

# ASDMライセンス、アップグレード、および互換性の問題のトラブルシューティング

## 内容

---

### [はじめに](#)

### [背景](#)

#### [ASDMのアップグレードの問題](#)

[問題 1.ASA/ASDMアップグレードをソースバージョンXからターゲットバージョンYにアップグレードするには、どうすればよいですか。](#)

[問題 2.ASA/ASDMの推奨バージョンを教えてください。](#)

[問題3.ASDMでASA/ASDMアップデートのチェックが失敗するには、Tools > Check for ASA/ASDM Updatesを使用します。](#)

[問題 4.特定の脆弱性に対する修正が含まれているのはどのバージョンですか。](#)

[問題5.「% ERROR: ASDM package is not digitally signed.Rejecting configuration.」というエラーメッセージが表示されます](#)

[問題 6.マルチコンテキストモードではASA/ASDMアップデートを確認できない](#)

[問題 7.「Cisco's General Terms form have not been accepted or rejected to continue to download.」というエラーメッセージが表示されます](#)

[問題 8.特定のハードウェアのソフトウェアをダウンロードできない](#)

[問題 9.「Error occurred in performing File Transfer HTTP Response code -1」エラーメッセージ](#)

#### [ASDM互換性の問題](#)

[問題 1.互換性のない Java バージョン](#)

[問題 2.ASAとASDMのバージョンに互換性がない](#)

[問題3.ASDMとOpenJDKのサポート](#)

[問題 4.ASDMとJava Azul Zuluの互換性](#)

[問題 5.警告：ファイルdisk0:/asdm-xxx.binにシグニチャが見つかりません](#)

[問題6.「% ERROR: ASDM package is not digitally signed.設定を拒否しています。」](#)

[問題7. "%ERROR：ファイルdisk0:/のシグネチャが有効ではありません"](#)

[問題 8.セキュアファイアウォールポスチャ\(Hostscan\)の互換性](#)

[問題 9.サポートされる最新バージョン](#)

[問題 10.LinuxでのASDMサポート](#)

[問題 11.ASDMのサポート終了](#)

#### [ASDMライセンスの問題](#)

[問題1: 3DES/AESスマートライセンスが欠落している](#)

[問題 2.Oracle Java JREのライセンス要件](#)

[問題3.マルチコンテキストモードのサイト間VPNライセンスに関するASDMの警告](#)

### [参考資料](#)

---

## はじめに

このドキュメントでは、ASDMライセンス、アップグレード、および互換性の問題のトラブルシ

ユーティリティプロセスについて説明します。

## 背景

このドキュメントは、Adaptive Security Appliance(ASA)Device Manager(ASDM)のトラブルシューティングシリーズの一部で、次のドキュメントとともに提供されています。

- [ASDM起動問題のトラブルシューティング](#)
- [ASDMの設定、認証、およびその他の問題のトラブルシューティング](#)
- [ASDM TLSのセキュリティ、証明書、および脆弱性の問題のトラブルシューティング](#)

## ASDMのアップグレードの問題

問題 1.ASA/ASDMアップグレードをソースバージョンXからターゲットバージョンYにアップグレードするには、どうすればよいですか。

ユーザは、ASA/ASDMをソースバージョンXからターゲットバージョンYにアップグレードする際に支援を必要とします。

トラブルシューティング – 推奨処置

1. ASA、ASDM、オペレーティングシステム、およびJavaのバージョンがターゲットバージョンと互換性があることを確認します。製品が影響を受けるかどうかを確認するには、このアドバイザリの「[Cisco Secure Firewall ASAリリースノート](#)、[Cisco Secure Firewall ASDMリリースノート](#)、[Cisco Secure Firewall ASAの互換性](#)。

ASA、ASDM、オペレーティングシステム、およびJavaのバージョンには互換性があり、ターゲットのバージョンが特定のハードウェアでサポートされている必要があります。

<https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html>

2. Firepower 4100/9300で稼働するASAの場合、Firepower eXtensible Operating System(FXOS)とASAソフトウェアのバージョンに互換性があることを確認します。『[Cisco Firepower 4100/9300 FXOSの互換性](#)』を参照してください。

3. ターゲット・バージョンの変更に関する知識を確認するには、[Cisco Secure Firewall ASAリリースノート](#)、[Cisco Secure Firewall ASDMリリースノート](#)の場合 Firepower 4100/9300。また、[FXOSリリースノート](#)。

4. リリースノートでアップグレードパスを必ず確認してください。この例では、バージョン7.22のリリースノートの表2に、以前のバージョンからターゲットバージョンへのアップグレードパスが記載されています。

**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: → <b>9.22</b>
9.19	–	Any of the following: → <b>9.22</b> → 9.20
9.18	–	Any of the following: → <b>9.22</b> → 9.20 → 9.19
9.17	–	Any of the following: → <b>9.22</b> → 9.20 → 9.19 → 9.18
9.16	–	Any of the following: → <b>9.22</b> → 9.20 → 9.19 → 9.18 → 9.17

5. 互換性の要件が満たされたら、「ソフトウェアのダウンロード」ページから対象のASA/ASDMおよびFXOSバージョン ( Firepower 4100/9300のみ ) をダウンロードします。この例に示すように、特定のハードウェアモデルを選択してください。推奨リリースには、次の金色の星が付いています。

Select a Product  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. 『Cisco Secure Firewall ASA Upgrade Guide』の「[Planning Your Upgrade](#)」の章と「[Upgrade the ASA](#)」の章を必ず読んでください。

#### 参考資料

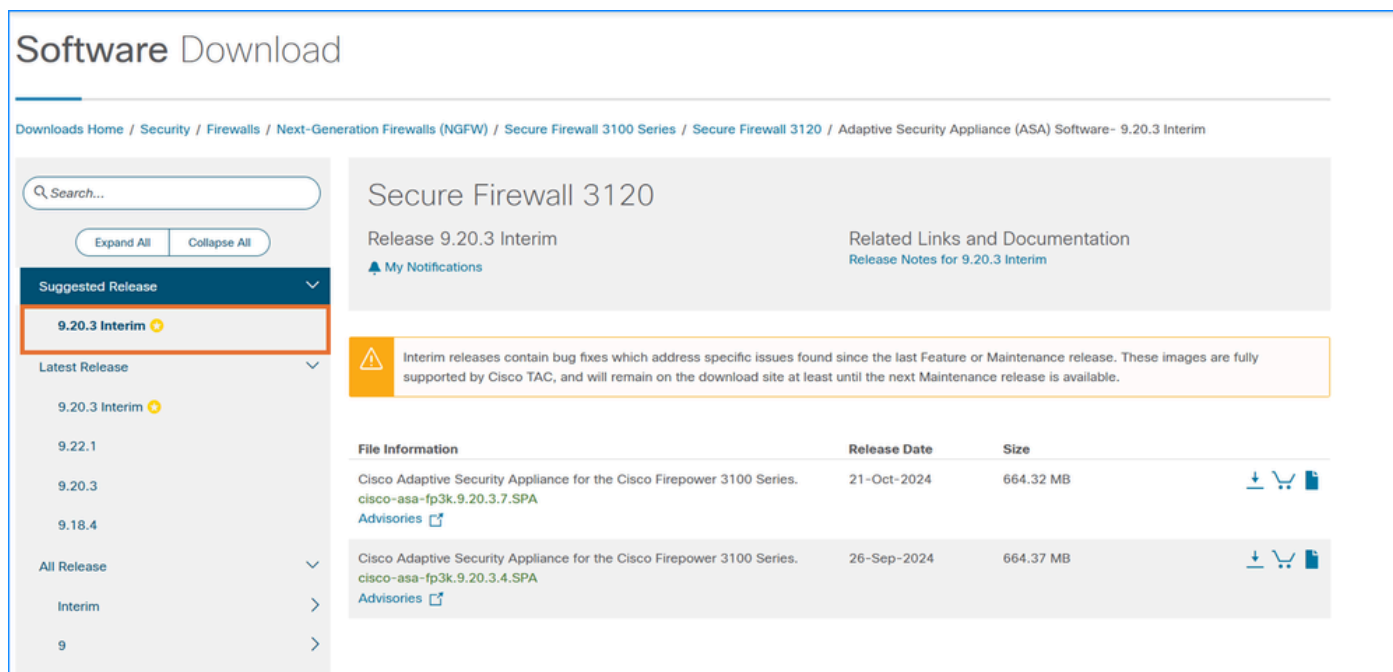
- [Cisco Secure Firewall ASAリリースノート](#)
- [Cisco Secure Firewall ASDMリリースノート](#)
- [Cisco Secure Firewall ASAの互換性](#)
- [Cisco Firepower 4100/9300 FXOSの互換性](#)
- [Cisco Secure Firewall ASA アップグレードガイド](#)

