Risoluzione dei problemi relativi alle licenze ASDM, agli aggiornamenti e alla compatibilità

Sommario

Introduzione

In questo documento viene descritto il processo di risoluzione dei problemi relativi alla licenza ASDM, all'aggiornamento e alla compatibilità.

Introduzione

Il documento fa parte della serie ASDM (Adaptive Security Appliance Device Manager) per la risoluzione dei problemi, insieme ai seguenti documenti:

- Risoluzione dei problemi di avvio di ASDM
- Risoluzione dei problemi di configurazione, autenticazione e altri problemi di ASDM
- Risoluzione dei problemi di sicurezza, certificati e vulnerabilità di ASDM TLS

Problemi di aggiornamento ASDM

Problema 1. Come aggiornare l'aggiornamento di ASA/ASDM dalla versione X di origine alla versione Y di destinazione?

L'utente ha bisogno di assistenza per un aggiornamento di ASA/ASDM dalla versione di origine X alla versione di destinazione Y.

Risoluzione dei problemi - Azioni consigliate

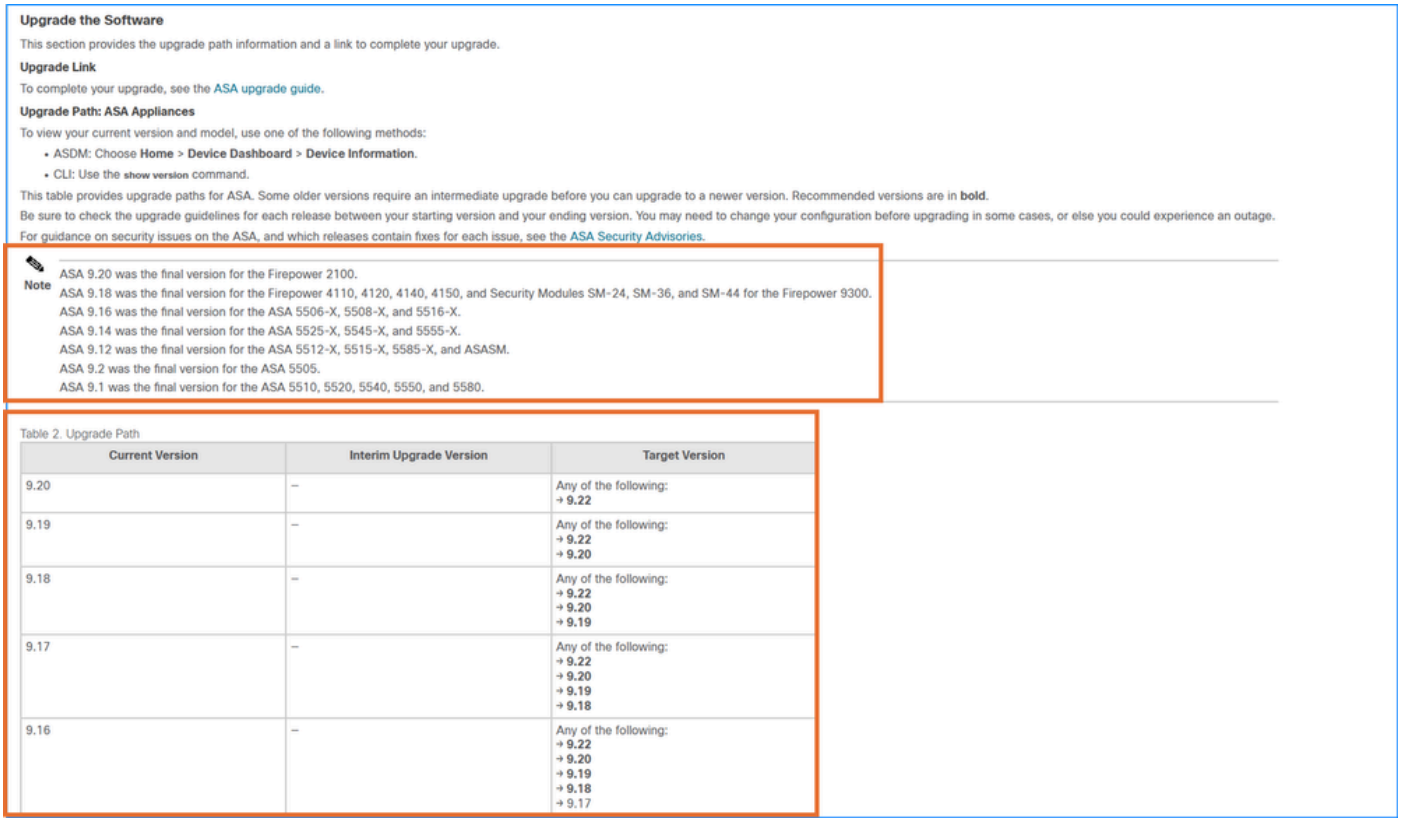
1. Verificare che le versioni ASA, ASDM, del sistema operativo e Java siano compatibili con la versione di destinazione. Per ulteriori informazioni, fare riferimento al Note sulla release di Cisco Secure Firewall ASA, Note sulla release di Cisco Secure Firewall ASDM, Compatibilità ASA Cisco Secure Firewall.

Le versioni ASA, ASDM, del sistema operativo e Java devono essere compatibili e le versioni di destinazione devono essere supportate su hardware specifico.
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

2. Per le appliance ASA in esecuzione su Firepower 4100/9300, verificare che le versioni del sistema operativo Firepower eXtensible Operating System (FXOS) e del software ASA siano compatibili. Fare riferimento alla sezione sulla compatibilità FXOS tra Cisco Firepower 4100/9300.

3. Assicurarsi di familiarizzare con le modifiche apportate alla versione target controllando il Note sulla release di Cisco Secure Firewall ASA, Note sulla release di Cisco Secure Firewall ASDM. Nel caso di Firepower 4100/9300, familiarizzare con le modifiche in FXOS controllando Note sulla release di FXOS.

4. Verificare il percorso di aggiornamento nelle note sulla versione. In questo esempio, la tabella 2 delle note sulla versione per la versione 7.22 contiene il percorso di aggiornamento dalle versioni precedenti alla versione di destinazione:



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.

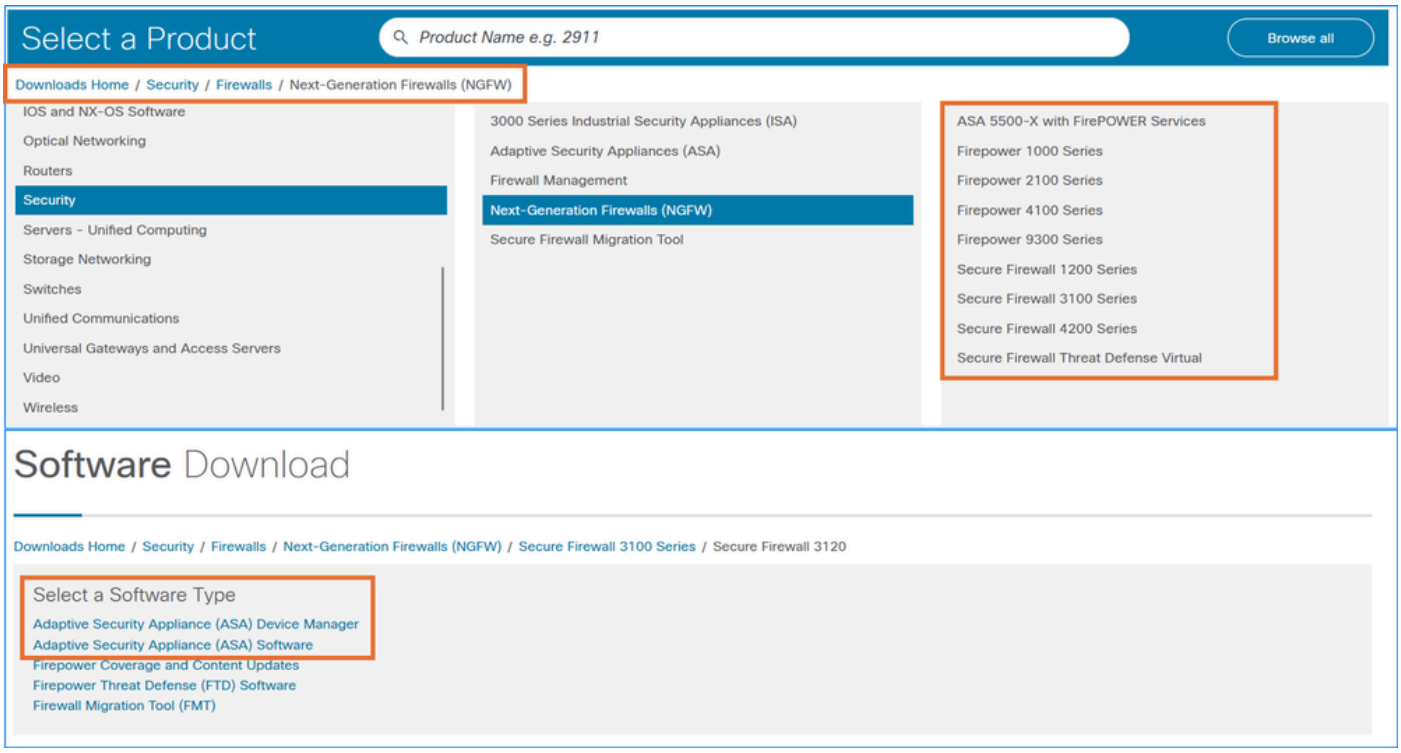
Note

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. Una volta soddisfatti i requisiti di compatibilità, scaricare le versioni ASA/ASDM e FXOS di destinazione (solo Firepower 4100/9300) dalla pagina di download del software. Selezionare i modelli hardware specifici, come illustrato nell'esempio. Le uscite suggerite sono contraddistinte da una stella d'oro:



6. Assicurarsi di passare attraverso il capitolo: Pianificazione dell'aggiornamento e capitolo: Aggiornare l'ASA nella guida all'aggiornamento dell'ASA di Cisco Secure Firewall.

