

# Solucionar Problemas de Licença, Atualização e Compatibilidade do ASDM

## Contents

---

### [Introdução](#)

### [Background](#)

### [Problemas de upgrade do ASDM](#)

[Problema 1. Como fazer o upgrade do ASA/ASDM da versão de origem X para a versão de destino Y?](#)

[Problema 2. Quais são as versões recomendadas para o ASA/ASDM?](#)

[Problema 3. Falha na verificação de atualização do ASA/ASDM no ASDM via Ferramentas > Verificar Atualizações do ASA/ASDM](#)

[Problema 4. Quais versões contêm correções para vulnerabilidades específicas?](#)

[Problema 5. "% ERRO: O pacote ASDM não está assinado digitalmente. Rejeitando a configuração." mensagem de erro](#)

[Problema 6. Não é possível verificar as Atualizações do ASA/ASDM no modo de contexto múltiplo](#)

[Problema 7. "Os Termos Gerais da Cisco não foram aceitos ou rejeitados para continuar o download." mensagem de erro](#)

[Problema 8. Não é possível fazer download de software para hardware específico](#)

[Problema 9. Mensagem de erro "Ocorreu um erro ao executar o código de resposta HTTP de transferência de arquivo -1"](#)

### [Problemas de compatibilidade do ASDM](#)

[Problema 1. Versão Java incompatível](#)

[Problema 2. Versão incompatível do ASA e do ASDM](#)

[Problema 3. Suporte a ASDM e OpenJDK](#)

[Problema 4. Compatibilidade com ASDM e Java Azul Zulu](#)

[Problema 5. AVISO: Assinatura não encontrada no arquivo disk0:/asdm-xxx.bin](#)

[Problema 6. "% ERRO: O pacote ASDM não está assinado digitalmente. Rejeitando a configuração."](#)

[Problema 7. "%ERRO: Assinatura inválida para o arquivo disk0:/ "](#)

[Problema 8. Compatibilidade com Postura de Firewall Segura \(Hostscan\)](#)

[Problema 9. Última versão suportada](#)

[Problema 10. Suporte a ASDM no Linux](#)

[Problema 11. Fim do suporte a ASDM](#)

### [Problemas de licença do ASDM](#)

[Problema 1. A Licença inteligente 3DES/AES está ausente](#)

[Problema 2. Requisitos de Licenciamento do Oracle Java JRE](#)

[Problema 3. Aviso do ASDM sobre Licença de VPN site a site no Modo Multicontexto](#)

### [Referências](#)

---

## Introdução

Este documento descreve o processo de solução de problemas de licença, atualização e compatibilidade do ASDM.

## Background

O documento faz parte da série de solução de problemas do Adaptive Security Appliance Device Manager (ASDM) juntamente com estes documentos:

- [Identificar e Solucionar Problemas de Inicialização do ASDM](#)
- [Solucionar Problemas de Configuração, Autenticação e Outros Problemas do ASDM](#)
- [Solucionar problemas de segurança, certificado e vulnerabilidade do ASDM TLS](#)

## Problemas de upgrade do ASDM

Problema 1. Como fazer o upgrade do ASA/ASDM da versão de origem X para a versão de destino Y?

O usuário precisa de assistência com um upgrade do ASA/ASDM da versão de origem X para a versão de destino Y.

Solução de problemas - Ações recomendadas

1. Certifique-se de que as versões do ASA, ASDM, sistema operacional e Java sejam compatíveis com a versão de destino. Consulte a seção [Notas da versão do Cisco Secure Firewall ASA](#), [Notas da versão do Cisco Secure Firewall ASDM](#), [Compatibilidade com o Cisco Secure Firewall ASA](#).

As versões ASA, ASDM, do sistema operacional e Java devem ser compatíveis, e as versões de destino devem ser suportadas em um hardware específico.

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

2. Para o ASA executado no Firepower 4100/9300, verifique se as versões do Firepower eXtensible Operating System (FXOS) e do software ASA são compatíveis. Consulte [Compatibilidade FXOS do Cisco Firepower 4100/9300](#).

3. Familiarizar-se com as alterações na versão de destino, verificando o [Notas da versão do Cisco Secure Firewall ASA](#), [Notas da versão do Cisco Secure Firewall ASDM](#). No caso de Firepower 4100/9300, também familiarize-se com as alterações no FXOS verificando o [Notas de versão do FXOS](#).

4. Verifique o caminho de atualização nas notas de versão. Neste exemplo, a [Tabela 2 nas notas de versão](#) da versão 7.22 contém o caminho de atualização das versões anteriores para a versão de destino:

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

5. Quando os requisitos de compatibilidade forem atendidos, faça o download das versões ASA/ASDM e FXOS de destino (somente Firepower 4100/9300) na página Download de Software. Certifique-se de selecionar os modelos de hardware específicos conforme mostrado neste exemplo. As versões sugeridas são marcadas com uma estrela dourada:

Select a Product

Product Name e.g. 2911

Browse all

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW)

IOS and NX-OS Software

Optical Networking

Routers

Security

Servers - Unified Computing

Storage Networking

Switches

Unified Communications

Universal Gateways and Access Servers

Video

Wireless

3000 Series Industrial Security Appliances (ISA)

Adaptive Security Appliances (ASA)

Firewall Management

Next-Generation Firewalls (NGFW)

Secure Firewall Migration Tool

ASA 5500-X with FirePOWER Services

Firepower 1000 Series

Firepower 2100 Series

Firepower 4100 Series

Firepower 9300 Series

Secure Firewall 1200 Series

Secure Firewall 3100 Series

Secure Firewall 4200 Series

Secure Firewall Threat Defense Virtual

## Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall 3100 Series / Secure Firewall 3120

Select a Software Type

Adaptive Security Appliance (ASA) Device Manager

Adaptive Security Appliance (ASA) Software

Firepower Coverage and Content Updates

Firepower Threat Defense (FTD) Software

Firewall Migration Tool (FMT)

6. Certifique-se de passar pelo [Capítulo: Planejando sua atualização](#) e o [capítulo: Atualize o ASA](#) no [Guia de atualização do Cisco Secure Firewall ASA](#).