問題 2.ASA/ASDMの推奨バージョンを教えてください。

ユーザは、ASA/ASDMの推奨バージョンについて質問します。

#### トラブルシューティング – 推奨処置

Cisco TACでは、ソフトウェアのバージョンに関する推奨事項を提供していません。ユーザは、ソフトウェアの品質、安定性、および長期利用性に基づいて、シスコ推奨リリースをダウンロードできます。推奨リリースには、次に示すように金色の星が付いています。



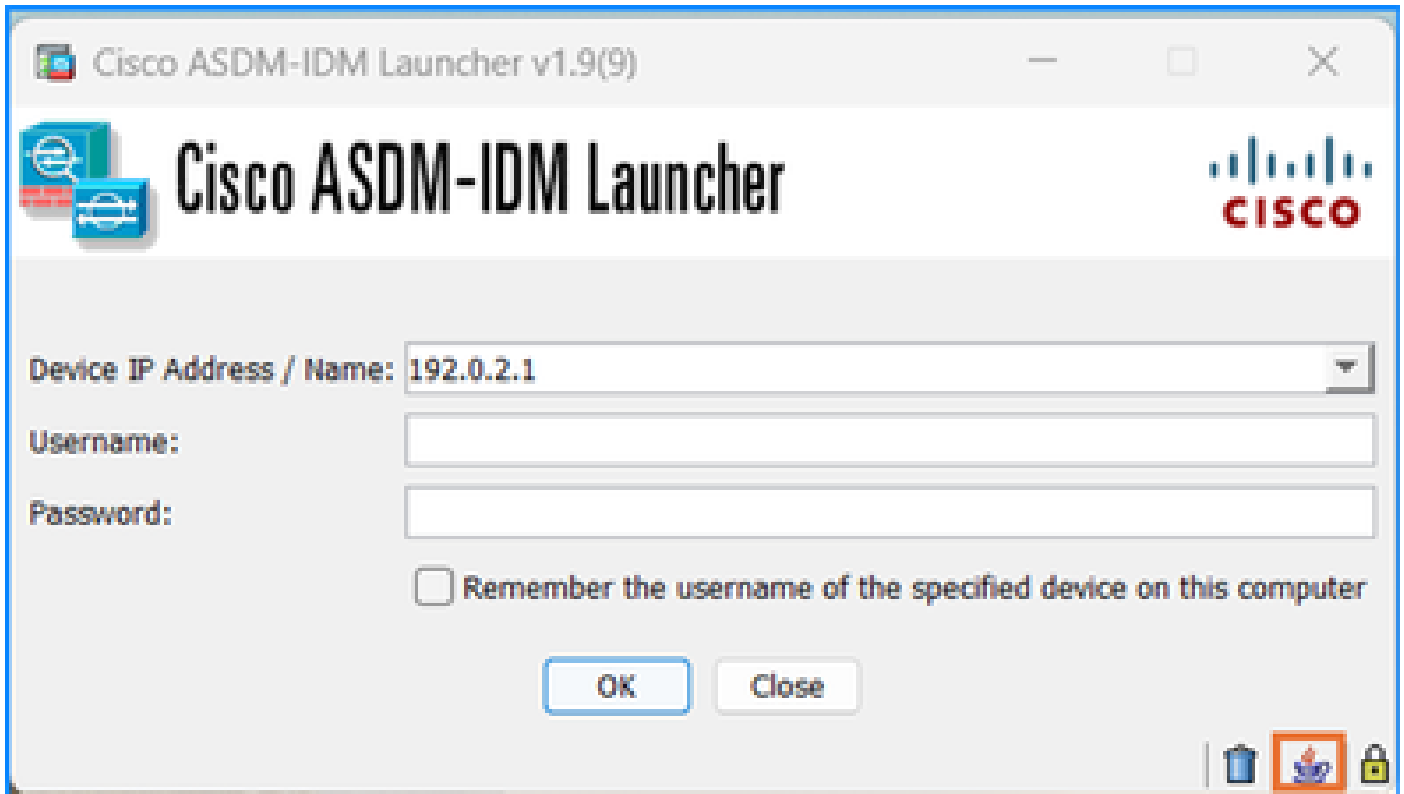
The screenshot shows the Cisco Software Download page for Secure Firewall 3120. The page title is "Software Download". The breadcrumb trail is: Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall 3100 Series / Secure Firewall 3120 / Adaptive Security Appliance (ASA) Software- 9.20.3 Interim. A search bar is present with "Search..." and buttons for "Expand All" and "Collapse All". A "Suggested Release" dropdown menu is open, showing "9.20.3 Interim" with a gold star icon, and "Latest Release" with a dropdown arrow. Below the dropdown, a list of releases is shown: "9.20.3 Interim" (gold star), "9.22.1", "9.20.3", "9.18.4", "All Release", "Interim", and "9". A warning message states: "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." A table of file information is displayed:

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	Download icons
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	Download icons

問題3.Tools > Check for ASA/ASDM Updates経由でASDM内のASA/ASDM更新チェックが失敗します。

Tools > Check for ASA/ASDM Updatesを使用してASDMのASA/ASDMアップデートを確認すると、失敗します。具体的には、次の症状が観察されます。

1. 正しい資格情報が入力されていても、[ログイン]ボタンをクリックすると、[ネットワークパスワードの入力]ウィンドウが再表示されます。
2. Javaコンソールのログに、「Meta data request failed」エラーが表示されます。