Riferimenti

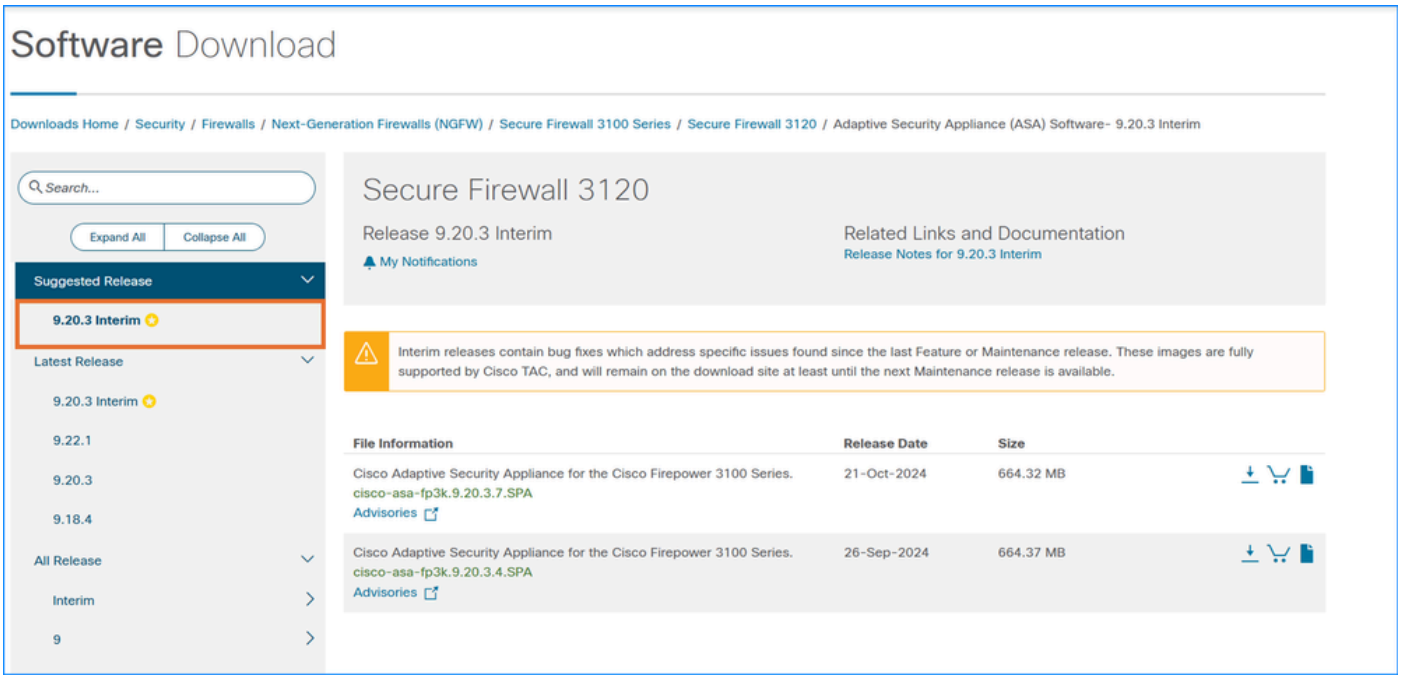
- Note sulla release di Cisco Secure Firewall ASA
- Note sulla release di Cisco Secure Firewall ASDM
- Compatibilità ASA Cisco Secure Firewall
- Cisco Firepower 4100/9300 FXOS Compatibilità
- Guida all'aggiornamento di Cisco Secure Firewall ASA

Problema 2. Quali sono le versioni consigliate per ASA/ASDM?

L'utente chiede informazioni sulle versioni consigliate per ASA/ASDM.

Risoluzione dei problemi - Azioni consigliate

Cisco TAC non fornisce raccomandazioni sulle versioni software. Gli utenti possono scaricare la release suggerita da Cisco in base alla qualità del software, alla stabilità e alla longevità. Le versioni suggerite sono contrassegnate da una stella dorata come mostrato di seguito:

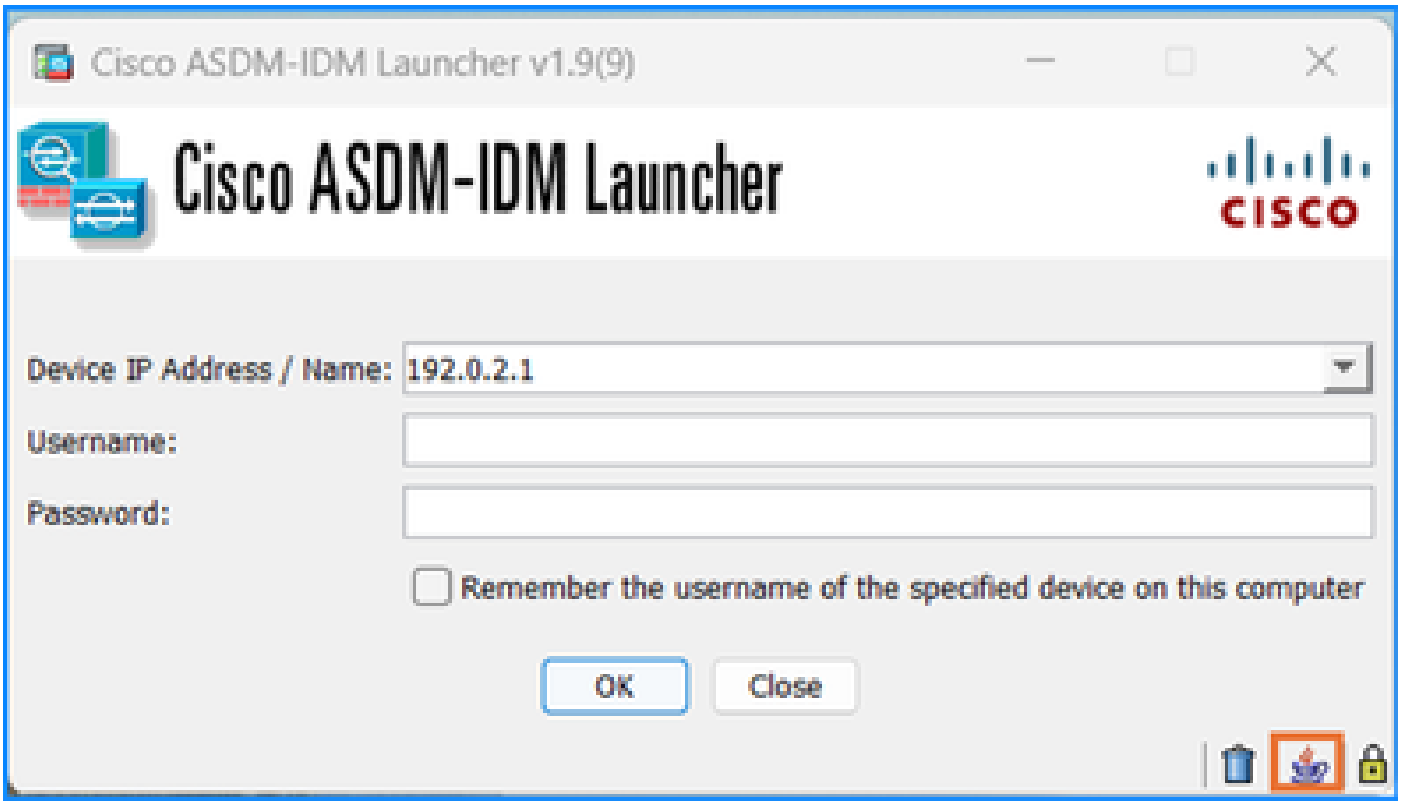


Problema 3. Controllo degli aggiornamenti ASA/ASDM non riuscito in ASDM tramite Strumenti > Controlla aggiornamenti ASA/ASDM

Il controllo degli aggiornamenti ASA/ASDM in ASDM tramite Tools > Check for ASA/ASDM Updates non riesce. In particolare, si osservano i seguenti sintomi:

1. Dopo aver fatto clic sul pulsante Login, la finestra Inserisci password di rete viene nuovamente visualizzata anche se sono state fornite le credenziali corrette.