## Referências

- [Notas da versão do Cisco Secure Firewall ASA](#)
- [Notas da versão do Cisco Secure Firewall ASDM](#)
- [Compatibilidade com o Cisco Secure Firewall ASA](#)
- [Compatibilidade com FXOS do Cisco Firepower 4100/9300](#)
- [Guia de atualização do Cisco Secure Firewall ASA](#)

Problema 2. Quais são as versões recomendadas para o ASA/ASDM?

O usuário pergunta sobre as versões recomendadas para ASA/ASDM.

Solução de problemas - Ações recomendadas

O Cisco TAC não fornece recomendações sobre as versões de software. Os usuários podem fazer o download da versão sugerida pela Cisco com base na qualidade, estabilidade e longevidade do software. As versões sugeridas são marcadas com uma estrela dourada como mostrado abaixo:

# Software Download

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

[Expand All](#) [Collapse All](#)

**Suggested Release**  
**9.20.3 Interim**

**Latest Release**  
9.20.3 Interim  
9.22.1  
9.20.3  
9.18.4  
All Release  
Interim  
9

## Secure Firewall 3120

Release 9.20.3 Interim

[My Notifications](#)

**Related Links and Documentation**  
[Release Notes for 9.20.3 Interim](#)

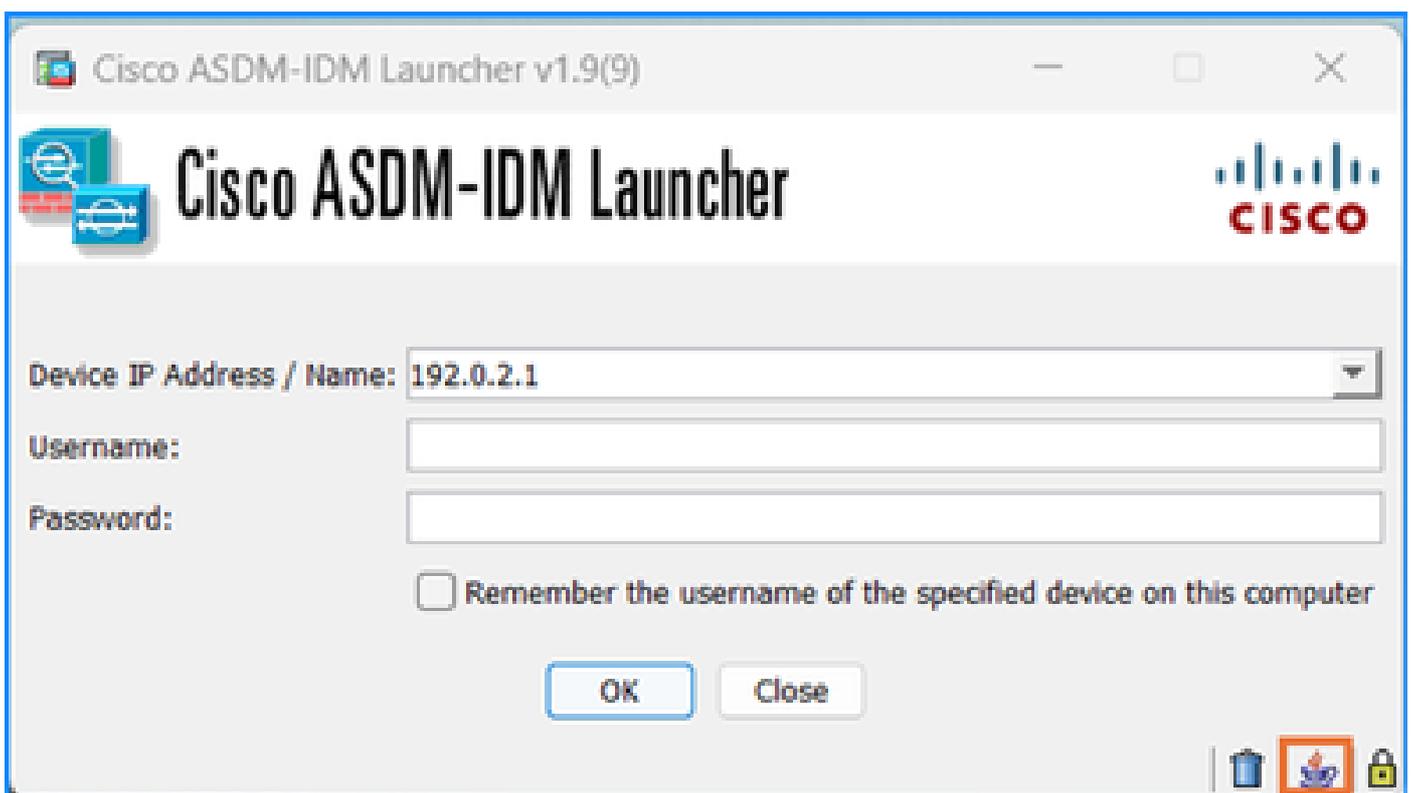
**Interim releases contain bug fixes which address specific issues found since the last Feature or Maintenance release. These images are fully supported by Cisco TAC, and will remain on the download site at least until the next Maintenance release is available.**

File Information	Release Date	Size	
Cisco Adaptive Security Appliance for the Cisco Firepower 3100 Series. cisco-asa-fp3k.9.20.3.7.SPA <a href="#">Advisories</a>	21-Oct-2024	664.32 MB	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Info</a>
Cisco Adaptive Security Appliance for the Cisco Firepower 3100 Series. cisco-asa-fp3k.9.20.3.4.SPA <a href="#">Advisories</a>	26-Sep-2024	664.37 MB	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Info</a>

### Problema 3. Falha na verificação de atualização do ASA/ASDM no ASDM via Ferramentas > Verificar Atualizações do ASA/ASDM

A verificação de atualizações do ASA/ASDM no ASDM via Tools > Check for ASA/ASDM Updates falha. Especificamente, estes sintomas são observados:

1. A janela Digitar Senha de Rede será exibida novamente depois que você clicar no botão Login, mesmo que as credenciais corretas sejam fornecidas.
2. Nos logs do console Java, o erro "Falha na solicitação de metadados" é mostrado:



<#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.
```

## Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID [CSCVf91260](#) "ASDM: A atualização do CCO não está funcionando devido a campos não ignoráveis. "Falha na solicitação de metadados". A solução alternativa é fazer o download de imagens diretamente da página de download e carregá-las no firewall.



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

---

## Problema 4. Quais versões contêm correções para vulnerabilidades específicas?

O usuário pergunta sobre as versões corrigidas de vulnerabilidades específicas.

## Solução de problemas - Ações recomendadas

1. Certifique-se de verificar o aviso de segurança para os produtos afetados.
2. No consultivo de segurança, forneça a versão de hardware e software existente ao verificador de software e clique em Verificar:

## 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.

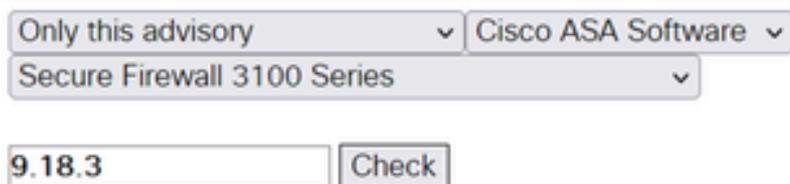
In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical 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. Se a versão fixa estiver disponível, observe as versões na coluna **FIXO PRIMEIRO OU NÃO AFETADO**:

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
<b>COMBINED FIRST FIXED OR NOT AFFECTED</b>			
9.18.3.55,9.18.4			

4. Siga as etapas do "Problema 1. Como fazer o upgrade do ASA/ASDM da versão X de origem para a versão Y de destino?" para atualizar o software.

Problema 5. "% ERRO: O pacote ASDM não está assinado digitalmente. Rejeitando a configuração." mensagem de erro

O "% ERRO: O pacote ASDM não está assinado digitalmente. Rejeitando a configuração." mensagem de erro quando uma nova imagem do ASDM é definida usando o comando `asdm image <image path>`.

Solução de problemas - Ações recomendadas

1. O ASA valida se a imagem do ASDM é uma imagem assinada digitalmente pela Cisco. Se você tentar executar uma imagem ASDM mais antiga com uma versão ASA com essa correção, o ASDM será bloqueado e a mensagem "%ERROR: A assinatura inválida para o arquivo disk0:/<filename>" é exibida na CLI do ASA. O ASDM versão 7.18(1.152) e posterior são retrocompatíveis com todas as versões do ASA, mesmo aquelas sem essa correção. Consulte a seção Notas importantes em [Notas de versão do Cisco ASDM, 7.17\(x\)](#).

2. Para o ASA em execução no Secure Firewall 3100, verifique o bug do software Cisco ID [CSCwc12322](#) "Erro de verificação de imagem ASDM assinada digitalmente nas plataformas FPR3100".

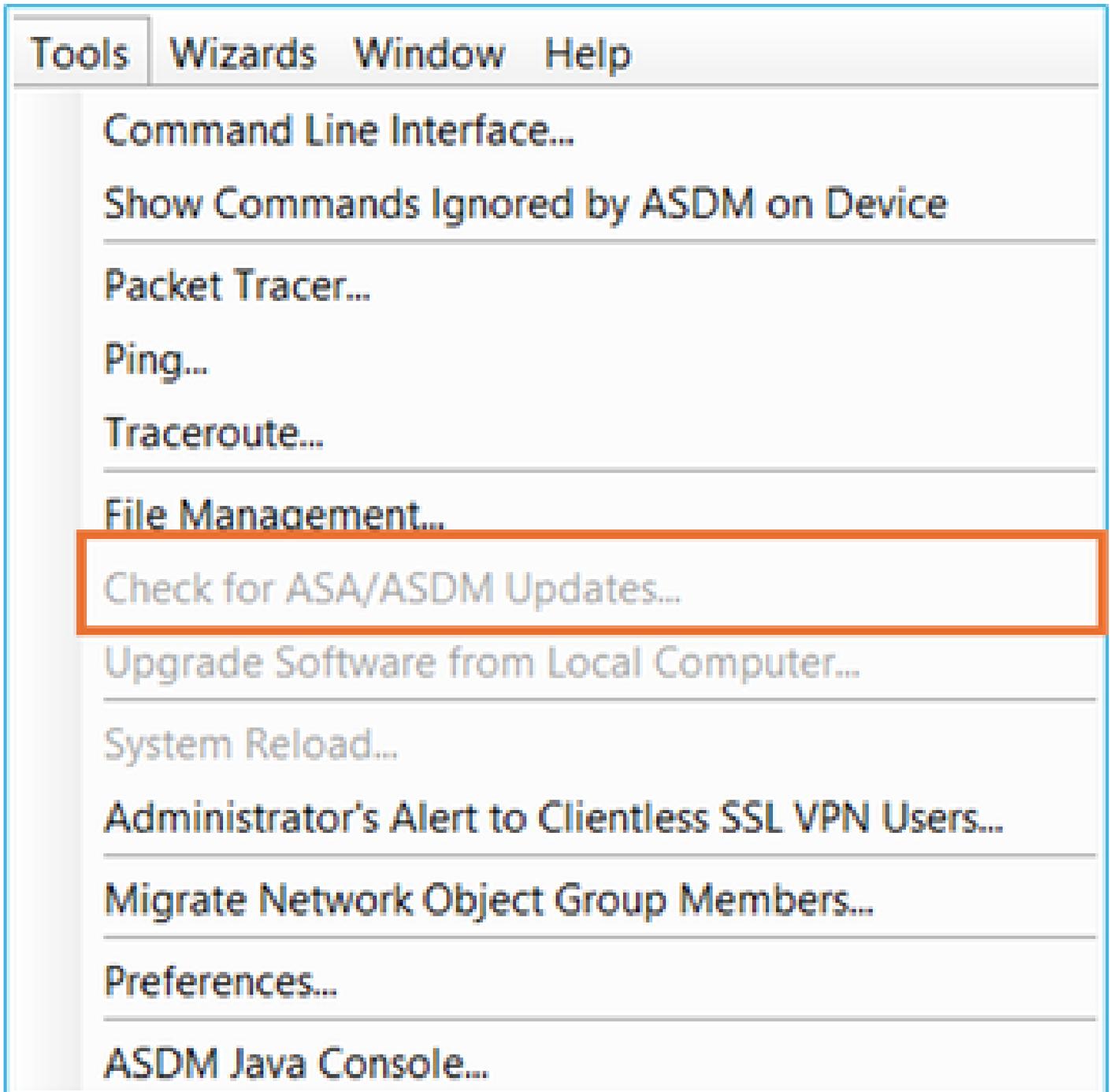
 Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Referências

- [Notas de versão do Cisco ASDM, 7.17\(x\)](#)

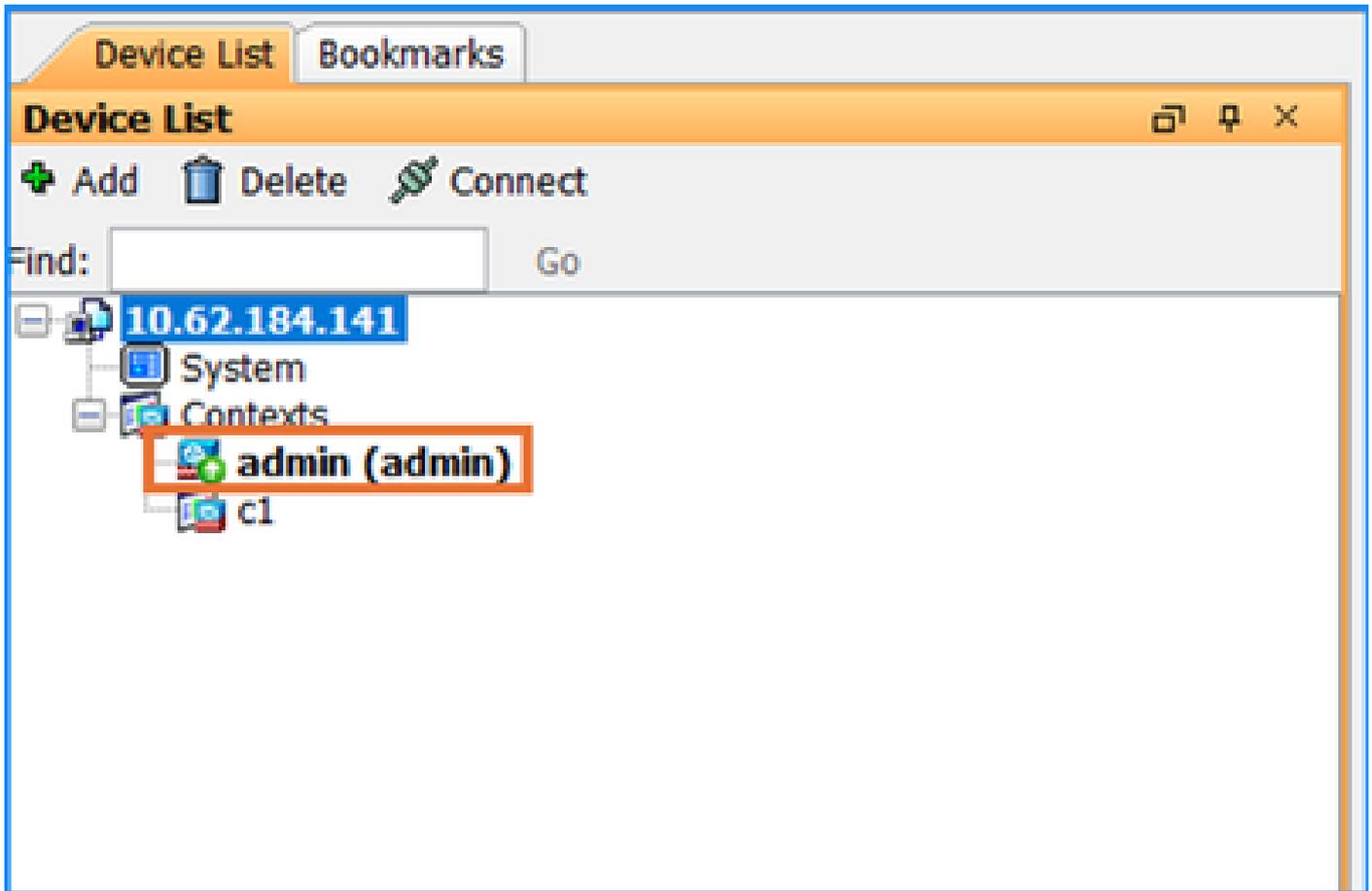
Problema 6. Não é possível verificar as Atualizações do ASA/ASDM no modo de contexto múltiplo

A opção Tools > Check for ASA/ASDM Updates está acinzentada no modo de contexto múltiplo:

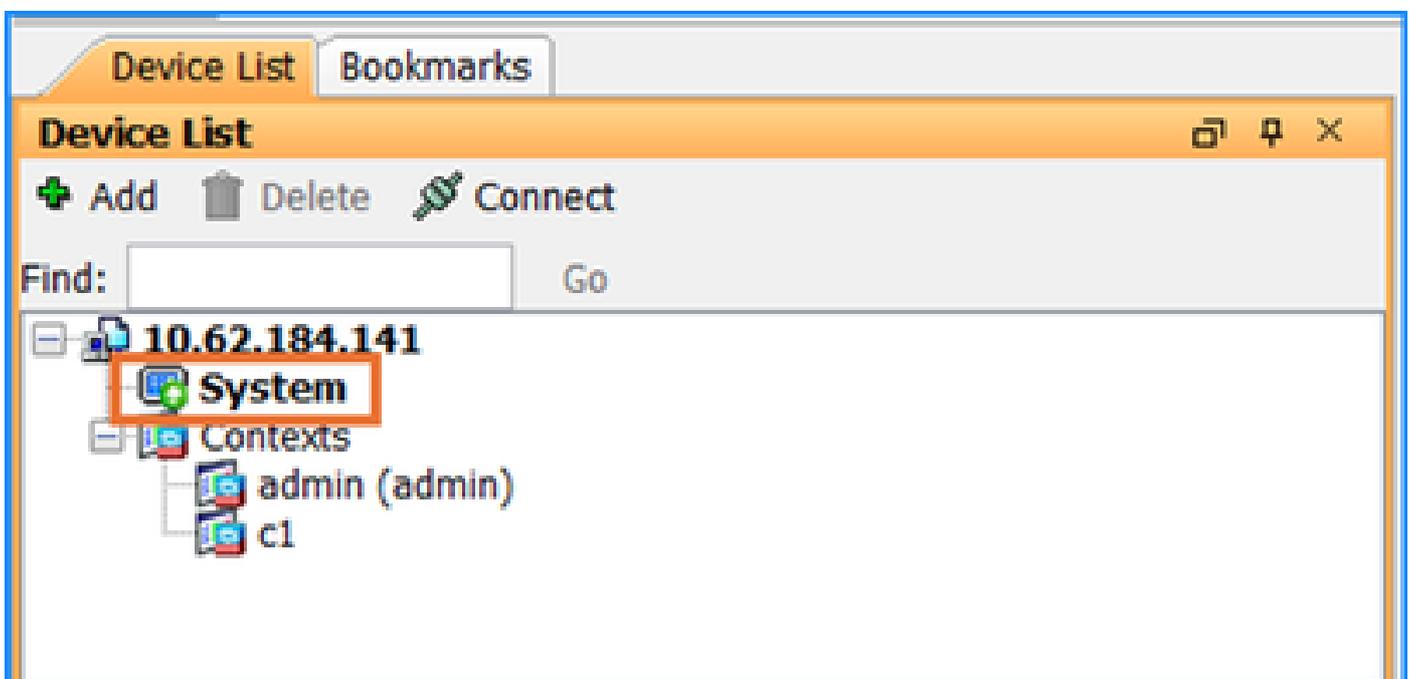


Solução de problemas - Ações recomendadas

Geralmente, essa opção fica acinzentada, pois na guia Device List o contexto de seleção atual é o contexto admin:



Nesse caso, certifique-se de alternar para o contexto do sistema clicando duas vezes no ícone System:



Problema 7. "Os Termos Gerais da Cisco não foram aceitos ou rejeitados para continuar o download." mensagem de erro

O formulário "Termos gerais da Cisco não foram aceitos ou rejeitados para continuar o download." Uma mensagem de erro é mostrada quando o usuário tenta atualizar as imagens do ASA/ASDM através do menu Ferramentas > Verificar Atualizações do ASA/ASDM.

Solução de problemas - Ações recomendadas

Essa mensagem de erro será mostrada se o [contrato de licença de usuário final \(EULA\)](#) não for aceito pelo usuário. Para continuar, certifique-se de aceitar o EULA.

Referências

- [Contrato de licença de usuário final \(EULA\)](#)

**Problema 8. Não é possível fazer download de software para hardware específico**

A página Download de software não mostra algumas versões de software ASA/ASDM para hardware específico.

Solução de problemas - Ações recomendadas

A disponibilidade de software para hardware específico depende principalmente da compatibilidade e dos marcos de EoL (End-of-Life, fim da vida útil). Em caso de incompatibilidade, produtos EoL ou adiamentos de versão, as versões de software geralmente não estão disponíveis para download.

Siga estas etapas para verificar a compatibilidade e as versões suportadas:

1. Verificar a compatibilidade entre as versões de software e hardware. Consulte a [Compatibilidade do Cisco Secure Firewall ASA](#).
  2. Verifique a data de lançamento do fim da manutenção de SW e a última data de suporte nos [avisos de fim da vida útil e fim das vendas](#)
- Data de término das versões de manutenção de SW - A última data em que a Engenharia da Cisco pode lançar qualquer versão final de manutenção de software ou correção de bugs. Após essa data, a Engenharia da Cisco não desenvolve, repara, mantém ou testa mais o software do produto.
  - Última data de suporte - A última data para receber o serviço e o suporte aplicáveis para o produto conforme autorizado pelos contratos de serviço ativos ou pelos termos e condições da garantia. Após essa data, todos os serviços de suporte para o produto estarão indisponíveis e o produto se tornará 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. Verifique as [Notas de Versão do Cisco Secure Firewall ASA](#) e as [Notas de Versão do Cisco Secure Firewall ASDM](#) para obter o adiamento ou a remoção da versão.

### Referências

- [Compatibilidade com o Cisco Secure Firewall ASA](#)
- [Avisos de fim da vida útil e fim das vendas](#)