<#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.
```

## トラブルシューティング – 推奨処置

ソフトウェアのCisco Bug ID [CSCvf91260](#) 「ASDM: CCOからのアップグレードが認識されないことが原因で機能しない」のフィールドを参照してください。「メタデータ要求に失敗しました」。回避策は、ダウンロードページから直接イメージをダウンロードし、ファイアウォールにアップロードすることです。

---

 注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

問題 4.特定の脆弱性に対する修正が含まれているのはどのバージョンですか。

ユーザは、特定の脆弱性の修正済みバージョンについて質問します。

トラブルシューティング – 推奨処置

1. 影響を受ける製品のセキュリティアドバイザリを必ず確認してください。
2. セキュリティアドバイザリで、既存のハードウェアとソフトウェアバージョンをSoftware Checkerに提供し、Checkをクリックします。

## 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	Check		



3. 修正済みのバージョンが利用可能な場合は、「最初の修正済みバージョンまたは影響を受けないバージョン」の列のバージョンに注意してください。

Home / Cisco Security / Cisco Software Checker

Cisco Security  
Cisco Software Checker

1 — 2 — 3 Results for selected Cisco Security Advisories:  
Show advisory list Export Selected

software release(s)

9.18.3

Recalculate Back Start Over

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
<input checked="" type="checkbox"/> 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. 「問題1」の手順を実行します。How to upgrade ASA/ASDM upgrade from the source version X to the target version Y?」セクションを参照して、ソフトウェアをアップグレードします。

問題5. 「% ERROR: ASDM package is not digitally signed.Rejecting configuration.」というエラーメッセージが表示されます

「% ERROR: ASDM package is not digitally signed.」というエラーメッセージが表示されます。Rejecting configuration.」というエラーメッセージが表示されます。

トラブルシューティング – 推奨処置

1. ASAは、ASDMイメージがシスコのデジタル署名付きイメージであるかどうかを検証します。この修正を含むASAバージョンで古いASDMイメージを実行しようとする、ASDMがブロックされ、ASA CLIに「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが表示されます。ASDMリリース7.18(1.152)以降には、この修正が適用されていないバージョンも含め、すべてのASAバージョンとの下位互換性があります。『Cisco ASDM 7.17(x)リリースノート』の「[重要な注意事項](#)」セクションを参照してください。

2. セキュアファイアウォール3100上で稼働するASAについては、ソフトウェアのCisco Bug ID [CSCwc12322](#) 「Digitally signed ASDM image verification error on FPR3100 platforms」を確認してください。

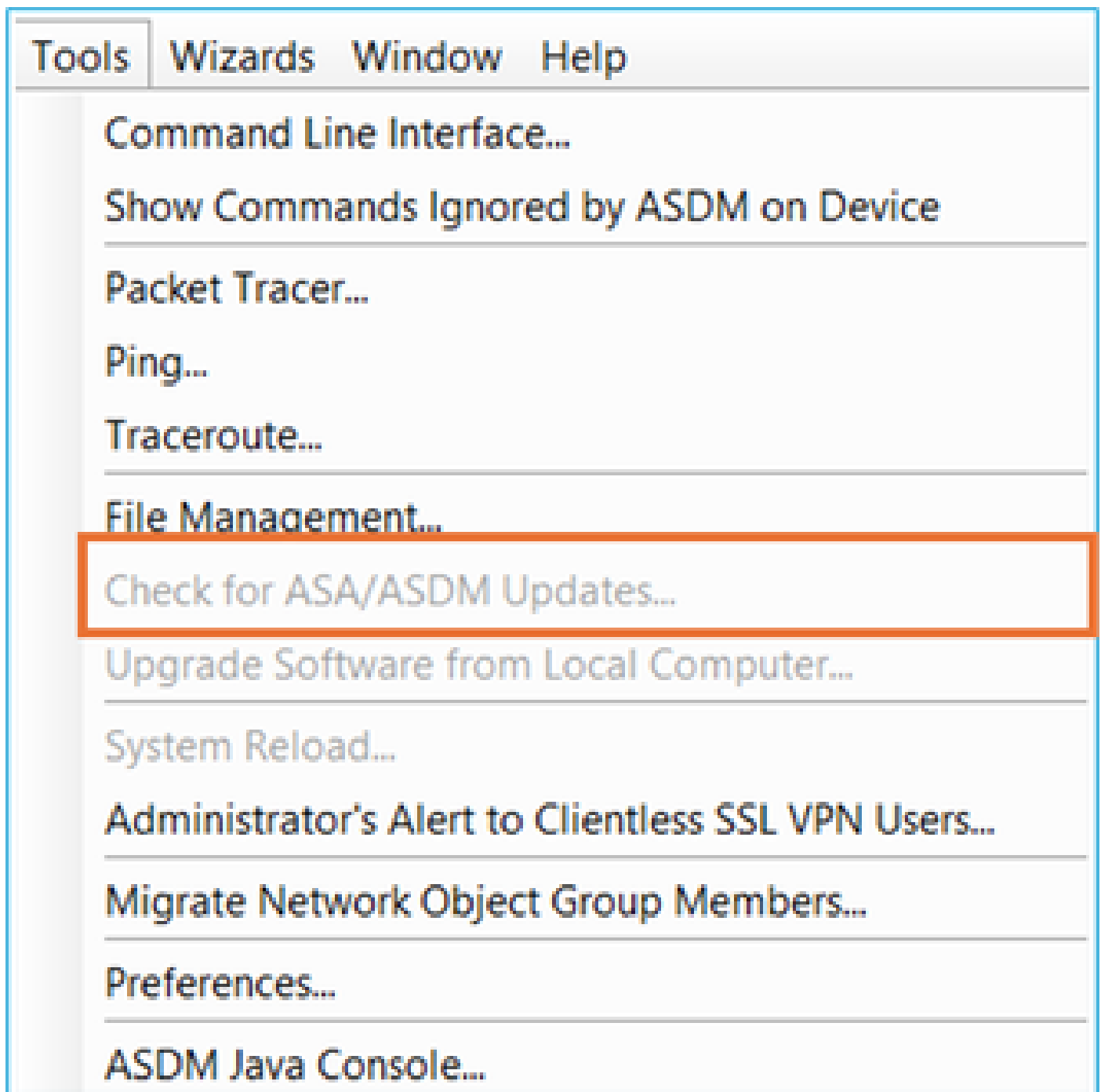
注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

## 参考資料

- [Cisco ASDM 7.17\(x\)のリリースノート](#)

問題 6. マルチコンテキストモードではASA/ASDMアップデートを確認できない

マルチコンテキストモードでは、「Tools」>「Check for ASA/ASDM Updates」オプションがグレー表示になります。

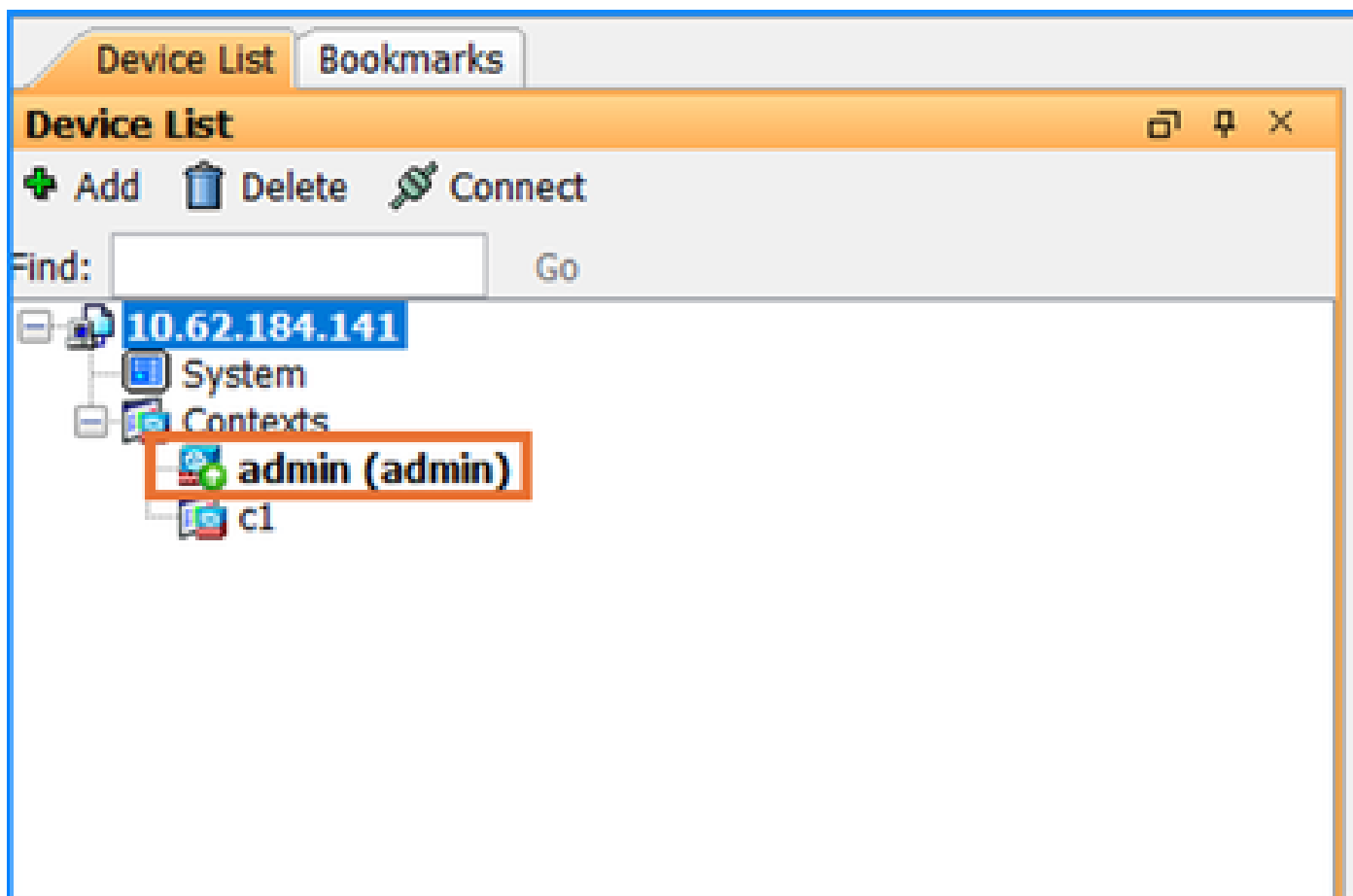


トラブルシューティング – 推奨処置

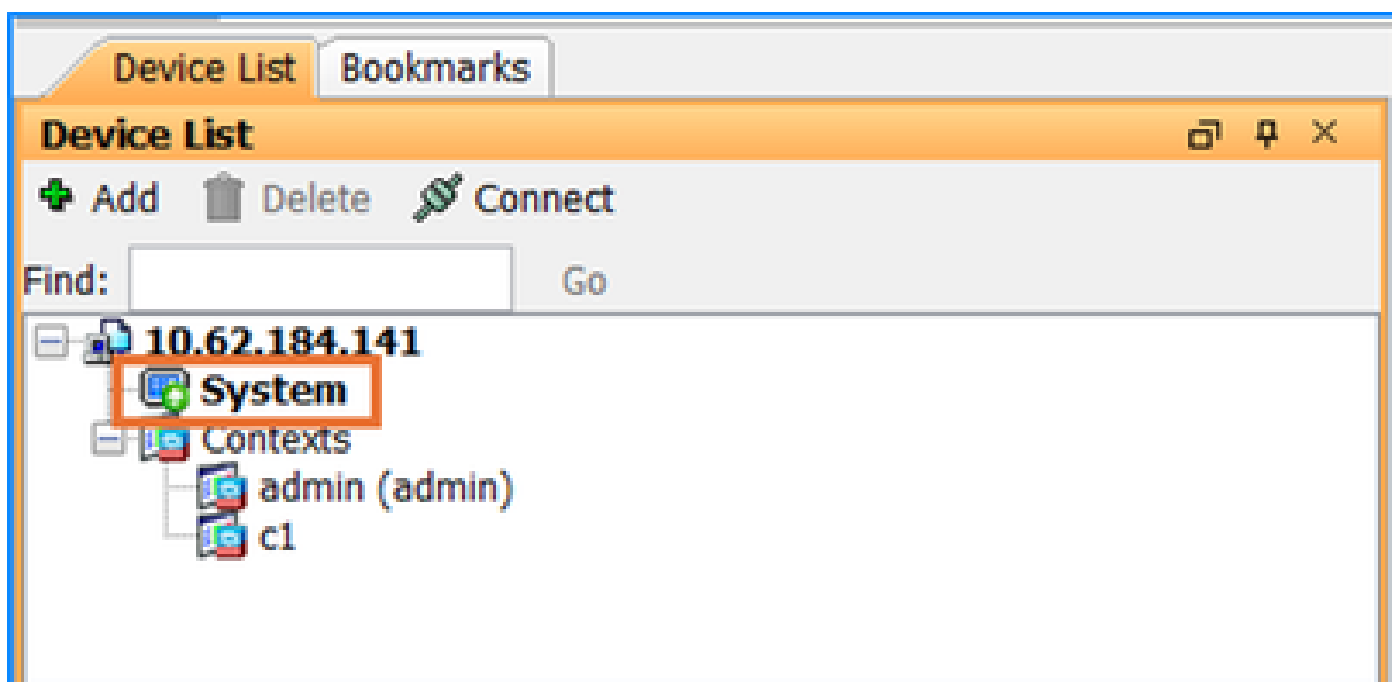
通常、このオプションはグレー表示されています。これは、デバイスリストタブで現在選択され



ているコンテキストが管理コンテキストになっているためです。



この場合、Systemアイコンをダブルクリックして、システムコンテキストに切り替えてください。



問題 7. 「Cisco's General Terms form have not been accepted or rejected to continue to download.」というエラーメッセージが表示されます

ユーザがTools > Check for ASA/ASDM Updates メニューを使用してASA/ASDMイメージを更新しようとする、 「Cisco's General Terms form have not been accepted or rejected to continue to download.」というエラーメッセージが表示されます。

#### トラブルシューティング – 推奨処置

このエラーメッセージは、[エンドユーザライセンス契約書\(EULA\)](#)がユーザに受け入れられない場合に表示されます。続行するには、EULAに同意してください。

#### 参考資料

- [エンドユーザライセンス契約書\(EULA\)](#)

#### 問題8：特定のハードウェアのソフトウェアをダウンロードできない

ソフトウェアのダウンロードページには、特定のハードウェアの一部のASA/ASDMソフトウェアバージョンは表示されません。

#### トラブルシューティング – 推奨処置

特定のハードウェアで利用可能なソフトウェアは、主に互換性とサポート終了(EoL)のマイルストーンによって異なります。非互換性、EoL製品、またはリリースの繰り延べの場合、ソフトウェアバージョンは通常ダウンロードできません。

互換性とサポートされているバージョンを確認するには、次の手順を実行してください。

1. ソフトウェアとハードウェアのバージョン間の互換性を確認します。『[Cisco Secure Firewall ASAの互換性](#)』を参照してください。
  2. [サポート終了および販売終了](#)通知で、ソフトウェアメンテナンスリリース終了日と[サポート終了日](#)を確認します。
