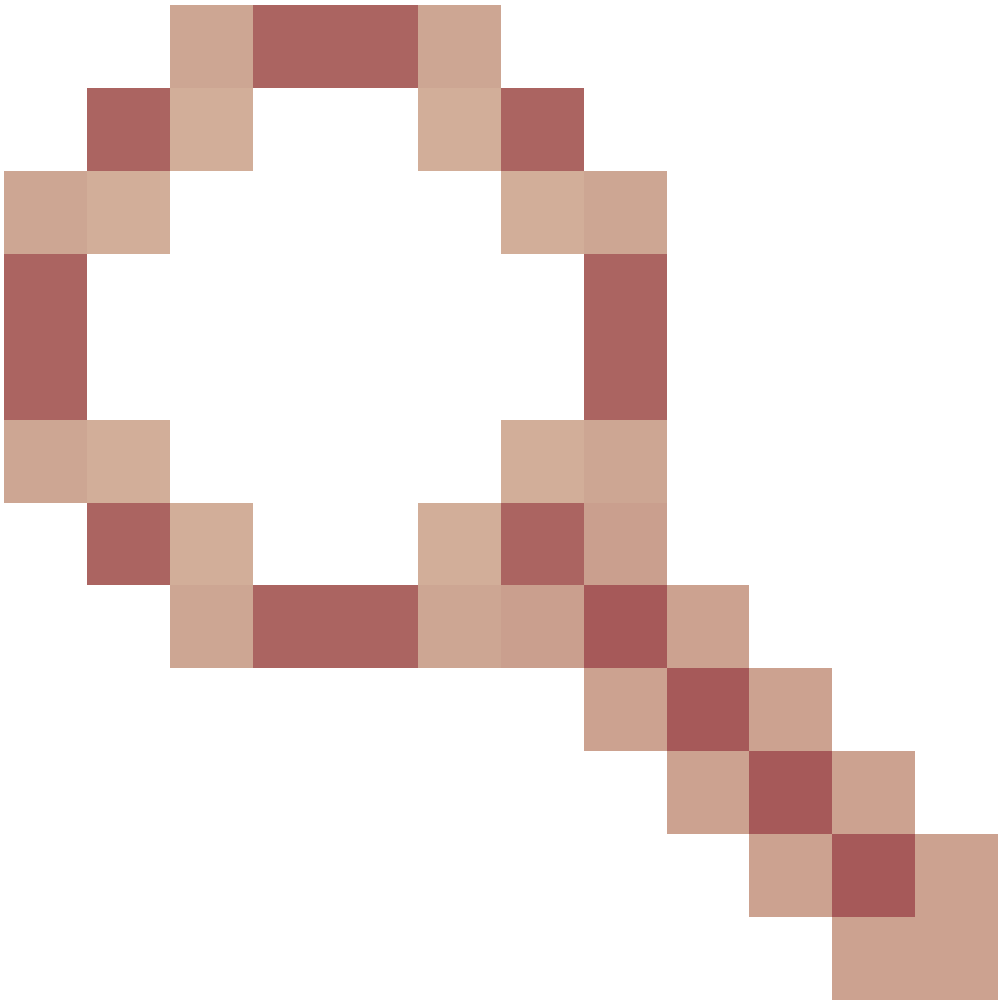


Problem 10. ASDM-Unterstützung unter Linux

Fehlerbehebung - empfohlene Maßnahmen

Linux wird nicht offiziell unterstützt.

Weiterführende Verbesserung:



Cisco Bug-ID CSCwk67345
ENH: Linux in die Liste der unterstützten Betriebssysteme aufnehmen

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

Problem 11. ASDM - Ende des Supports

Fehlerbehebung - empfohlene Maßnahmen

Beachten Sie die End-of-Life- und End-of-Sale-Hinweise zu ASA/ASDM:

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

Probleme mit ASDM-Lizenzen

In diesem Abschnitt werden die häufigsten Probleme im Zusammenhang mit ASDM-Lizenzen behandelt.

Das Smart Licensing-Modell wird verwendet von:

- Chassis-Registrierung für Firepower 4100/9300: Lizenzmanagement für die ASA
- ASAv, Firepower 1000, Firepower 2100, Firepower 9300 und Firepower 4100: Lizenzen: Smart Software-Lizenzierung (ASAv, ASA mit Firepower)

Alle anderen Modelle verwenden den Produktaktivierungsschlüssel (PAK).