- [Notas da versão do Cisco Secure Firewall ASA](#)
- [Notas da versão do Cisco Secure Firewall ASDM](#)

## Problema 9. Mensagem de erro "Ocorreu um erro ao executar o código de resposta HTTP de transferência de arquivo -1"

A mensagem de erro "Erro ao executar o código de resposta HTTP de transferência de arquivo -1" é mostrada quando o usuário carrega um arquivo no firewall usando a opção Ferramentas ASDM > Gerenciamento de arquivos.

Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID de software [CSCvf85831](#) "Erro ASDM "Ocorreu um erro ao executar o código de resposta HTTP de transferência de arquivo -1" durante o upload da imagem".

## Problemas de compatibilidade do ASDM

Esta seção aborda os problemas mais comuns relacionados à compatibilidade do ASDM.

Em geral, o ASDM deve ser compatível com estes componentes:

- ASA
- Java
- Sistema operacional (SO)
- Navegador
- módulo SFR (se for usado)

Portanto, antes de instalar ou atualizar o ASDM, é altamente recomendável sempre verificar primeiro esta tabela:

## 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

Em seguida, a tabela Compatibilidade do ASA e do ASDM por Modelo, por exemplo:

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

### Notas:

As novas versões do ASA exigem a versão do ASDM coordenador ou uma versão posterior; você não pode usar uma versão antiga do ASDM com uma nova versão do ASA.

### Exemplo 1

Você não pode usar o ASDM 7.17 com o ASA 9.18. Para os intervalos do ASA, você pode continuar a usar a versão atual do ASDM, a menos que indicado o contrário. Por exemplo, você pode usar o ASA 9.2(1.2) com o ASDM 7.2(1).

### Exemplo 2

Você tem o ASAS 9.8(4)32. Você pode usar o ASDM 7.19(1) para gerenciá-lo, já que o ASDM é compatível com versões anteriores, a menos que seja mencionado de outra forma nas notas de versão do ASDM.

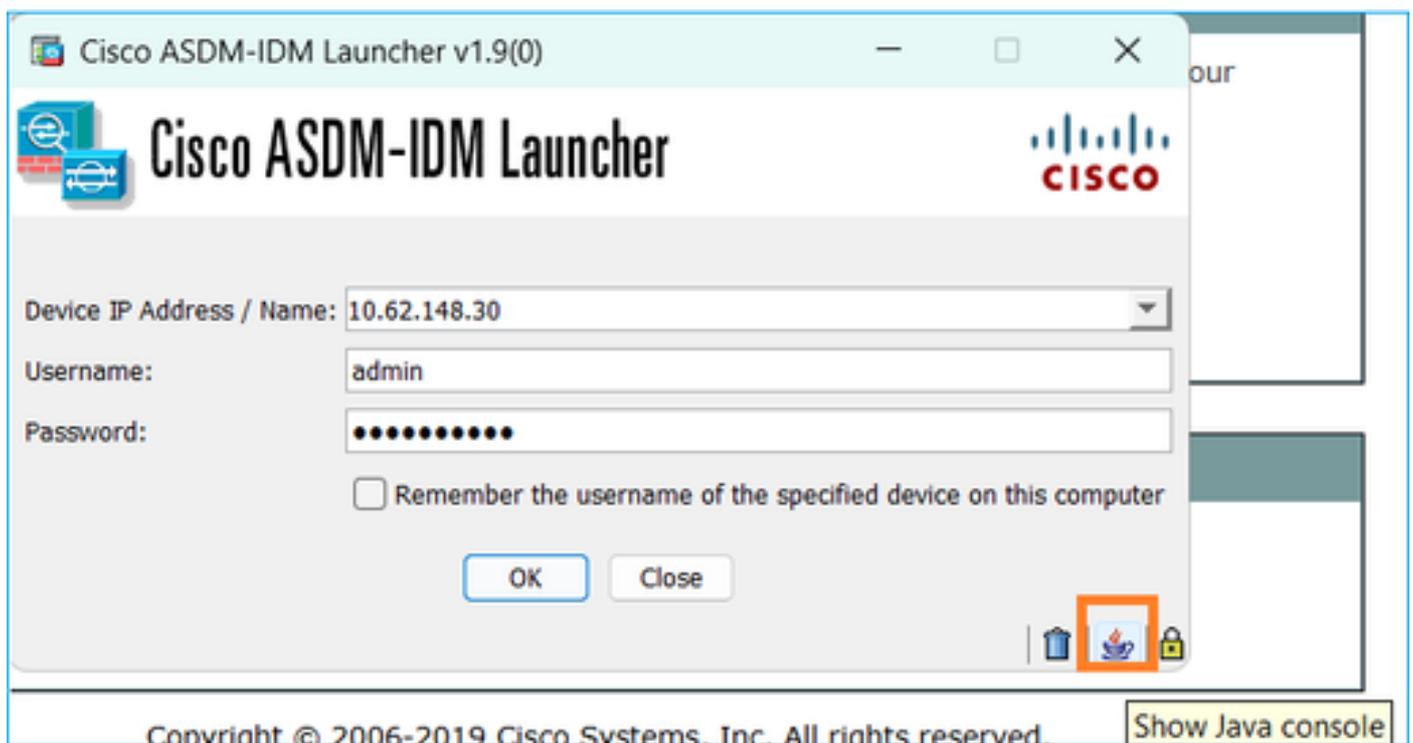
## Referências

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

## Problema 1. Versão Java incompatível

### Solução de problemas - Etapas recomendadas

Verifique os registros do console Java:



Em seguida, verifique os guias de compatibilidade do Java e do 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/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](https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#id_65776)

## Problema 2. Versão incompatível do ASA e do ASDM

Se você encontrar versões incompatíveis do ASA e do ASDM, poderá perder o acesso à interface do usuário do ASDM.

### Solução de problemas - Etapas recomendadas

Você precisa instalar a versão do ASDM a partir da CLI do dispositivo, copiar a imagem na flash do ASA via TFTP e definir a imagem do ASDM usando o comando "asdm image", conforme explicado no guia abaixo:

<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>

## Exemplo