- End of SW Maintenance Releases Date (ソフトウェアメンテナンスリリース終了日) : シスコエンジニアリングが最終のソフトウェアメンテナンスリリースまたはバグ修正をリリースできる最終日。この期間を過ぎると、シスコのエンジニアリング部門では、製品ソフトウェアの開発、修理、メンテナンス、テストを行わなくなります。
  - サポート終了日 : 有効なサービス契約または保証条件によって認められている製品に適用されるサービスとサポートを受けられる最終日。この日を過ぎると、製品のすべてのサポートサービスは提供されなくなり、製品は廃止となります。

## 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. リリースの保留や削除については、『[Cisco Secure Firewall ASAリリースノート](#)』および『[Cisco Secure Firewall ASDMリリースノート](#)』を確認してください。

### 参考資料

- [Cisco Secure Firewall ASAの互換性](#)
- [サポート終了と販売終了の通知](#)

- [Cisco Secure Firewall ASAリリースノート](#)
- [Cisco Secure Firewall ASDMリリースノート](#)

## 問題 9. 「Error occurred in performing File Transfer HTTP Response code -1」 エラーメッセージ

ユーザがASDM Tools > File Managementオプションを使用してファイアウォールにファイルをアップロードすると、「Error occurred in performing File Transfer HTTP Response code -1」というエラーメッセージが表示されます。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCvf85831](#) 「ASDM error "Error occurred in performing File Transfer HTTP Response code -1" during image upload」を参照してください。

## ASDM互換性の問題

このセクションでは、ASDMの互換性に関連する最も一般的な問題について説明します。

一般に、ASDMは次のコンポーネントと互換性がある必要があります。

- ASA
- JAVA
- オペレーティング システム ( OS )
- ブラウザ
- SFRモジュール ( 使用されている場合 )

したがって、ASDMをインストールまたはアップグレードする前に、必ず次の表を最初に確認することを強くお勧めします。

## 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): <ul style="list-style-type: none"> <li>• 11</li> <li>• 10</li> </ul> <b>Note</b> See Windows 10 in <a href="#">ASDM Compatibility Notes</a> if you have problems with the ASDM shortcut. <ul style="list-style-type: none"> <li>• 8</li> <li>• 7</li> <li>• Server 2016 and Server 2019</li> <li>• Server 2012 R2</li> <li>• Server 2012</li> <li>• Server 2008</li> </ul>	Yes	No support	Yes	8.0 version 8u261 or later	1.8 <b>Note</b> 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

次に、モデルごとのASAとASDMの互換性の表を示します。次に例を示します。

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	YES
9.20(2)	7.20(2)	YES	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	YES

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

注：

新しいASAバージョンには、調整ASDMバージョン以降が必要です。古いバージョンのASDMを新しいバージョンのASAで使用することはできません。

例 1

ASDM 7.17をASA 9.18と一緒に使用することはできません。ASAの内部では、特に指定がない限り、現在のASDMバージョンを引き続き使用できます。たとえば、ASA 9.22(1.2)をASDM 7.22(1)で使用できます。

例 2

ASAS 9.8(4)32を使用している。ASDMリリースノートに特に記載がない限り、ASDMには下位互換性があるため、ASDM 7.19(1)を使用して管理できます。

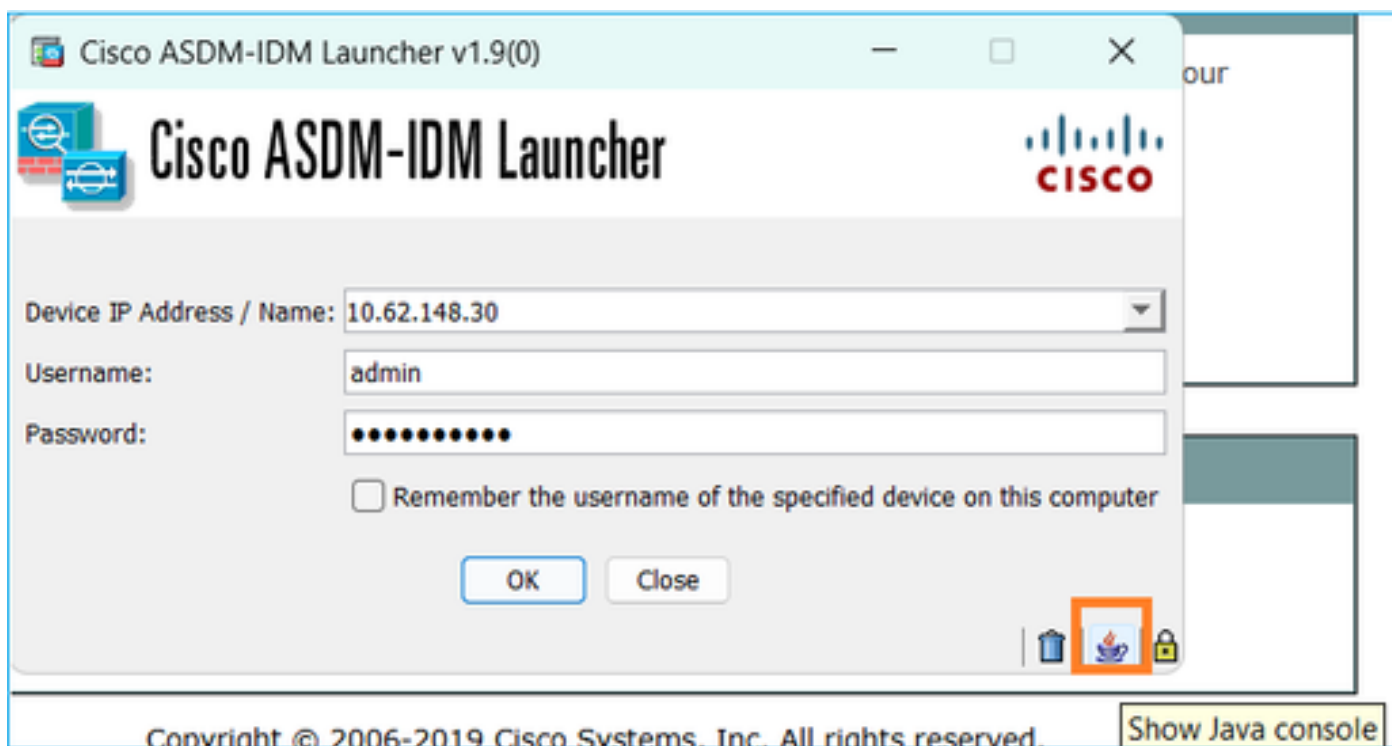
## 参考資料

- [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/asdm/7_22/release/notes/rn722.html#id_25469)
- [https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id\\_65776](https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id_65776)

## 問題 1.互換性のない Java バージョン

トラブルシューティング – 推奨手順

Javaコンソールログを確認します。



次に、JavaとASAの互換性ガイドを確認します。

- [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/asdm/7_22/release/notes/rn722.html#id_25469)
- [https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id\\_65776](https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id_65776)

## 問題 2.ASAとASDMのバージョンに互換性がない

互換性のないバージョンのASAとASDMが実行されると、ASDM UIへのアクセスが失われる可能性があります。

トラブルシューティング – 推奨手順

デバイスのCLIからASDMバージョンをインストールし、TFTP経由でASAのフラッシュにイメージをコピーして、次のガイドで説明するように、コマンド「asdm image」を使用してASDMイメージを設定する必要があります。



<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>

例