2. Nei log della console Java viene visualizzato l'errore "Richiesta metadati non riuscita":



<#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.
```

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCvf91260 "ASDM: L'aggiornamento da CCO non funziona a causa di campi non ignorabili. "Richiesta metadati non riuscita". Per ovviare al problema, scaricare le immagini direttamente dalla pagina di download e caricarle nel firewall.

Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 4. Quali versioni contengono correzioni per vulnerabilità specifiche?

L'utente chiede informazioni sulle versioni corrette di vulnerabilità specifiche.

Risoluzione dei problemi - Azioni consigliate

1. Assicurarsi di controllare l'advisory per i prodotti interessati.
2. Nell'advisory della sicurezza, fornire la versione hardware e software esistente al controllo software e fare clic su 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.

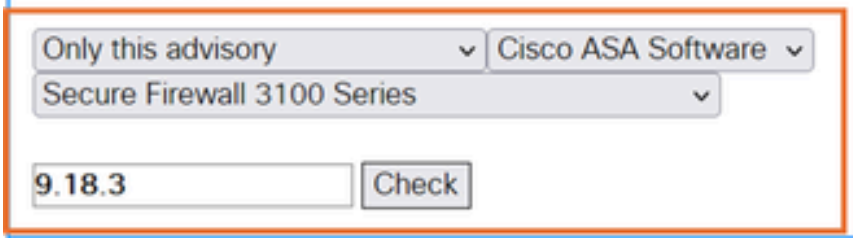
In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical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

Cisco ASA, FMC, and FTD Software

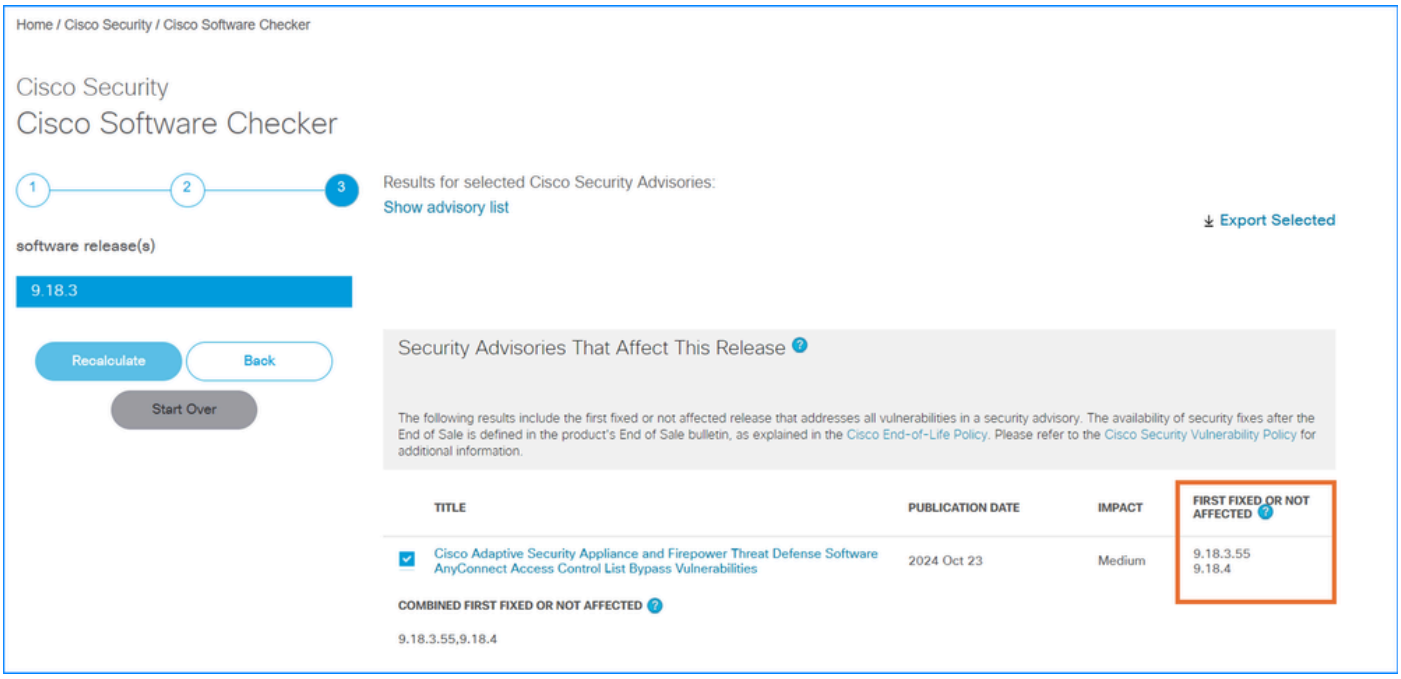
To help customers determine their exposure to vulnerabilities in Cisco ASA, FMC, and FTD Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described 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**.



3. Se la versione fissa è disponibile, annotare le versioni nella colonna PRIMO FISSO O NON INTERESSATO:



4. Eseguire i passaggi descritti in "Problema 1. Come aggiornare ASA/ASDM dalla versione X di origine alla versione Y di destinazione?" per aggiornare il software.

Problema 5. "% ERRORE: Il pacchetto ASDM non è firmato digitalmente. Rifiuto della configurazione in corso." Messaggio di errore

L'ERRORE "%: Il pacchetto ASDM non è firmato digitalmente. Rifiuto della configurazione in corso." Quando si imposta una nuova immagine ASDM con il comando asdm image <image path> (percorso immagine ASDM).

Risoluzione dei problemi - Azioni consigliate

1. L'ASA convalida se l'immagine ASDM è un'immagine Cisco con firma digitale. Se si tenta di eseguire un'immagine ASDM precedente con una versione ASA con questa correzione, ASDM viene bloccato e viene visualizzato il messaggio "%ERRORE: La firma non valida per il file disk0:/<filename>" viene visualizzata nella CLI dell'ASA. ASDM release 7.18(1.152) e successive sono compatibili con tutte le versioni precedenti delle appliance ASA, anche quelle senza questa correzione. Fare riferimento alla sezione Note importanti nelle note di rilascio per Cisco ASDM, 7.17(x).

2. Per l'appliance ASA su Secure Firewall 3100, controllare l'ID bug Cisco CSCwc12322 del software "Digital signed ASDM image verify error on FPR3100 platform".

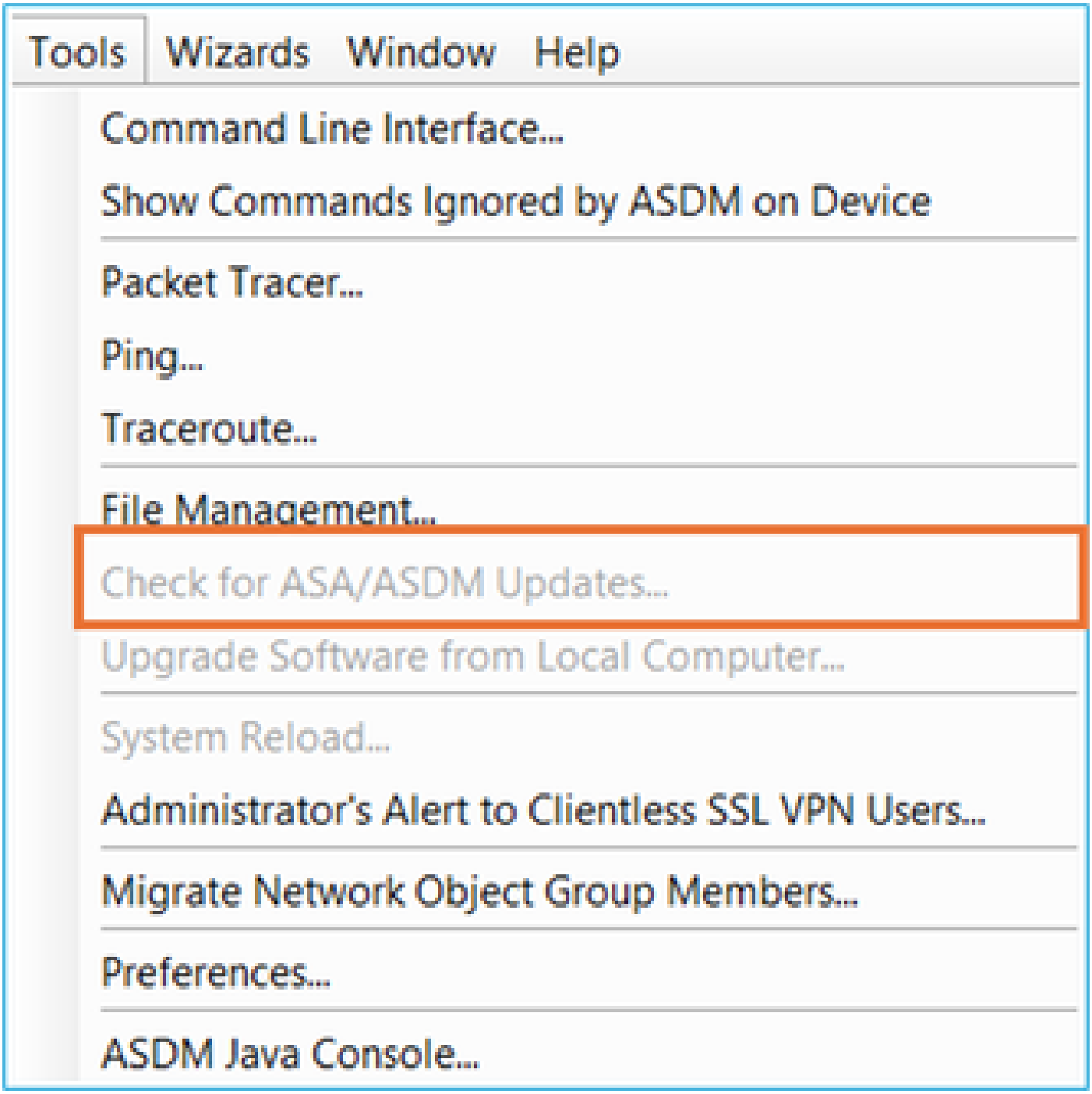
Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Riferimenti

- Note sulla release per Cisco ASDM, 7.17(x)

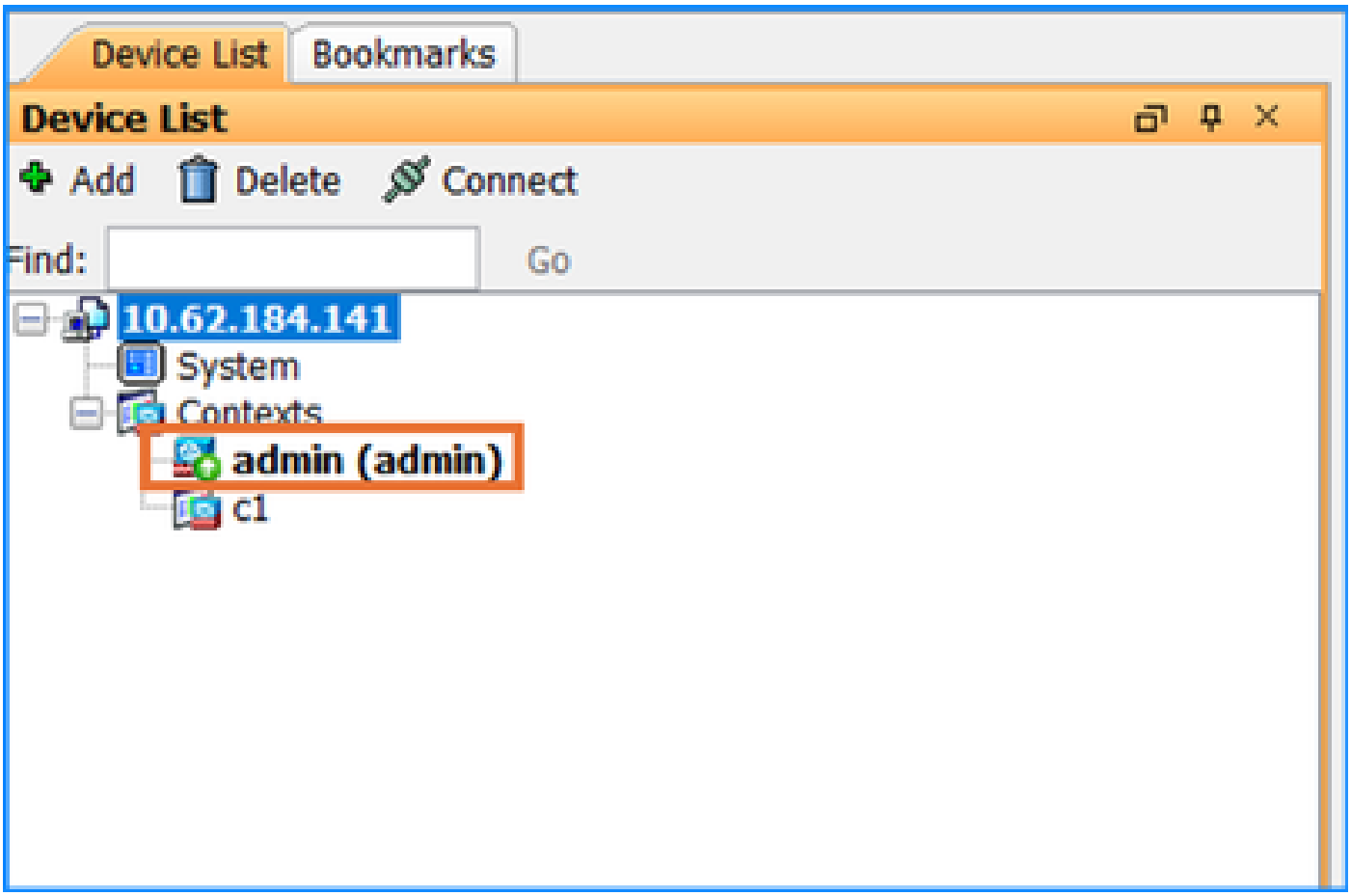
Problema 6. Impossibile verificare la presenza di aggiornamenti ASA/ASDM in modalità a più contesti

L'opzione Tools > Check for ASA/ASDM Updates (Strumenti > Controlla aggiornamenti ASA/ASDM) è disattivata in modalità a più contesti:

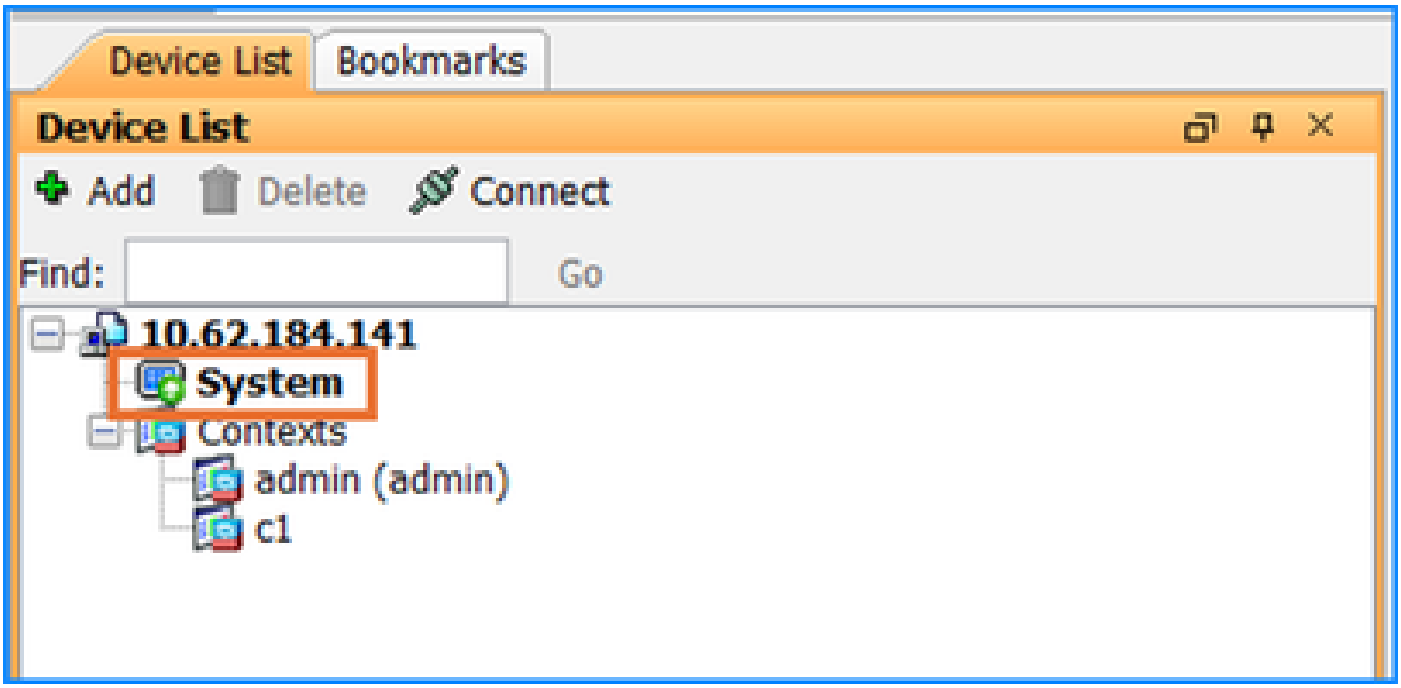


Risoluzione dei problemi - Azioni consigliate

In genere, questa opzione è disattivata perché nella scheda Elenco dispositivi il contesto di selezione corrente è il contesto amministrativo:



In tal caso, accertarsi di passare al contesto del sistema facendo doppio clic sull'icona Sistema:



Problema 7. "Il modulo delle condizioni generali di Cisco non è stato accettato o rifiutato per continuare il download." Messaggio di errore

"Il modulo delle condizioni generali di Cisco non è stato accettato o rifiutato per continuare il

download." Quando l'utente tenta di aggiornare le immagini ASA/ASDM tramite il menu Tools > Check for ASA/ASDM Updates (Strumenti > Controlla aggiornamenti ASA/ASDM), viene visualizzato un messaggio di errore.

Risoluzione dei problemi - Azioni consigliate

Questo messaggio di errore viene visualizzato se il Contratto di Licenza con l'utente finale (EULA) non viene accettato dall'utente. Per continuare, assicurarsi di accettare l'EULA.

Riferimenti

- Contratto di licenza con l'utente finale

Problema 8. Impossibile scaricare il software per hardware specifico

La pagina Download del software non mostra alcune versioni del software ASA/ASDM per hardware specifico.

Risoluzione dei problemi - Azioni consigliate