Referenzen

- Funktionslizenzen für die Cisco Secure Firewall der ASA-Serie - Modellrichtlinien

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

Problem 1. 3DES/AES Smart License fehlt

ASDM erfordert eine Strong Encryption-Lizenz (3DES/AES) auf ASA, es sei denn, Sie greifen über die Management-Schnittstelle darauf zu. Um den ASDM-Zugriff über eine Datenschnittstelle zu ermöglichen, benötigen Sie die 3DES/AES-Lizenz.

So fordern Sie eine 3DES/AES-Lizenz von Cisco an:

1. Besuchen Sie https://www.cisco.com/go/license
2. Klicken Sie auf Continue to Product License Registration (Produktlizenzregistrierung).
3. Klicken Sie im Lizenzierungsportal neben dem Textfeld auf Weitere Lizenzen abrufen.
4. Wählen Sie IPS, Crypto, Other... aus der Dropdown-Liste aus.
5. Geben Sie ASA in das Feld Search by Keyword (Nach Stichwort suchen) ein.
6. Wählen Sie in der Produktliste Cisco ASA 3DES/AES License aus, und klicken Sie auf Next (Weiter).
7. Geben Sie die Seriennummer der ASA ein, und gehen Sie durch die Eingabeaufforderungen, um eine 3DES/AES-Lizenz für die ASA anzufordern.

Fehlerbehebung - empfohlene Maßnahmen

Um die Lizenz zu aktivieren und sich beim Cisco Smart Licensing-Portal zu registrieren, stellen Sie sicher, dass die folgenden Komponenten installiert sind:

- Die ASA-Uhr zeigt die richtige Zeit an. Es wird empfohlen, einen NTP-Server zu verwenden.
- Weiterleitung an das Cisco Smart Licensing-Portal
- HTTPS-Datenverkehr wird nicht von der Firewall zum Lizenzportal blockiert. Eine Erfassung auf der Firewall kann dies bestätigen.
- Wenn ein HTTP-Proxy-Server verwendet werden soll, geben Sie den entsprechenden Befehl ein. Beispiel:

<#root>

```
ciscoasa(config)#
```

call-home

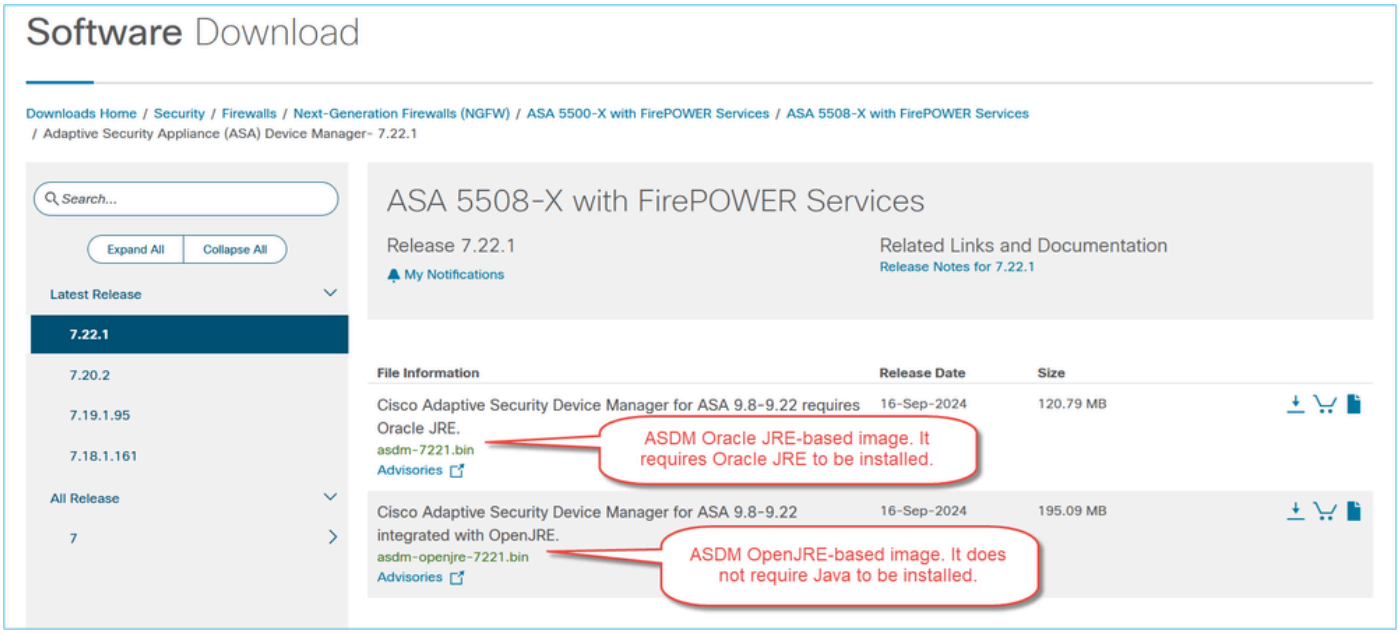
```
ciscoasa(cfg-call-home)#
http-proxy 10.1.1.1 port 443
```