```
<#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
```

### 問題3.ASDMとOpenJDKのサポート

Cisco ASDMイメージはOpenJDKを正式にはサポートしていません。したがって、次の2つのオプションを使用できます。

- Oracle JRE : ホストPC上でASDMを起動するためのJava Web Startランタイムが含まれています。この方法を使用するには、64ビットのOracle JREをローカルPCにインストールする必要があります。これはJavaの公式ウェブサイトからダウンロードできます。

- OpenJRE：開いているJREイメージはOracleイメージと同じですが、イメージ自体にASDMを起動するためのJava Web Start機能があるため、ローカルPCに64ビットOracle JREをインストールする必要がない点が異なります。これが、OpenJREイメージのサイズがOracle JREより大きい理由です。OpenJREはASDM openJRE開発サイクルの開始時に利用可能な最新の安定したバージョンでコンパイルされるため、少し古いJavaリリースを使用して表示されることが予想されます。

## Oracle JREとOpenJRE

	Oracle JRE	OpenJREの
エンドホストにJavaをインストールする必要がある	Yes	いいえ（独自のJavaが統合されています）
独自仕様	Yes	いいえ（オープンソース）
Image size	中	Javaも統合されているため大きい
イメージ名	asdm-xxxx.bin（デフォルト）	asdm-openjre-xxxx.bin（xxxxを含む）

### 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

Search...

Expand All Collapse All

Latest Release

- 7.22.1
- 7.20.2
- 7.19.1.95
- 7.18.1.161

All Release

- 7

#### ASA 5508-X with FirePOWER Services

Release 7.22.1 Related Links and Documentation

[My Notifications](#) [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 <a href="#">Advisories</a>	16-Sep-2024	120.79 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin <a href="#">Advisories</a>	16-Sep-2024	195.09 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>

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

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

ヒント：ASDM Launcherのバージョンを変更する場合は、まず既存のASDM Launcherをアンインストールしてから、HTTPS経由でASAに接続して新しいバージョンをインストールします。

参考資料

- [https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_22/release/notes/rn722.html#id\\_25472](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472)
- OpenJDK：完全な開発環境とランタイム環境、オープンソース、GPLライセンス。
- Oracle JRE：ランタイム環境のみ、専用ライセンス。実稼働環境での使用には商用ライセンスが必要です。
- OpenJRE：ランタイム環境のみ、オープンソース、GPLライセンス。
- <https://www.oracle.com/java/technologies/javase/jre8-readme.html>

#### 問題 4.ASDMとJava Azul Zuluの互換性

Oracle JREベースのASDMイメージでは、Java Azul Zuluはサポートされていません。一方、ASDM OpenJREベースのイメージには、Azul Zuluの統合が含まれています。使用可能なオプションについては、「問題3」の推奨事項を確認してください。

#### 問題 5.警告：ファイルdisk0:/asdm-xxx.binにシグニチャが見つかりません

以下に例を挙げます。