La disponibilità del software per hardware specifico dipende principalmente dalla compatibilità e dalle fasi cardine di fine ciclo di vita (EoL). In caso di incompatibilità, prodotti EoL o rinvii di rilascio, le versioni software non sono generalmente disponibili per il download.

Per verificare la compatibilità e le versioni supportate, eseguire i passaggi seguenti:

1. Verificare la compatibilità tra le versioni software e hardware. Fare riferimento alla sezione sulla compatibilità ASA per Cisco Secure Firewall.
2. Controllare la data di fine del rilascio del software di manutenzione e l'ultima data di supporto negli avvisi di fine del ciclo di vita e di fine vendita

- Data di fine del rilascio del software di manutenzione: ultima data utile in cui Cisco Engineering può rilasciare le versioni finali del software di manutenzione o le correzioni dei bug. Dopo questa data, Cisco Engineering non sviluppa, ripara, mantiene o testa più il software del prodotto.
- Ultima data supporto: ultima data utile per ricevere assistenza e supporto applicabili per il prodotto in base ai contratti di assistenza attivi o ai termini e alle condizioni della garanzia. Dopo questa data, tutti i servizi di supporto per il prodotto non saranno disponibili e il prodotto diventerà obsoleto.

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. Per il differimento o la rimozione del rilascio, consultare le note di rilascio di Cisco Secure Firewall ASA e le note di rilascio di Cisco Secure Firewall ASDM.

Riferimenti

- Compatibilità ASA Cisco Secure Firewall
- Notifiche di fine del ciclo di vita e di fine vendita

- Note sulla release di Cisco Secure Firewall ASA
- Note sulla release di Cisco Secure Firewall ASDM

Problema 9. Messaggio di errore "Errore durante l'esecuzione del codice di risposta HTTP per il trasferimento di file -1"

Quando l'utente carica un file nel firewall utilizzando l'opzione Strumenti ASDM > Gestione file, viene visualizzato il messaggio di errore "Errore durante l'esecuzione del trasferimento del file con codice di risposta HTTP -1".

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCvf85831 del software "ASDM error has been Performed in File Transfer HTTP Response code -1" during image upload" (Errore ASDM durante l'esecuzione del codice di risposta HTTP per il trasferimento file -1).

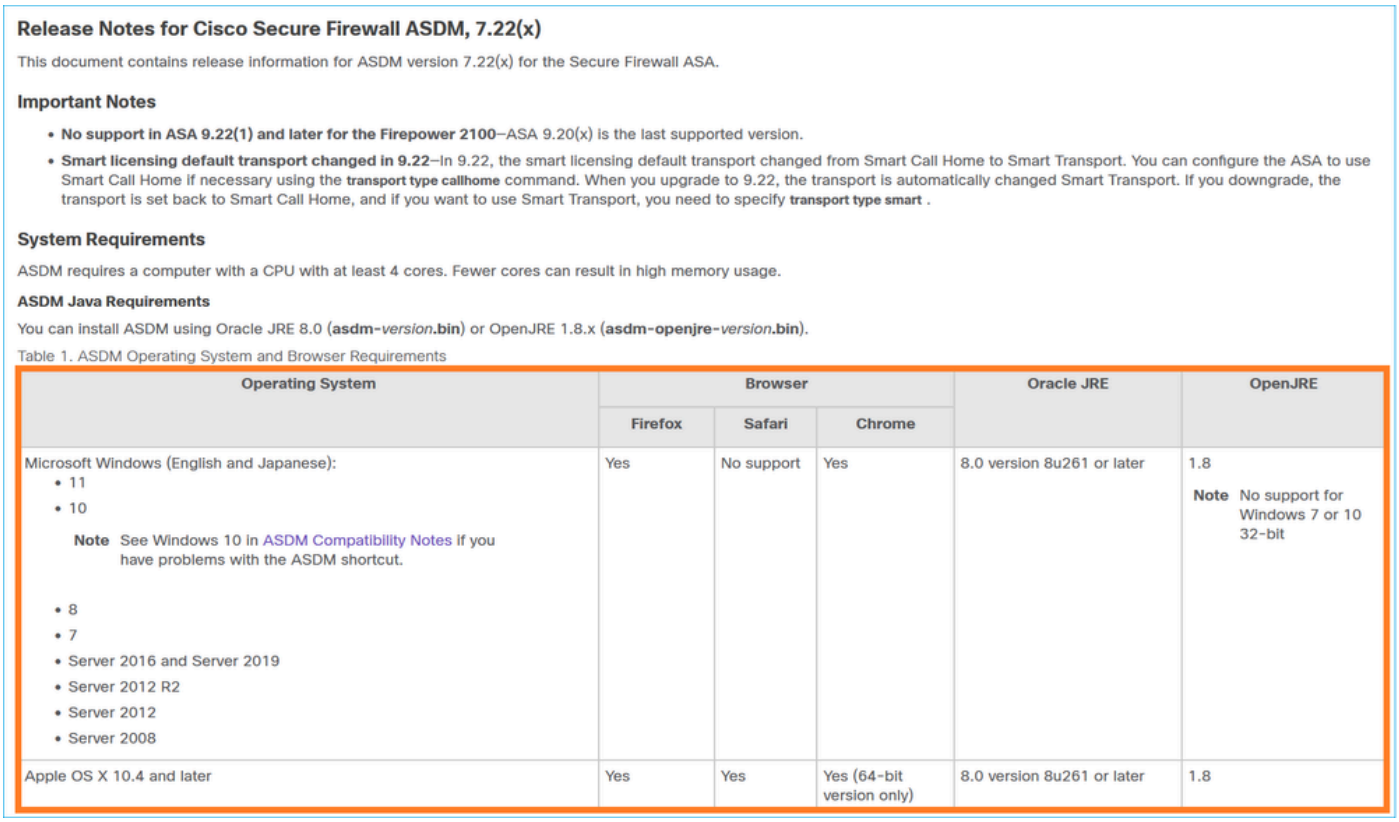
Problemi di compatibilità ASDM

In questa sezione vengono illustrati i problemi più comuni relativi alla compatibilità ASDM.

In generale, ASDM deve essere compatibile con i seguenti componenti:

- ASA
- Java
- Sistema operativo (OS)
- Browser
- Modulo SFR (se utilizzato)

Pertanto, prima di installare o aggiornare ASDM, si consiglia di controllare sempre prima questa tabella:



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

Quindi la tabella Compatibilità ASA e ASDM per modello, ad esempio:

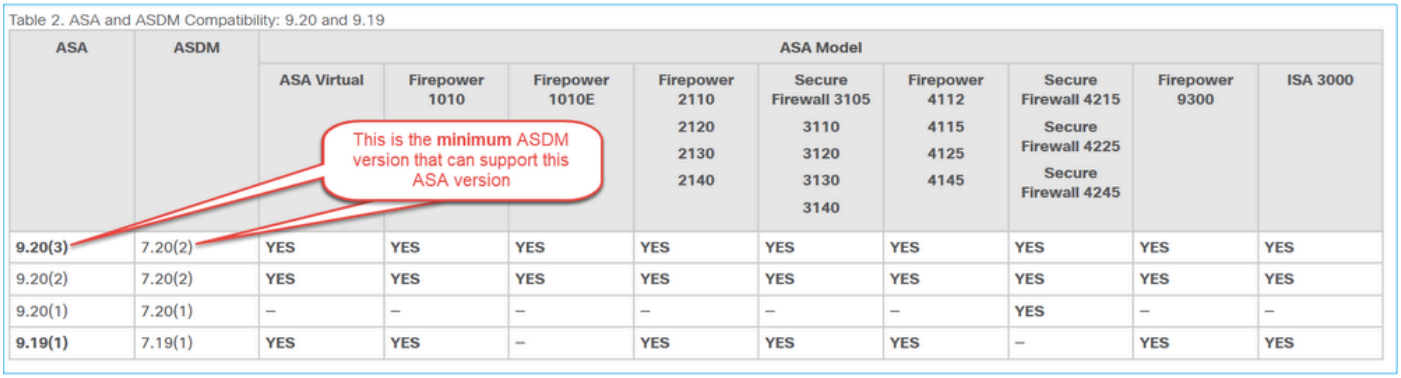


Table 2. ASA and ASDM Compatibility: 9.20 and 9.19

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

Note:

Le nuove versioni ASA richiedono la versione ASDM di coordinamento o una versione successiva; non è possibile usare una versione precedente di ASDM con una nuova versione di ASA.

Esempio 1

Non è possibile usare ASDM 7.17 con ASA 9.18. Per gli interni ASA, è possibile continuare a usare la versione ASDM corrente, a meno che non sia specificato diversamente. Ad esempio, è possibile usare ASA 9.2(1.2) con ASDM 7.2(1).

Esempio 2

Si dispone di ASAS 9.8(4)32. È possibile utilizzare ASDM 7.19(1) per gestirlo poiché ASDM è compatibile con le versioni precedenti, a meno che non sia diversamente indicato nelle note sulla versione di ASDM.

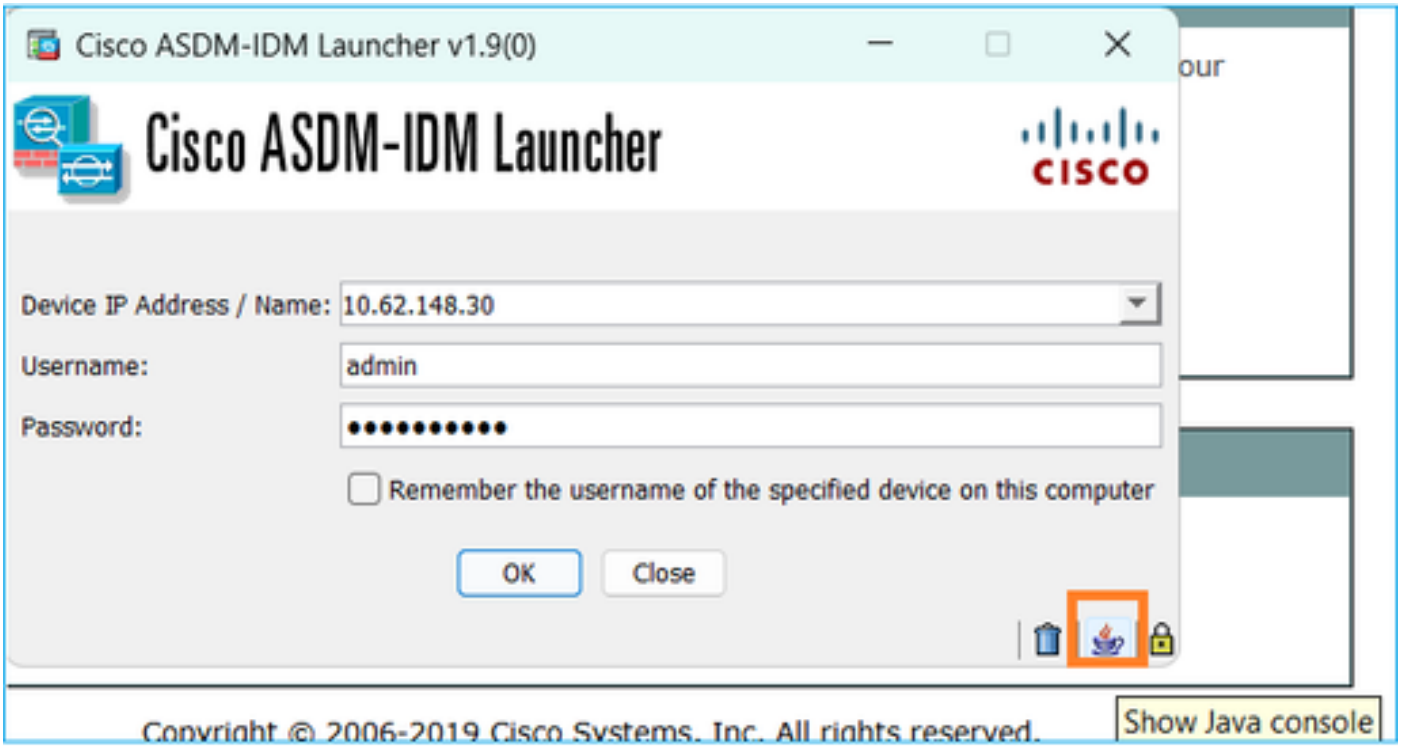
Riferimenti

- 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

Problema 1. Versione Java non compatibile

Risoluzione dei problemi - Passi consigliati

Controllare i log della console Java:



Quindi, controllare le guide alla compatibilità Java e ASA:

- 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

Problema 2. Versione ASA e ASDM non compatibili

Se si eseguono versioni ASA e ASDM non compatibili, è possibile perdere l'accesso all'interfaccia utente di ASDM.

Risoluzione dei problemi - Passi consigliati

È necessario installare la versione ASDM dalla CLI del dispositivo, copiare l'immagine nella memoria flash dell'ASA tramite TFTP e impostare l'immagine ASDM utilizzando il comando "asdm image" come spiegato nella guida di seguito:

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

Esempio

<#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
```