Problem 2: Oracle Java JRE-Lizenzanforderungen

Fehlerbehebung - empfohlene Maßnahmen

ASDM .bin-Bilddatei gibt es in zwei Varianten:

- Oracle JRE: Enthält die Java Web Start-Laufzeit zum Starten von ASDM auf dem Host-PC. Um diese Methode verwenden zu können, muss die 64-Bit-Version von Oracle JRE auf dem lokalen PC installiert sein. Sie können diese auf der offiziellen Website von Java herunterladen.
- OpenJRE: Das offene JRE-Image ist mit dem Oracle-Image identisch, der Unterschied besteht jedoch darin, dass Sie das 64-Bit-Oracle JRE nicht auf dem lokalen PC installieren müssen, da das Image selbst über die Java Web Start-Funktion verfügt, um den ASDM zu starten.



Falls Sie sich für die Verwendung des Oracle-basierten ASDM-Images entscheiden, benötigen Sie eine Java-Lizenz, wenn Sie es für nicht-persönliche Zwecke verwenden. Oracle Java SE Licensing - Häufig gestellte Fragen:

Zur privaten Verwendung wird Java auf einem Desktop- oder Laptop-Computer verwendet, um z. B. Spiele zu spielen oder andere persönliche Anwendungen auszuführen. Wenn Sie Java auf einem Desktop- oder Laptop-Computer als Teil eines Geschäftsbetriebs verwenden, ist dies kein persönlicher Gebrauch. Zum Beispiel könnten Sie eine Java-Produktivitätsanwendung verwenden, um Ihre eigenen Hausaufgaben oder Ihre persönlichen Steuern zu erledigen, aber Sie könnten sie nicht verwenden, um Ihre Buchhaltung zu erledigen.

Wenn Sie keine Java-Lizenzen anwenden möchten, können Sie das OpenJRE-basierte ASDM-Image verwenden.

Referenzen

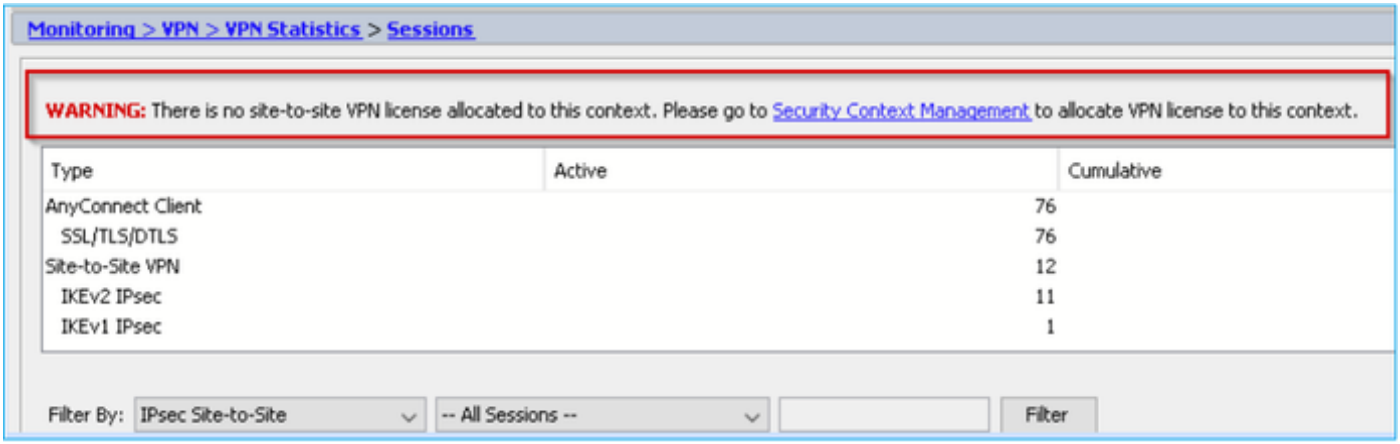
- https://www.oracle.com/java/technologies/javase/jdk-faqs.html
- ASDM Java-Anforderungen für ASDM 7.22: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- ASDM-Kompatibilitätshinweise für ASDM 7.2: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476

Anmerkung: Überprüfen Sie die Versionshinweise für die verwendete ASDM-Version.