```
<#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.
```

#### トラブルシューティング – 推奨手順

これは通常、ASAとASDMの互換性の問題です。ASDM互換性ガイドを調べて、ASDMがASAイメージと互換性があることを確認します。ASAとASDMの互換性マトリクスは次のリンクに掲載されています。

[https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id\\_65776](https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html#id_65776)

問題6. 「% ERROR: ASDM package is not digitally signed.設定を拒否しています。」


新しいASDMイメージを設定するときに、このエラーメッセージを表示するには、`asdm image <image path>` (登録ユーザ専用) コマンドを使用して、アップグレードを実行します。

#### トラブルシューティング – 推奨処置

1. ASAは、ASDMイメージがシスコのデジタル署名付きイメージであるかどうかを検証します。この修正を含むASAバージョンで古いASDMイメージを実行しようとする、ASDMがブロックされ、ASA CLIに「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが表示されます。ASDMリリース7.18(1.152)以降には、この修正が適用されていないバージョンも含め、すべてのASAバージョンとの下位互換性があります。「重要事項」セクション([Cisco ASDM 7.17\(x\)のリリースノート](#))。
2. ホストPCでJavaバージョンを更新します。
3. Secure Firewall 3100で稼働しているASAについては、ソフトウェアのCisco Bug ID [CSCwvc12322](#) 「FPR3100プラットフォームでのデジタル署名付きASDMイメージ検証エラー」

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwvc12322>

---

 注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題7. "%ERROR: Signature not valid for file disk0:/<filename>"

ファイルのコピー中にエラーが表示されます。次に例を示します。