```
<#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. Suporte a ASDM e OpenJDK

A imagem do Cisco ASDM não suporta o OpenJDK oficialmente. Portanto, há duas opções disponíveis:

- Oracle JRE: Contém o tempo de execução do Java Web Start para iniciar o ASDM no PC host. Para usar esse método, você precisa que o Oracle JRE de 64 bits seja instalado no PC local. Você pode fazer o download no site oficial do Java.

- OpenJRE: A imagem aberta do JRE é a mesma do Oracle, mas a diferença é que você não precisa instalar o Oracle JRE de 64 bits no PC local, pois a imagem em si tem o recurso Java Web Start para iniciar o ASDM. Esse é o motivo pelo qual o tamanho da imagem do OpenJRE é maior que o do Oracle JRE. Observe que é esperado ver o OpenJRE usando uma versão Java um pouco mais antiga, pois eles são compilados com a versão estável mais recente disponível no início do ciclo de desenvolvimento do ASDM openJRE.

## Oracle JRE versus OpenJRE

	Oracle JRE	OpenJRE
Exige que o Java esteja instalado no host final	Yes	Não (tem seu próprio Java integrado)
Proprietário	Yes	Não (código aberto)
Tamanho da imagem	Médio	Maior, pois também tem Java integrado
Nome da imagem	asdm-xxxx.bin	asdm-openjre-xxxx.bin

### 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

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
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

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

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

Tip: Se você decidir alterar a versão do iniciador ASDM, primeiro desinstale o iniciador ASDM existente e, em seguida, instale o novo conectando-se ao ASA via HTTPS.

## Referências

- [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: Ambiente completo de desenvolvimento e tempo de execução, código aberto, licença GPL.
- Oracle JRE: Somente ambiente de tempo de execução, licença proprietária, requer uma licença comercial para uso em produção.
- OpenJRE: Somente ambiente de tempo de execução, código aberto, licença GPL.
- <https://www.oracle.com/java/technologies/javase/jre8-readme.html>

#### Problema 4. Compatibilidade com ASDM e Java Azul Zulu

As imagens ASDM baseadas no Oracle JRE não suportam Java Azul Zulu. Por outro lado, as imagens baseadas no ASDM OpenJRE vêm com a integração da Azul Zulu. Verifique as recomendações do 'Problema 3' para obter as opções disponíveis.

#### Problema 5. AVISO: Assinatura não encontrada no arquivo disk0:/asdm-xxx.bin

Exemplo:

```
<#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.
```

#### Solução de problemas - Etapas recomendadas

Este é geralmente um problema de compatibilidade ASA vs ASDM. Verifique o guia de compatibilidade do ASDM e certifique-se de que seu ASDM seja compatível com a imagem do ASA. Você pode encontrar a matriz de compatibilidade do ASA e do ASDM em:

[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)

#### Problema 6. "% ERRO: O pacote ASDM não está assinado digitalmente. Rejeitando a configuração."

Esta mensagem de erro pode ser mostrada quando uma nova imagem do ASDM é definida usando o comando `asdm image <image path> comando`.