Problema 3. Supporto ASDM e OpenJDK

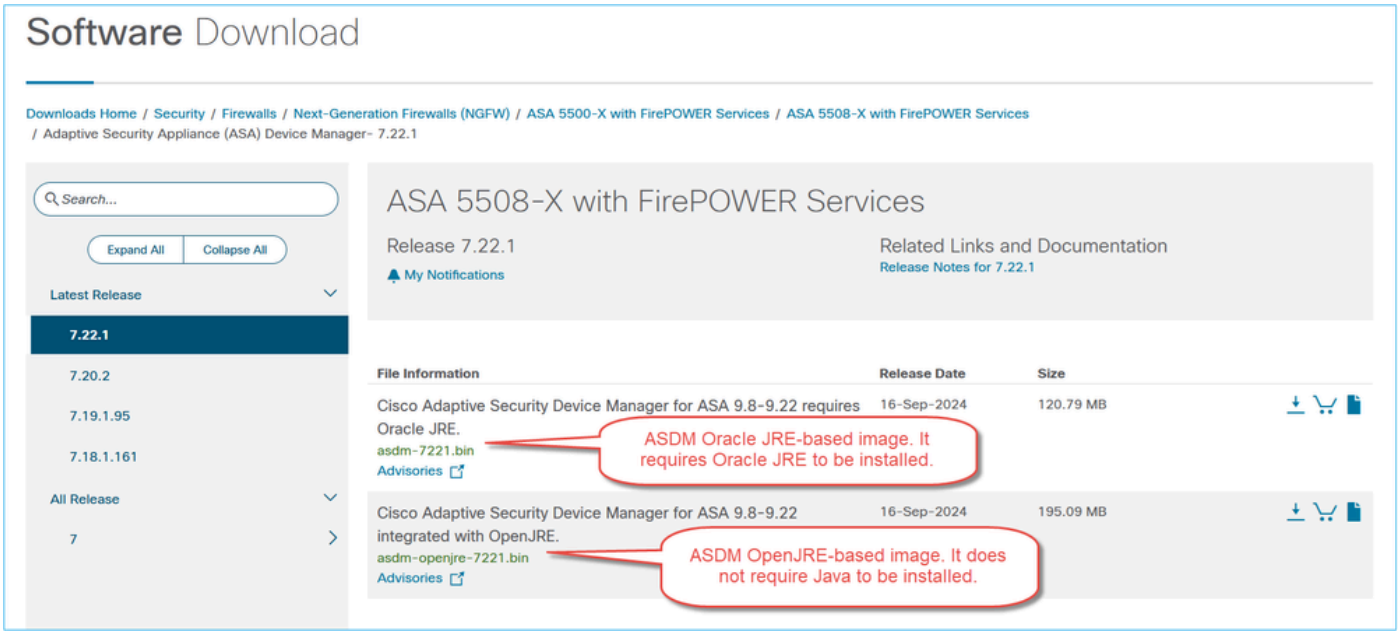
L'immagine Cisco ASDM non supporta ufficialmente OpenJDK. Pertanto, sono disponibili due opzioni:

- Oracle JRE: Contiene il runtime Java Web Start per avviare ASDM sul PC host. Per utilizzare questo metodo è necessario che Oracle JRE a 64 bit sia installato sul PC locale. Potete scaricarlo dal sito ufficiale di Java.

- OpenJRE: L'immagine JRE aperta è uguale a quella di Oracle, ma la differenza è che non è necessario installare Oracle JRE a 64 bit sul PC locale, poiché l'immagine stessa dispone della funzione Java Web Start per avviare ASDM. Questo è il motivo per cui le dimensioni dell'immagine OpenJRE sono maggiori di quelle di Oracle JRE. Si noti che è previsto che OpenJRE utilizzi una versione di Java meno recente, in quanto vengono compilati con l'ultima versione stabile disponibile all'inizio del ciclo di sviluppo di ASDM openJRE.

Oracle JRE e OpenJRE

	Oracle JRE	OpenJRE
Richiede l'installazione di Java sull'host finale	Sì	No (ha il proprio Java integrato)
Proprietario	Sì	No (open source)
Dimensioni immagine	Media	Più grande poiché ha anche Java integrato
Nome immagine	asdm-xxxx.bin	asdm-openjre-xxxx.bin



Suggerimento: Se si decide di modificare la versione del servizio di avvio ASDM, disinstallare prima il servizio di avvio ASDM esistente e quindi installare la nuova appliance connettendosi all'appliance ASA tramite HTTPS.

Riferimenti

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- OpenJDK Ambiente di sviluppo e runtime completo, open-source, licenza GPL.
- Oracle JRE: Solo ambiente di runtime, licenza proprietaria, richiede una licenza commerciale per l'utilizzo in produzione.
- OpenJRE: Solo ambiente di runtime, open-source, licenza GPL.
- https://www.oracle.com/java/technologies/javase/jre8-readme.html

Problema 4. Compatibilità tra ASDM e Java Azul Zulu

Le immagini ASDM basate su Oracle JRE non supportano Java Azure Zulu. D'altra parte, le immagini basate su ASDM OpenJRE vengono integrate in Azul Zulu. Per informazioni sulle opzioni disponibili, vedere le raccomandazioni relative al problema 3.

Problema 5. AVVISO: Firma non trovata nel file disk0:/asdm-xxx.bin

Esempio:

<#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.
```

Risoluzione dei problemi - Passi consigliati

In genere, si tratta di un problema di compatibilità tra ASA e ASDM. Controllare la guida alla compatibilità ASDM e verificare che l'ASDM sia compatibile con l'immagine ASA. La matrice di compatibilità ASA e ASDM è disponibile all'indirizzo:

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

Problema 6. "% ERRORE: Il pacchetto ASDM non è firmato digitalmente. Rifiuto della configurazione in corso."

Questo messaggio di errore può essere visualizzato quando si imposta una nuova immagine ASDM utilizzando asdm image <percorso immagine>

Risoluzione dei problemi - Azioni consigliate

1. L'ASA convalida se l'immagine ASDM è un'immagine Cisco con firma digitale. Se si tenta di eseguire un'immagine ASDM precedente con una versione ASA con questa correzione, ASDM viene bloccato e viene visualizzato il messaggio "%ERRORE: La firma non valida per il file disk0:/<filename>" viene visualizzata nella CLI dell'ASA. ASDM release 7.18(1.152) e successive sono compatibili con tutte le versioni precedenti delle appliance ASA, anche quelle senza questa correzione. Fare riferimento alla sezione Note importanti in Note sulla release per Cisco ASDM, 7.17(x).

2. Aggiornare la versione Java sul PC host.

3. Per un'appliance ASA in esecuzione su Secure Firewall 3100, controllare l'ID bug Cisco del software CSCwc1232 "Errore di verifica dell'immagine ASDM con firma digitale sulle piattaforme FPR3100"

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

Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 7. "%ERRORE: Firma non valida per il file disk0:/<nomefile>"

L'errore viene visualizzato durante la copia del file, ad esempio:

<#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.
```

Risoluzione dei problemi - Azioni consigliate

ASA 9.14(4.14) e versioni successive richiedono ASDM 7.18(1.152) o versioni successive. L'ASA convalida ora se l'immagine ASDM è un'immagine Cisco con firma digitale. Se si tenta di eseguire

un'immagine ASDM precedente alla versione 7.18(1.152) con una versione ASA con questa correzione, ASDM viene bloccato e viene visualizzato il messaggio "%ERROR: La firma non valida per il file disk0:/<filename>" viene visualizzata nella CLI dell'ASA.

Questa modifica è stata introdotta a causa della vulnerabilità dell'esecuzione di codice arbitrario sul lato client di Cisco ASDM e ASA Software (CVE ID CVE-2022-20829)

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

Se il dispositivo funziona in modalità Piattaforma, seguire le istruzioni riportate nel presente documento per caricare l'immagine: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_zp4_dzj_cjb

Riferimenti

- Note sulla release di ASDM: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3
- Guida all'aggiornamento dell'ASA: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task_E9EE51964590499999B1D976F66E2771

Problema 8. Compatibilità Della Postura Del Firewall Protetta (Hostscan)

La versione di Hostscan dipende più dalla versione di AnyConnect che dalla versione di ASA. Entrambe le versioni sono disponibili qui: Download del software - Cisco Systems:

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

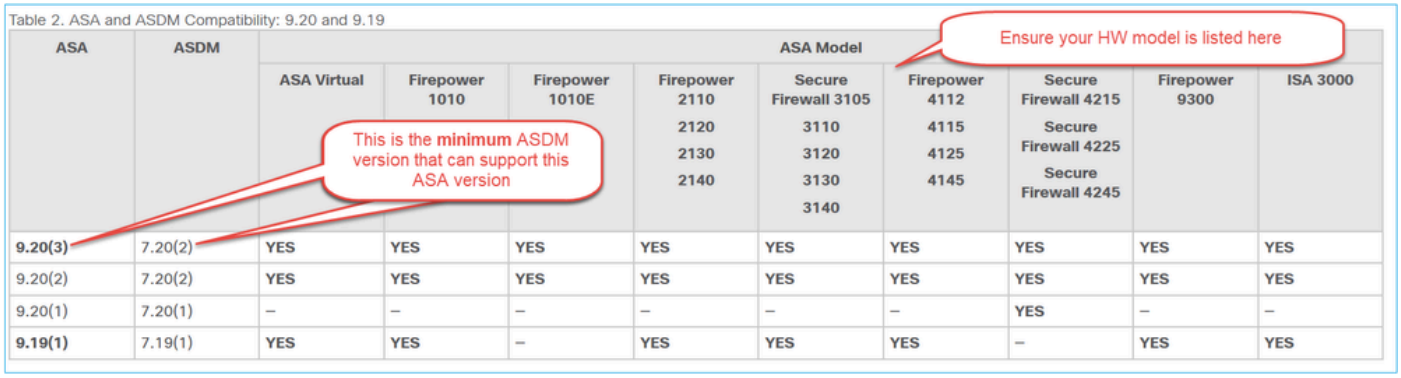
Problema 9. Ultima versione supportata

Risoluzione dei problemi - Azioni consigliate

Se si desidera conoscere l'ultima versione supportata di ASDM per il firewall, sono disponibili principalmente due documenti da controllare:

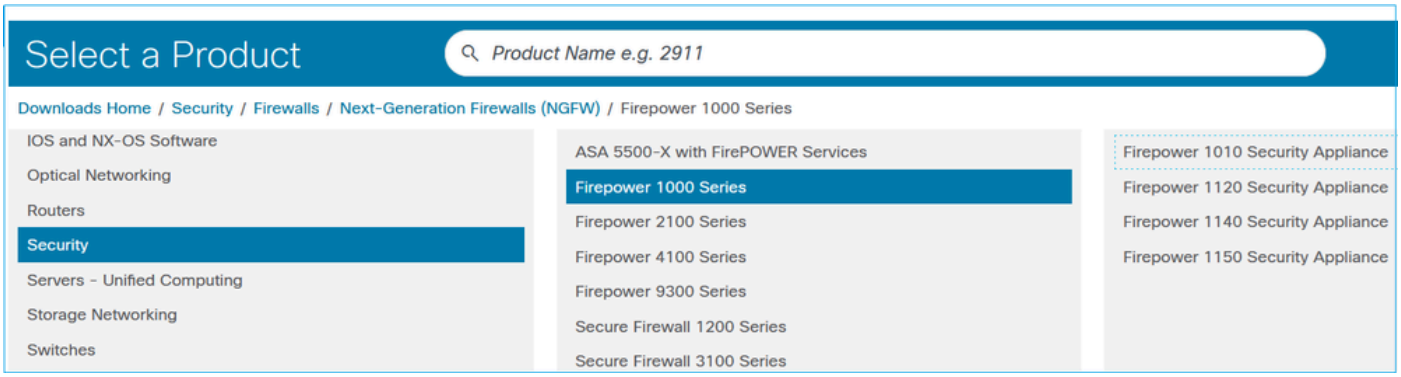
- Note sulla release di ASDM: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3