```
<#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.
```

## トラブルシューティング – 推奨処置

ASA 9.14(4.14)以降では、ASDM 7.18(1.152)以降が必要です。ASAは、ASDMイメージがシスコのデジタル署名付きイメージであるかどうかを検証します。この修正を含むASAバージョン 7.18(1.152)よりも古いASDMイメージを実行しようとする、ASDMがブロックされ、ASA

CLIに「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが表示されま  
す。

この変更は、Cisco ASDMおよびASAソフトウェアクライアント側の任意のコード実行の脆弱性  
(CVE ID CVE-2022-20829)が原因で導入されました

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

デバイスがプラットフォームモードで動作している場合は、このドキュメントの手順に従ってイ  
メージをアップロードします。 [https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic\\_zp4\\_dzj\\_cjb](https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_zp4_dzj_cjb)

#### 参考資料

- ASDMリリースノート：  
[https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_14/release/notes/rn714.html#reference\\_yw3](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3)
- ASAアップグレードガイド：  
[https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task\\_E9EE51964590499999B1D976F66E2771](https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task_E9EE51964590499999B1D976F66E2771)

## 問題 8. セキュアファイアウォールポスチャ(Hostscan)の互換性

ホストスキャンのバージョンは、ASAのバージョンよりもAnyConnectのバージョンに依存しま  
す。両方のバージョンは、次のリンクからダウンロードできます。ソフトウェアダウンロード：シ  
スコ：

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

## 問題 9. サポートされる最新バージョン

トラブルシューティング – 推奨処置

ファイアウォールでサポートされている最新のASDMバージョンを知るには、主に次の2つのドク  
ュメントを確認します。

- ASDMリリースノート：  
[https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_14/release/notes/rn714.html#reference\\_yw3](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3)

具体的には、ASAモデルテーブル

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

Ensure your HW model is listed here

2番目のドキュメントはSWダウンロードページです。

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

Select a Product

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

- IOS and NX-OS Software
- Optical Networking
- Routers
- Security**
- Servers - Unified Computing
- Storage Networking
- Switches

- 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

- Firepower 1010 Security Appliance
- Firepower 1120 Security Appliance
- Firepower 1140 Security Appliance
- Firepower 1150 Security Appliance

ハードウェアでサポートされているソフトウェアトレインごとに最新のASDMバージョンを確認できます。次に例を示します。

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

Search...

Expand All Collapse All

- Latest Release
  - 7.22.1**
  - 7.20.2
  - 7.19.1.95
  - 7.18.1.161
- All Release
  - 7
  - 22
  - 20

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 <a href="#">Advisories</a>	16-Sep-2024	120.79 MB	<a href="#">↓</a> <a href="#">🛒</a>
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin <a href="#">Advisories</a>	16-Sep-2024	195.09 MB	<a href="#">↓</a> <a href="#">🛒</a>

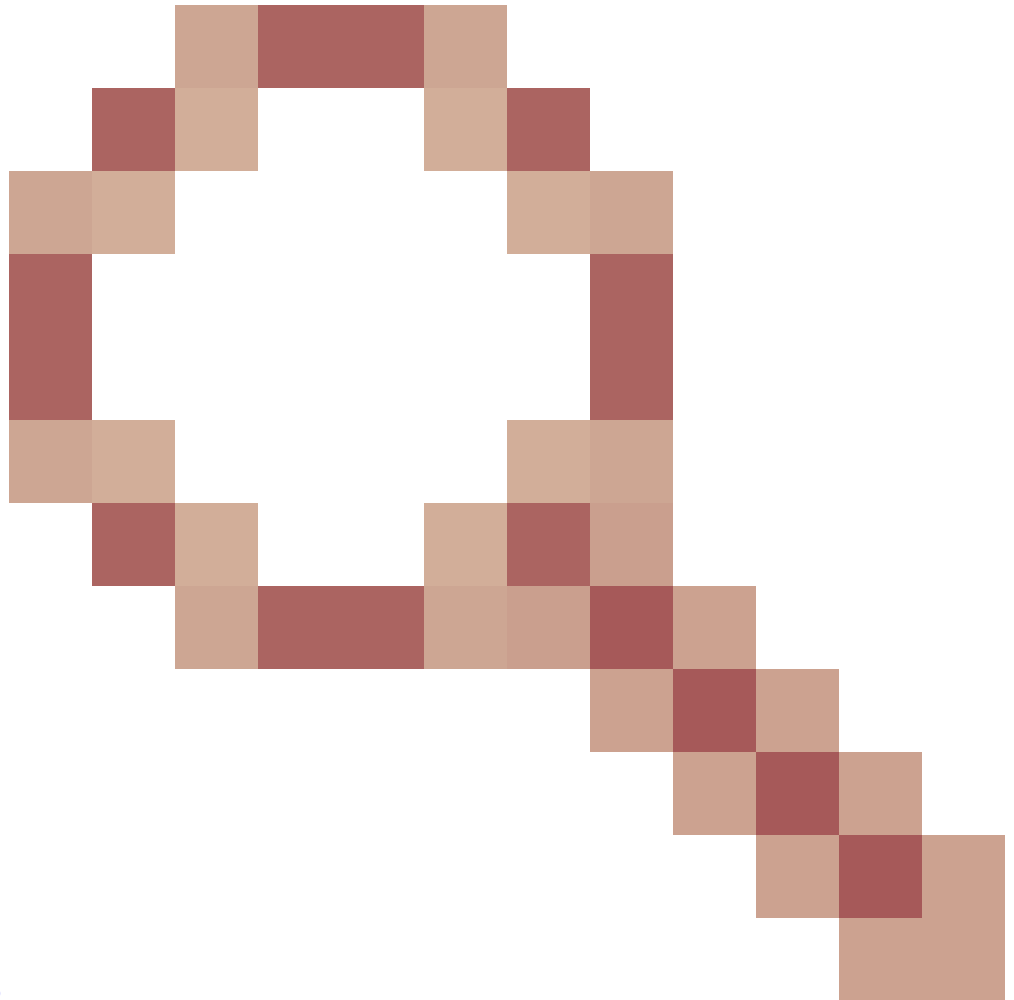
## 問題 10.LinuxでのASDMサポート

トラブルシューティング - 推奨処置

Linuxは公式にはサポートされていません。



関連する機能拡張：



Cisco Bug ID [CSCwk67345](#)

ENH：サポートされるOSのリストにLinuxを含める

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

## 問題 11.ASDMのサポート終了

トラブルシューティング – 推奨処置

ASA/ASDMの『サポート終了および販売終了の通知』を参照してください。

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

## ASDMライセンスの問題

このセクションでは、ASDMライセンスに関連する最も一般的な問題について説明します。

スマートライセンスモデルは、次のユーザによって使用されます。

- Firepower 4100/9300シャーシの登録：ASAのライセンス管理
- ASA、Firepower 1000、Firepower 2100、Firepower 9300、およびFirepower 4100：ライセンス：Smart Software Licensing(ASA、ASA on Firepower)

その他のモデルはすべて、製品認証キー(PAK)ライセンスを使用します

#### 参考資料

- Cisco Secure Firewall ASAシリーズ機能ライセンス – モデルガイドライン

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

#### 問題1: 3DES/AESスマートライセンスが欠落している

管理インターフェイスを使用してASAにアクセスしない限り、ASDMには強力な暗号化ライセンス(3DES/AES)が必要です。データインターフェイスを介したASDMアクセスを有効にするには、3DES/AESライセンスを取得する必要があります。

3DES/AESライセンスをシスコに要求するには、次の手順を実行します。

1. <https://www.cisco.com/go/license>にアクセスします。
2. Continue to Product License Registrationをクリックします。
3. ライセンシングポータルで、テキストフィールドの横にあるGet Other Licensesをクリックします。
4. ドロップダウンリストからIPS, Crypto, Other...を選択します。
5. Search by KeywordフィールドにASAと入力します。
6. ProductリストからCisco ASA 3DES/AES Licenseを選択し、Nextをクリックします。
7. ASAのシリアル番号を入力し、プロンプトに従ってASAの3DES/AESライセンスを要求します。

#### トラブルシューティング – 推奨処置

ライセンスを有効にしてCisco Smart Licensingポータルに登録するには、次の項目が配置されていることを確認します。

- ASAクロックは正しい時刻を示しています。NTPサーバを使用することを推奨します。
- Cisco Smart Licensingポータルへのルーティング
- ファイアウォールからライセンスポータルへのHTTPSトラフィックはブロックされません。ファイアウォール上のキャプチャ収集によってこれを確認できます。
- HTTPプロキシサーバを使用する必要がある場合は、必要なコマンドを含めます。次に例を示します。