## Solução de problemas - Ações recomendadas

1. O ASA valida se a imagem do ASDM é uma imagem assinada digitalmente da Cisco. Se você tentar executar uma imagem ASDM mais antiga com uma versão ASA com essa correção, o ASDM será bloqueado e a mensagem "%ERROR: A assinatura inválida para o arquivo disk0:/<filename>" é exibida na CLI do ASA. O ASDM versão 7.18(1.152) e posterior são retrocompatíveis com todas as versões do ASA, mesmo aquelas sem essa correção. Consulte a seção Observações Importantes em [Notas de versão do Cisco ASDM, 7.17\(x\)](#).
2. Atualize a versão Java no PC host.
3. Para o ASA em execução no Secure Firewall 3100, verifique a ID de bug do software Cisco [CSCwc12322](#) "Erro de verificação de imagem ASDM assinada digitalmente nas plataformas FPR3100"

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

---

 Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

---

## Problema 7. "%ERRO: Assinatura inválida para o arquivo disk0:/<filename>"

O erro é mostrado durante a cópia do arquivo, por exemplo:

```
<#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.
```

## Solução de problemas - Ações recomendadas

O ASA 9.14(4.14) e posterior requer o ASDM 7.18(1.152) ou posterior. O ASA agora valida se a imagem do ASDM é uma imagem assinada digitalmente pela Cisco. Se você tentar executar uma

imagem ASDM mais antiga que a 7.18(1.152) com uma versão ASA com esta correção, o ASDM será bloqueado e a mensagem "%ERROR: A assinatura inválida para o arquivo disk0:/<filename>" é exibida na CLI do ASA.

Essa alteração foi introduzida devido à vulnerabilidade de execução de código arbitrário no cliente do software Cisco ASDM e ASA (ID do CVE CVE-2022-20829)

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

Caso o dispositivo opere no modo de plataforma, siga as instruções deste documento para carregar a imagem: [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)

## Referências

- Notas da versão do ASDM:  
[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)
- Guia de atualização do ASA:  
[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)

## Problema 8. Compatibilidade com Postura de Firewall Segura (Hostscan)

A versão do Hostscan depende mais da versão do AnyConnect do que da versão do ASA. Você pode encontrar ambas as versões aqui: Download de software - Cisco Systems:

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

## Problema 9. Última versão suportada

Solução de problemas - Ações recomendadas

Se você quiser saber a versão mais recente do ASDM com suporte para seu firewall, há principalmente dois documentos a serem verificados:

- Notas da versão do ASDM:  
[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)

Especificamente, a tabela do Modelo ASA

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

O segundo documento é a página de download de SW:

<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

Você pode encontrar as versões mais recentes do ASDM por treinamento de SW suportadas pelo seu HW, por exemplo:

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](#)

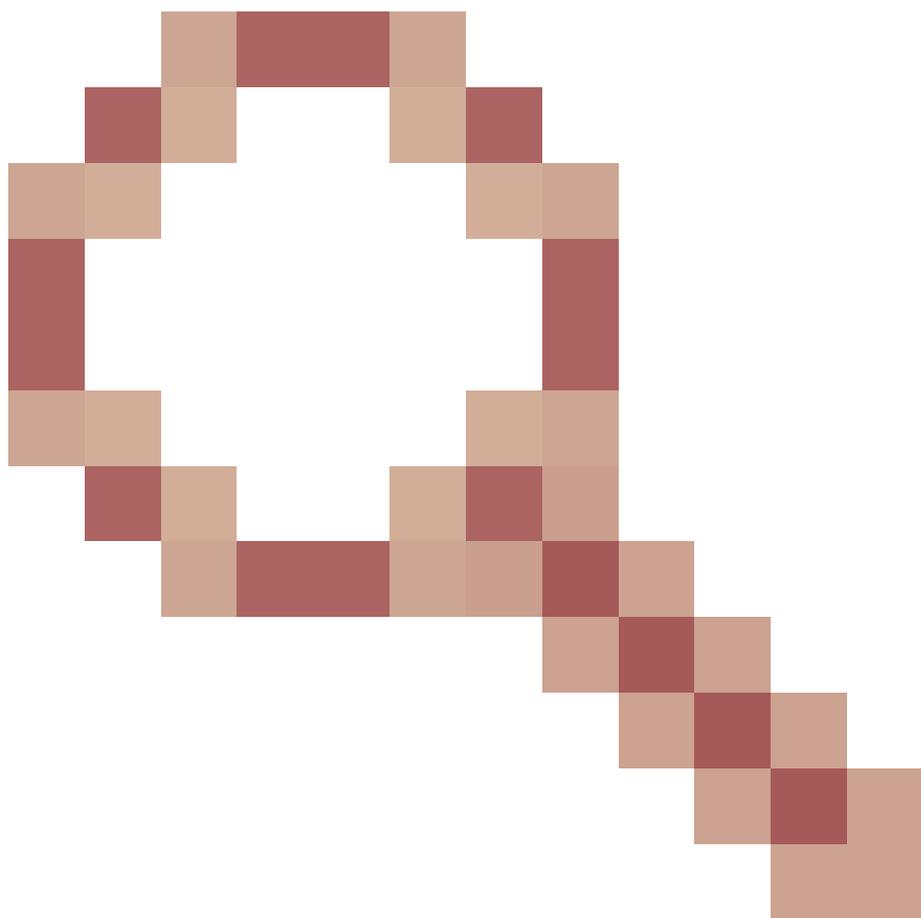
File Information	Release Date	Size	
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 requires Oracle JRE. asdm-7221.bin <a href="#">Advisories</a>	16-Sep-2024	120.79 MB	<a href="#">↓</a> <a href="#">🛒</a>
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin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

## Problema 10. Suporte a ASDM no Linux

Solução de problemas - Ações recomendadas

O Linux não é oficialmente suportado.

Aprimoramento relacionado:



ID de bug da Cisco [CSCwk67345](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwk67345)

ENH: Incluir o Linux na lista de sistemas operacionais suportados

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

Problema 11. Fim do suporte a ASDM

Solução de problemas - Ações recomendadas

Consulte os Avisos de Fim da Vida Útil e Fim das Vendas do ASA/ASDM:

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

## Problemas de licença do ASDM

Esta seção aborda os problemas mais comuns relacionados à licença do ASDM.