In particolare, la tabella del modello ASA

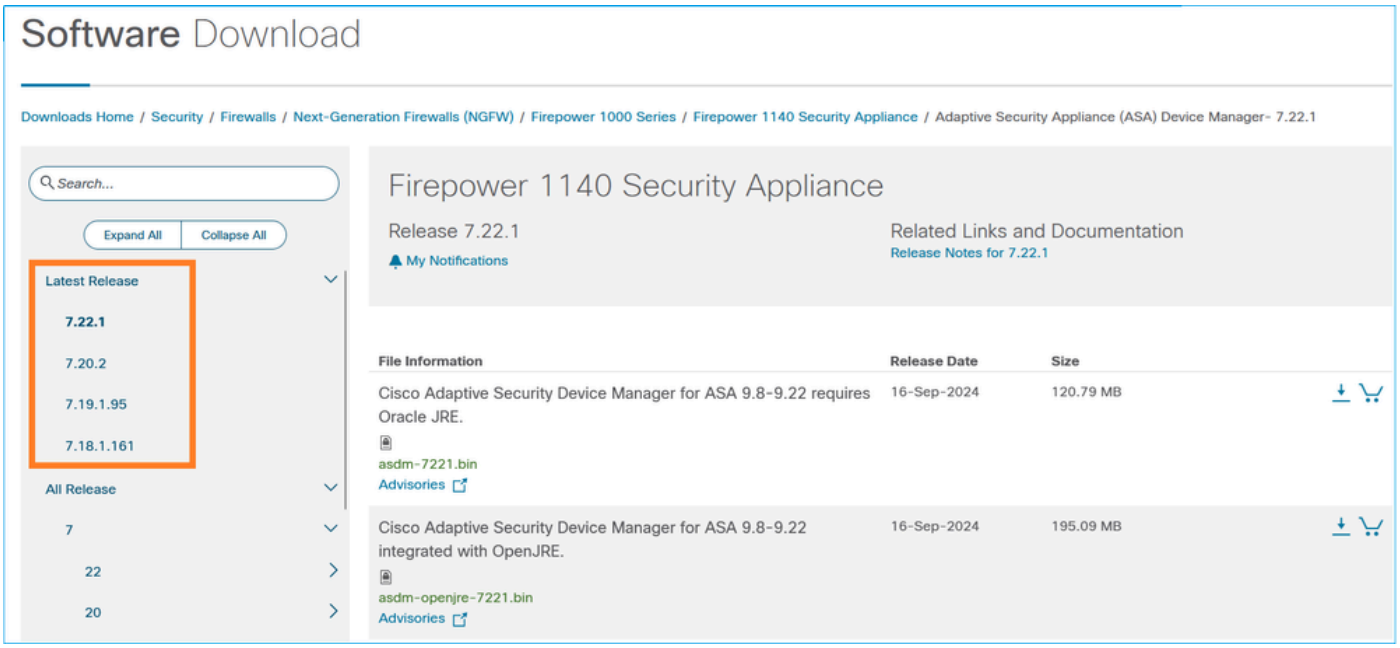


Il secondo documento è la pagina di download del software:

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



È possibile trovare le versioni più recenti di ASDM per ciascun treno SW supportato dal proprio hardware, ad esempio:

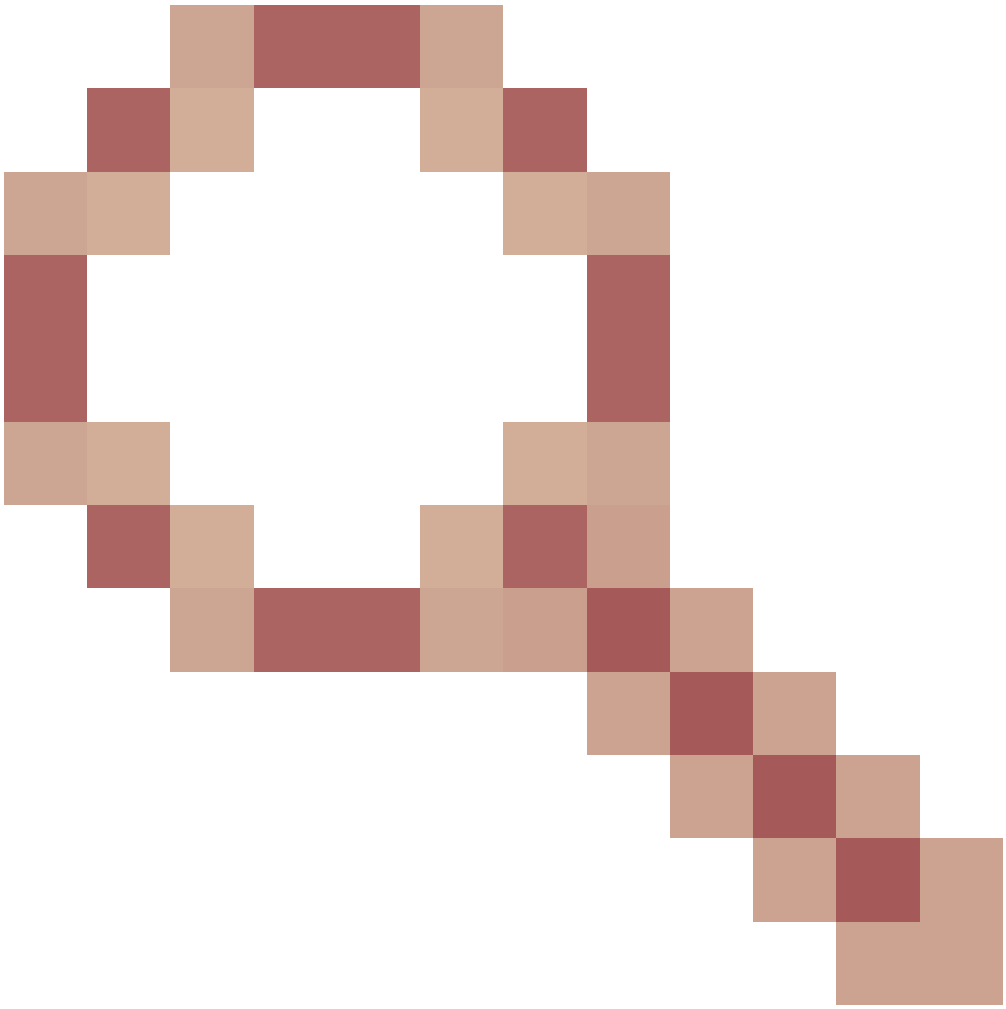


Problema 10. Supporto ASDM su Linux

Risoluzione dei problemi - Azioni consigliate

Linux non è ufficialmente supportato.

Miglioramento correlato:



ID bug Cisco CSCwk67345
ENH: Includi Linux nell'elenco dei sistemi operativi supportati

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

Problema 11. Termine del supporto ASDM

Risoluzione dei problemi - Azioni consigliate

Vedere gli avvisi di fine del ciclo di vita e di fine vendita di ASA/ASDM:

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

Problemi di licenza ASDM

In questa sezione vengono illustrati i problemi più comuni relativi alle licenze ASDM.

Il modello Smart Licensing viene utilizzato da:

- Registrazione chassis Firepower 4100/9300: Gestione delle licenze per l'appliance ASA
- ASAv, Firepower 1000, Firepower 2100, Firepower 9300 e Firepower 4100: Licenze: Smart Software Licensing (ASAv, ASA su Firepower)

Tutti gli altri modelli usano la licenza Product Authorization Key (PAK)

Riferimenti

- Licenze per funzionalità Cisco Secure Firewall serie ASA - Linee guida modello

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

Problema 1. Licenza Smart 3DES/AES mancante

ASDM richiede una licenza Strong Encryption (3DES/AES) sull'appliance ASA, a meno che non si acceda ad essa utilizzando l'interfaccia di gestione. Per abilitare l'accesso ASDM su un'interfaccia dati, è necessario ottenere la licenza 3DES/AES.

Per richiedere una licenza 3DES/AES da Cisco:

1. Visitare il sito Web all'indirizzo https://www.cisco.com/go/license
2. Fare clic su Continue to Product License Registration (Continua alla registrazione delle licenze dei prodotti).
3. Nel portale delle licenze, fare clic su Get Other Licenses accanto al campo di testo.
4. Selezionare IPS, Crypto, Other... dall'elenco a discesa.
5. Digitare ASA nel campo Search by Keyword (Cerca per parola chiave).
6. Selezionare Cisco ASA 3DES/AES License nell'elenco dei prodotti, quindi fare clic su Next (Avanti).
7. Immettere il numero di serie dell'appliance ASA e seguire le istruzioni per richiedere una licenza 3DES/AES per l'appliance ASA.

Risoluzione dei problemi - Azioni consigliate

Per abilitare la licenza e registrarsi al portale Cisco Smart Licensing, verificare che i seguenti elementi siano presenti:

- L'orologio dell'ASA visualizza l'ora corretta. Si consiglia di utilizzare un server NTP.
- Routing verso il portale Cisco Smart Licensing.
- Il traffico HTTPS non è bloccato dal firewall al portale delle licenze. Una raccolta di acquisizione sul firewall può confermarlo.
- Se è necessario utilizzare un server proxy HTTP, includere il comando necessario, ad esempio:

<#root>

```
ciscoasa(config)#
```

call-home

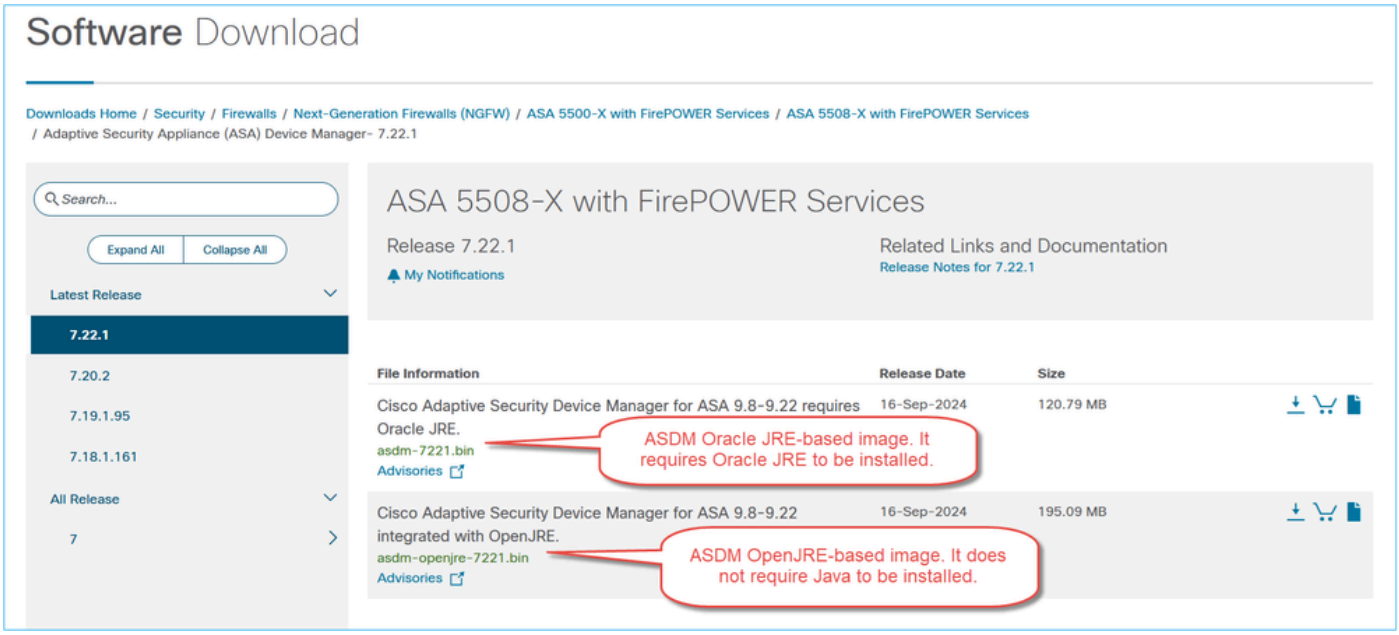
```
ciscoasa(cfg-call-home)#
http-proxy 10.1.1.1 port 443
```

Problema 2. Requisiti di licenza di Oracle Java JRE

Risoluzione dei problemi - Azioni consigliate

Il file di immagine .bin ASDM è disponibile in due versioni:

- Oracle JRE: Contiene il runtime Java Web Start per avviare ASDM sul PC host. Per utilizzare questo metodo è necessario che Oracle JRE a 64 bit sia installato sul PC locale. Potete scaricarlo dal sito ufficiale di Java.
- OpenJRE: L'immagine JRE aperta è uguale a quella di Oracle, ma la differenza è che non è necessario installare Oracle JRE a 64 bit sul PC locale, poiché l'immagine stessa dispone della funzione Java Web Start per avviare ASDM.



Se si decide di utilizzare l'immagine ASDM basata su Oracle, è necessario disporre di una licenza Java quando si utilizza l'immagine per scopi non personali. Domande frequenti su Oracle Java SE Licensing:

Per uso personale si intende l'utilizzo di Java in un computer desktop o portatile per eseguire attività quali giochi o altre applicazioni personali. Se si utilizza Java in un computer desktop o portatile come parte di qualsiasi operazione aziendale, non si tratta di un utilizzo personale. È possibile, ad esempio, utilizzare un'applicazione di produttività Java per eseguire i compiti o le imposte personali, ma non è possibile utilizzarla per la contabilità aziendale.

Se non si desidera applicare alcuna licenza Java, è possibile utilizzare l'immagine ASDM basata su OpenJRE.

Riferimenti

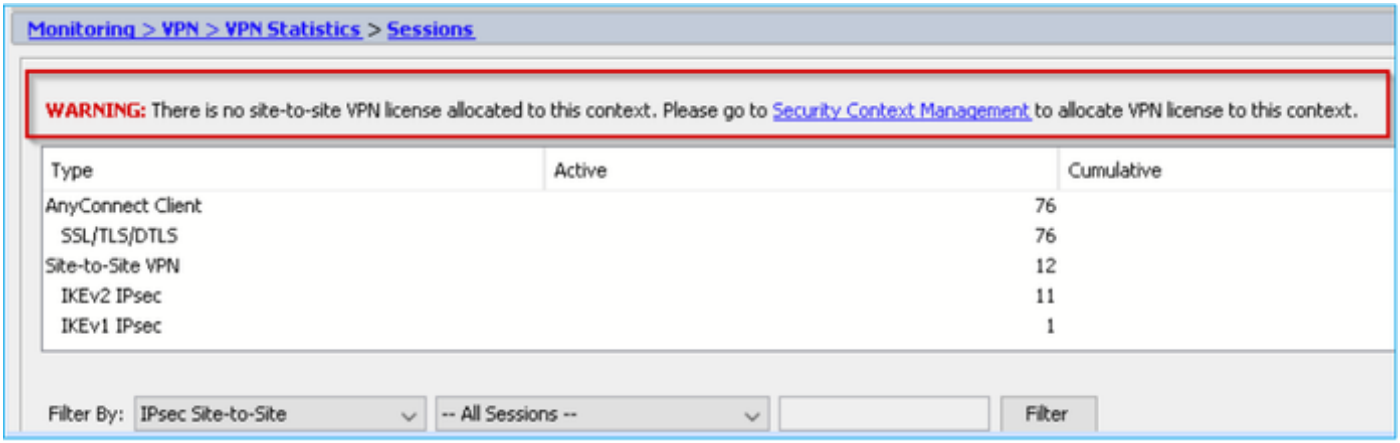
- https://www.oracle.com/java/technologies/javase/jdk-faqs.html
- Requisiti Java ASDM per ASDM 7.2: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- Note sulla compatibilità ASDM per ASDM 7.2: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476

Nota: Consultare le note sulla versione di ASDM in uso.

Problema 3. Avviso ASDM sulla licenza VPN da sito a sito in modalità multicast

ASDM visualizza quanto segue:

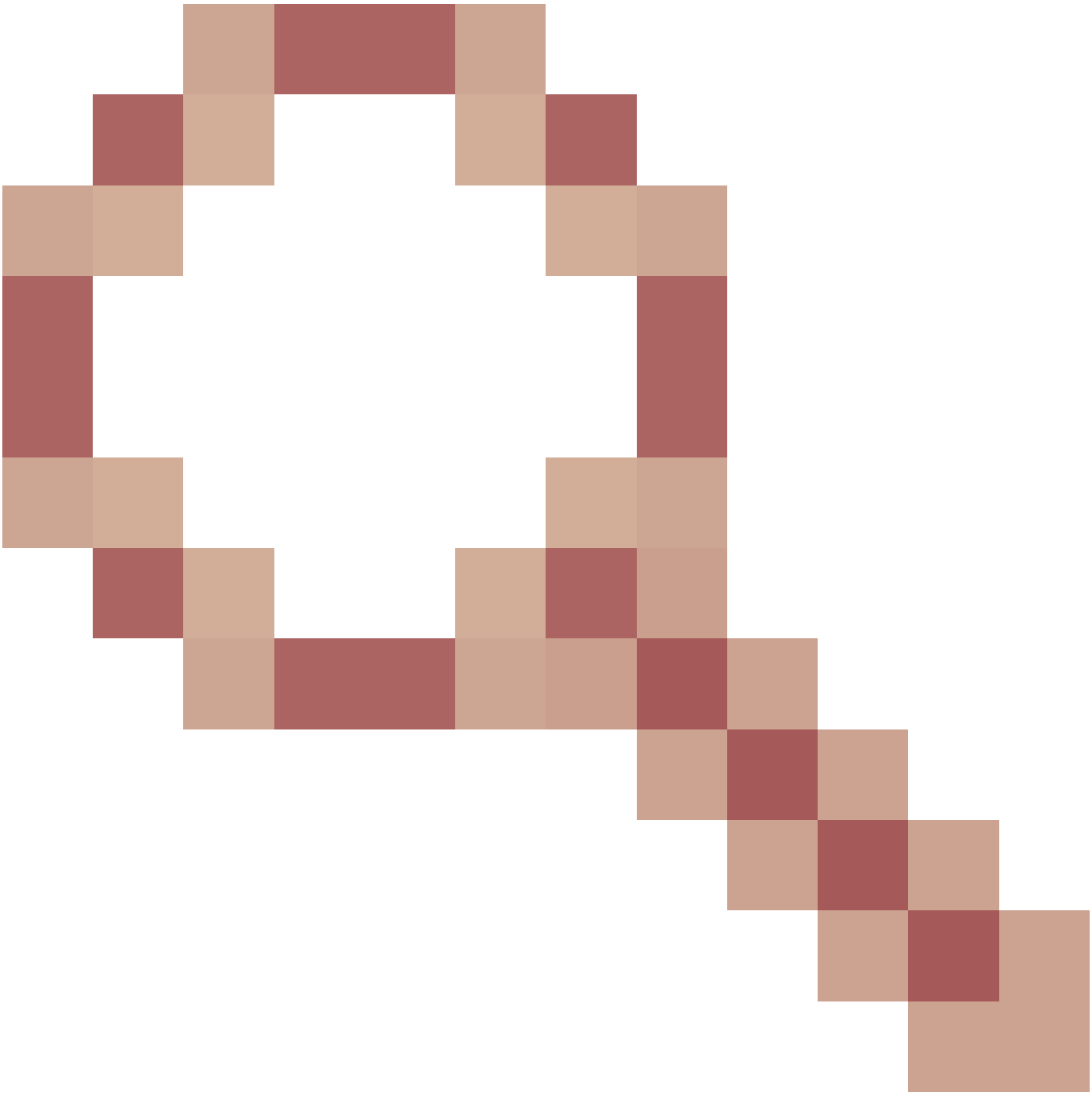
AVVISO: Nessuna licenza VPN da sito a sito allocata a questo contesto. Accedere a Gestione contesto di sicurezza per allocare la licenza VPN a questo contesto.



Risoluzione dei problemi - Azioni consigliate

Si tratta di un difetto del software cosmetico tracciato da:

ID bug Cisco CSCvj6962



ASDM 7.9(2) ASA 9.6(4)8 - errore persistente L2L multi-contesto

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

È possibile effettuare la sottoscrizione al difetto in modo da ricevere una notifica sugli aggiornamenti del difetto.

Riferimenti

- Guide alla configurazione ASDM
- Compatibilità Cisco ASA e ASDM per modello

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).