```
<#root>
```

```
ciscoasa(config)#
```

```
call-home
```

```
ciscoasa(cfg-call-home)#
```

```
http-proxy 10.1.1.1 port 443
```

## 問題 2.Oracle Java JREのライセンス要件

### トラブルシューティング – 推奨処置

ASDM .binイメージファイルには、次の2つの種類があります。

- Oracle JRE：ホストPC上でASDMを起動するためのJava Web Startランタイムが含まれています。この方法を使用するには、64ビットのOracle JREをローカルPCにインストールする必要があります。これはJavaの公式ウェブサイトからダウンロードできます。
- OpenJRE：開いているJREイメージはOracleイメージと同じですが、イメージ自体にASDMを起動するためのJava Web Start機能があるため、ローカルPCに64ビットOracle JREをインストールする必要がない点が異なります。

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

Search...

Expand All Collapse All

Latest Release

7.22.1

7.20.2

7.19.1.95

7.18.1.161

All Release

7

### ASA 5508-X with FirePOWER Services

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	Download
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	Download

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

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


OracleベースのASDMイメージを使用する場合は、Javaライセンスを個人的な用途以外で使用する必要があります。Oracle Java SEライセンスに関するFAQ:

個人的な用途とは、デスクトップまたはラップトップコンピュータでJavaを使用して、ゲームのプレイや他のパーソナルアプリケーションの実行などを行うことです。業務の一環としてデスクトップまたはラップトップコンピュータでJavaを使用している場合は、個人的な用途ではありません。たとえば、Java生産性アプリケーションを使用して独自の宿題や個人課税を行うことは可能ですが、ビジネス会計を行うことはできません。

Javaライセンスを適用しない場合は、OpenJREベースのASDMイメージを使用できます。

参考資料

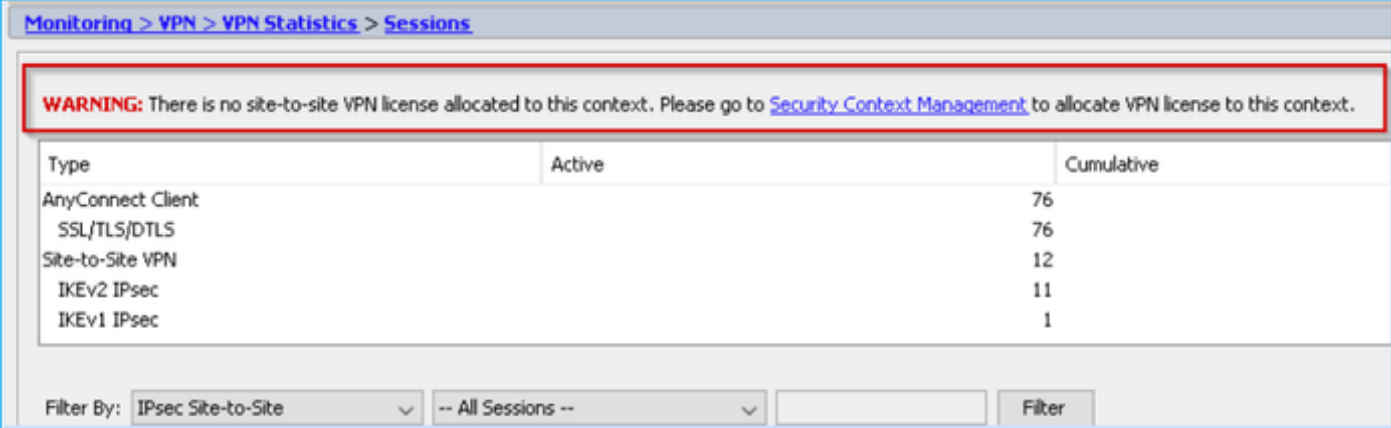
- <https://www.oracle.com/java/technologies/javase/jdk-faqs.html>
- ASDM 7.22用のASDM Javaの要件  
: [https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_22/release/notes/rn722.html#id\\_25472](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472)
- ASDM 7.22のASDM互換性ガイド  
: [https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_22/release/notes/rn722.html#id\\_25476](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476)

 注：使用しているASDMバージョンのリリースノートを確認してください。

### 問題3. マルチコンテキストモードのサイト間VPNライセンスに関するASDMの警告

ASDMでは次の情報が表示されます。

警告：このコンテキストにはサイト間VPNライセンスが割り当てられていません。VPNライセンスをこのコンテキストに割り当てるには、セキュリティコンテキスト管理に移動してください。



The screenshot shows the ASDM interface for monitoring VPN sessions. A red-bordered warning box at the top states: "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." Below the warning is a table with the following data:

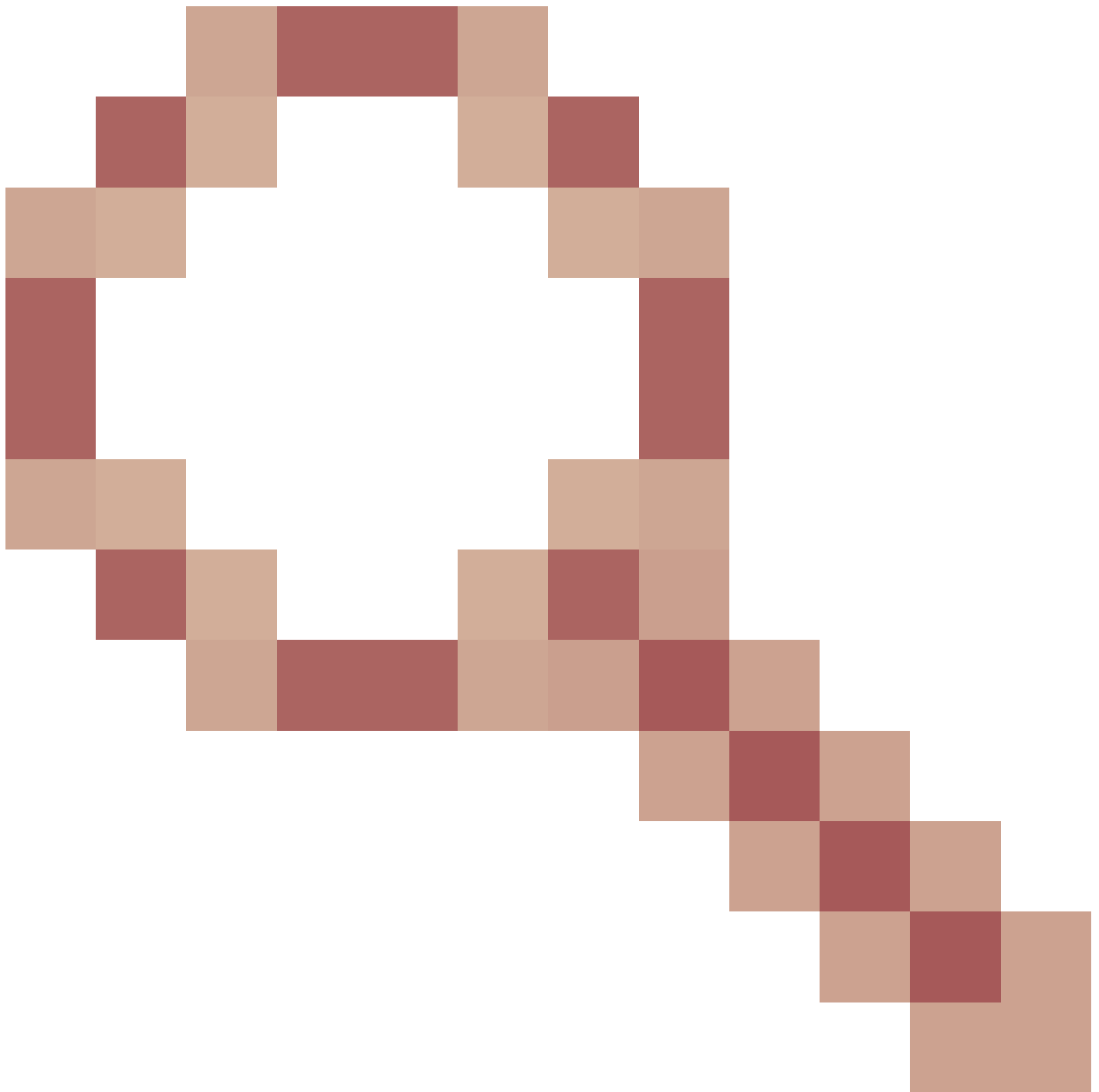
Type	Active	Cumulative
AnyConnect Client		76
SSL/TLS/DTLS		76
Site-to-Site VPN		12
IKEv2 IPsec		11
IKEv1 IPsec		1

At the bottom of the table, there are filter options: "Filter By: IPsec Site-to-Site" (dropdown), "-- All Sessions --" (dropdown), and a "Filter" button.

### トラブルシューティング – 推奨処置

これは、次によって追跡される表面的なソフトウェア不具合です。

Cisco Bug ID [CSCvj66962](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvj66962)



ASDM 7.9(2) ASA 9.6(4)8マルチコンテキストL2L永続的エラー

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

不具合を購読すると、不具合の更新に関する通知を受け取ることができます。

## 参考資料

- [ASDM設定ガイド](#)
- [モデルごとのCisco ASAとASDMの互換性](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。