Problem 3. ASDM-Warnung über Site-to-Site-VPN-Lizenz im Multi-Context-Modus

Der ASDM zeigt Folgendes an:

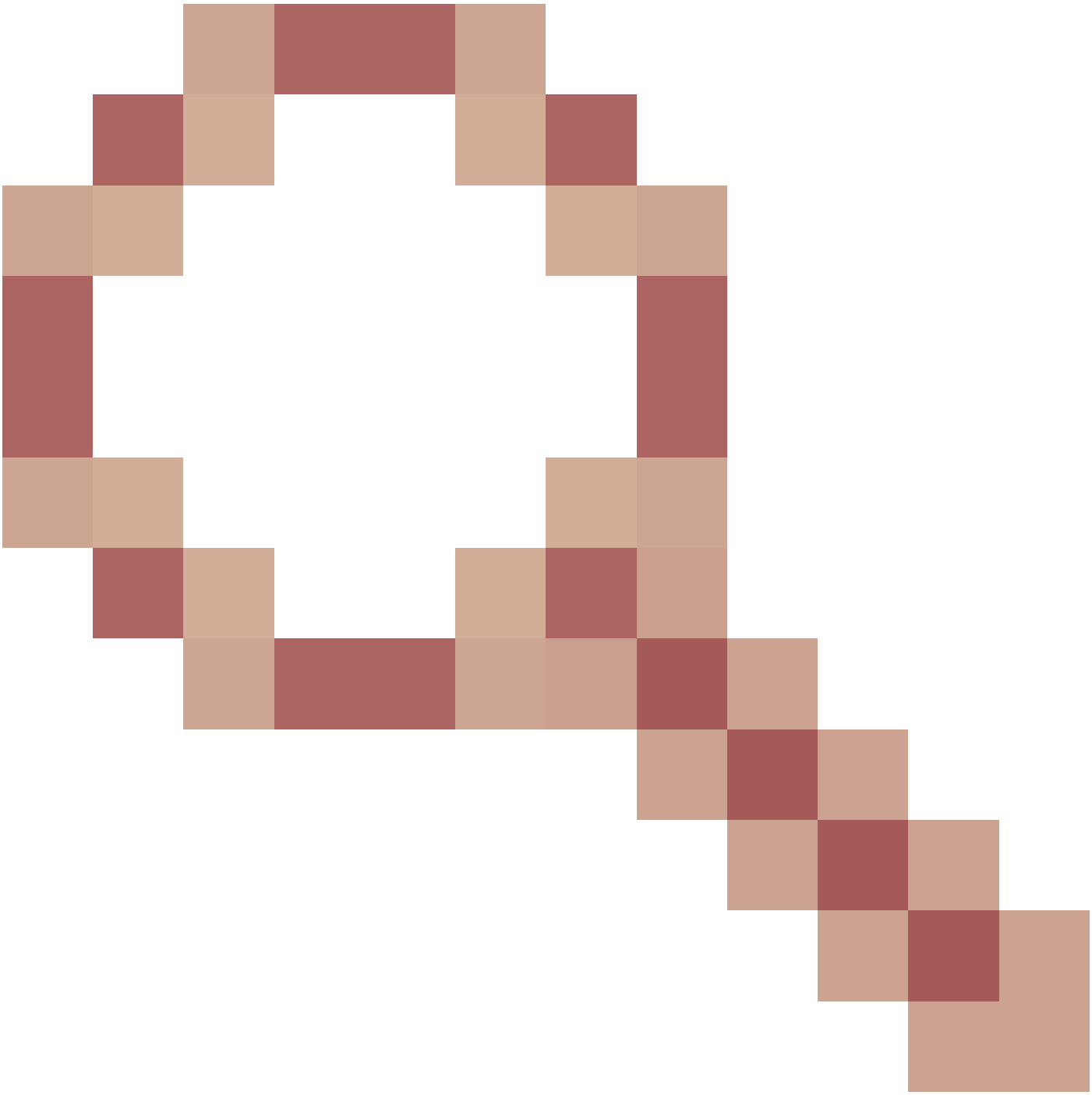
Warnung: Diesem Kontext ist keine Site-to-Site-VPN-Lizenz zugeordnet. Gehen Sie zu Security Context Management, um diesem Kontext eine VPN-Lizenz zuzuweisen.



Fehlerbehebung - empfohlene Maßnahmen

Dies ist ein Fehler in der kosmetischen Software, der verfolgt wird von:

Cisco Bug-ID CSCvj66962



ASDM 7.9(2) ASA 9.6(4)8, persistenter L2L-Multi-Context-Fehler

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

Sie können den Fehler abonnieren, sodass Sie eine Benachrichtigung über Defekt-Updates erhalten.

Referenzen

- ASDM-Konfigurationsanleitungen
- Kompatibilität von Cisco ASA und ASDM pro Modell

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.