O modelo Smart Licensing é usado por:

- Registro do chassi do Firepower 4100/9300: Gerenciamento de licenças para o ASA
- ASAv, Firepower 1000, Firepower 2100, Firepower 9300 e Firepower 4100: Licenças:

Licenciamento de software inteligente (ASAv, ASA no Firepower)

Todos os outros modelos usam o licenciamento da chave de autorização do produto (PAK)

Referências

- Licenças de recursos do Cisco Secure Firewall ASA Series - Diretrizes de modelo

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

## Problema 1. A Licença inteligente 3DES/AES está ausente

O ASDM requer uma licença de criptografia forte (3DES/AES) no ASA, a menos que você a acesse usando a interface de gerenciamento. Para habilitar o acesso ASDM em uma interface de dados, você precisa obter a licença 3DES/AES.

Para solicitar uma licença 3DES/AES da Cisco:

1. Acesse <https://www.cisco.com/go/license>
2. Clique em Continuar para o registro da licença do produto.
3. No Portal de licenciamento, clique em Obter outras licenças ao lado do campo de texto.
4. Escolha IPS, Crypto, Other... na lista suspensa.
5. Digite ASA no campo Pesquisar por palavra-chave.
6. Selecione Cisco ASA 3DES/AES License na lista Product e clique em Next.
7. Digite o número de série do ASA e examine os prompts para solicitar uma licença 3DES/AES para o ASA.

Solução de problemas - Ações recomendadas

Para habilitar a licença e registrar-se no portal Cisco Smart Licensing, certifique-se de que estes itens estejam em vigor:

- O relógio ASA mostra a hora correta. A recomendação é usar um servidor NTP.
- Roteamento para o portal Cisco Smart Licensing.
- O tráfego HTTPS não é bloqueado do firewall para o portal de licenciamento. Uma coleta de captura no firewall pode confirmar isso.
- Se houver necessidade de usar um servidor proxy HTTP, inclua o comando necessário, por exemplo:

```
<#root>
```

```
ciscoasa(config)#
```

```
call-home
```

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

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

## Problema 2. Requisitos de Licenciamento do Oracle Java JRE

### Solução de problemas - Ações recomendadas

O arquivo de imagem .bin do ASDM é fornecido de duas maneiras:

- Oracle JRE: Contém o tempo de execução do Java Web Start para iniciar o ASDM no PC host. Para usar esse método, você precisa que o Oracle JRE de 64 bits seja instalado no PC local. Você pode fazer o download no site oficial do Java.
- OpenJRE: A imagem aberta do JRE é a mesma do Oracle, mas a diferença é que você não precisa instalar o Oracle JRE de 64 bits no PC local, pois a imagem em si tem o recurso Java Web Start para iniciar o ASDM.

**Software Download**

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

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 Buy
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 Buy

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

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

Caso decida usar a imagem ASDM baseada no Oracle, você precisará ter uma licença Java ao usá-la para usos não-pessoais. Perguntas frequentes sobre licenciamento do Oracle Java SE:

O uso pessoal é usar Java em um computador desktop ou laptop para fazer coisas como jogar jogos ou executar outros aplicativos pessoais. Se você estiver usando Java em um computador desktop ou laptop como parte de qualquer operação comercial, isso não será de uso pessoal. Por exemplo, você poderia usar um aplicativo de produtividade Java para fazer seu dever de casa ou seus impostos pessoais, mas não poderia usá-lo para fazer contabilidade comercial.

Se não quiser aplicar nenhuma licença Java, você pode usar a imagem ASDM baseada no OpenJRE.

### Referências

- <https://www.oracle.com/java/technologies/javase/jdk-faqs.html>
- Requisitos Java do ASDM para o ASDM 7.22:  
[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)

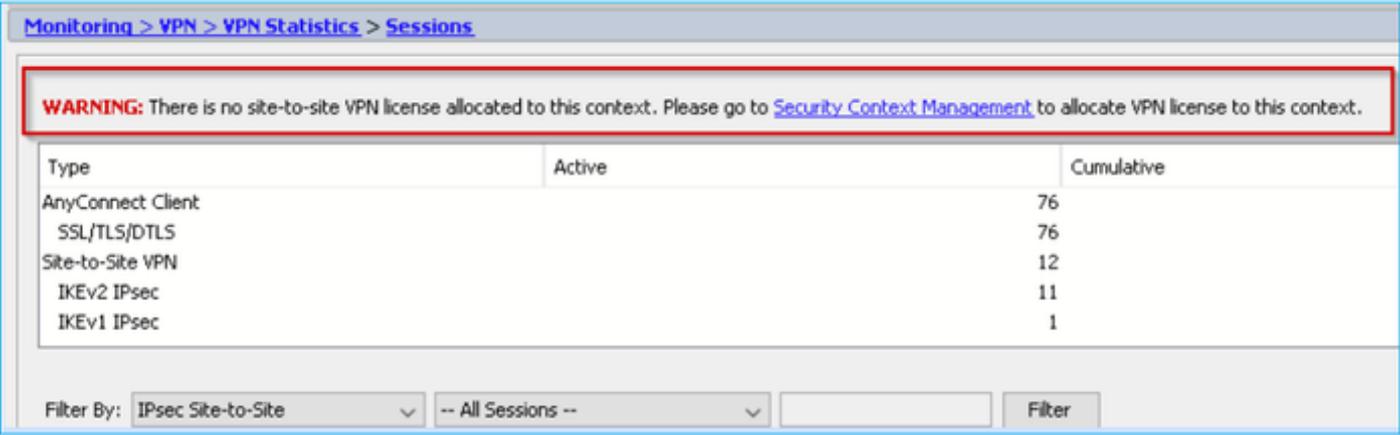
- Notas de Compatibilidade do ASDM para ASDM 7.22:  
[https://www.cisco.com/c/en/us/td/docs/security/asdm/7\\_22/release/notes/rn722.html#id\\_25476](https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476)

 Note: Verifique as notas de versão da versão do ASDM que você usa.

### Problema 3. Aviso do ASDM sobre Licença de VPN site a site no Modo Multicontexto

O ASDM exibe isto:

AVISO: Não há licença de VPN site a site alocada para este contexto. Vá para Gerenciamento de contexto de segurança para alocar a licença de VPN para este contexto.



The screenshot shows the ASDM interface for monitoring VPN sessions. At the top, there is a warning message: "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:

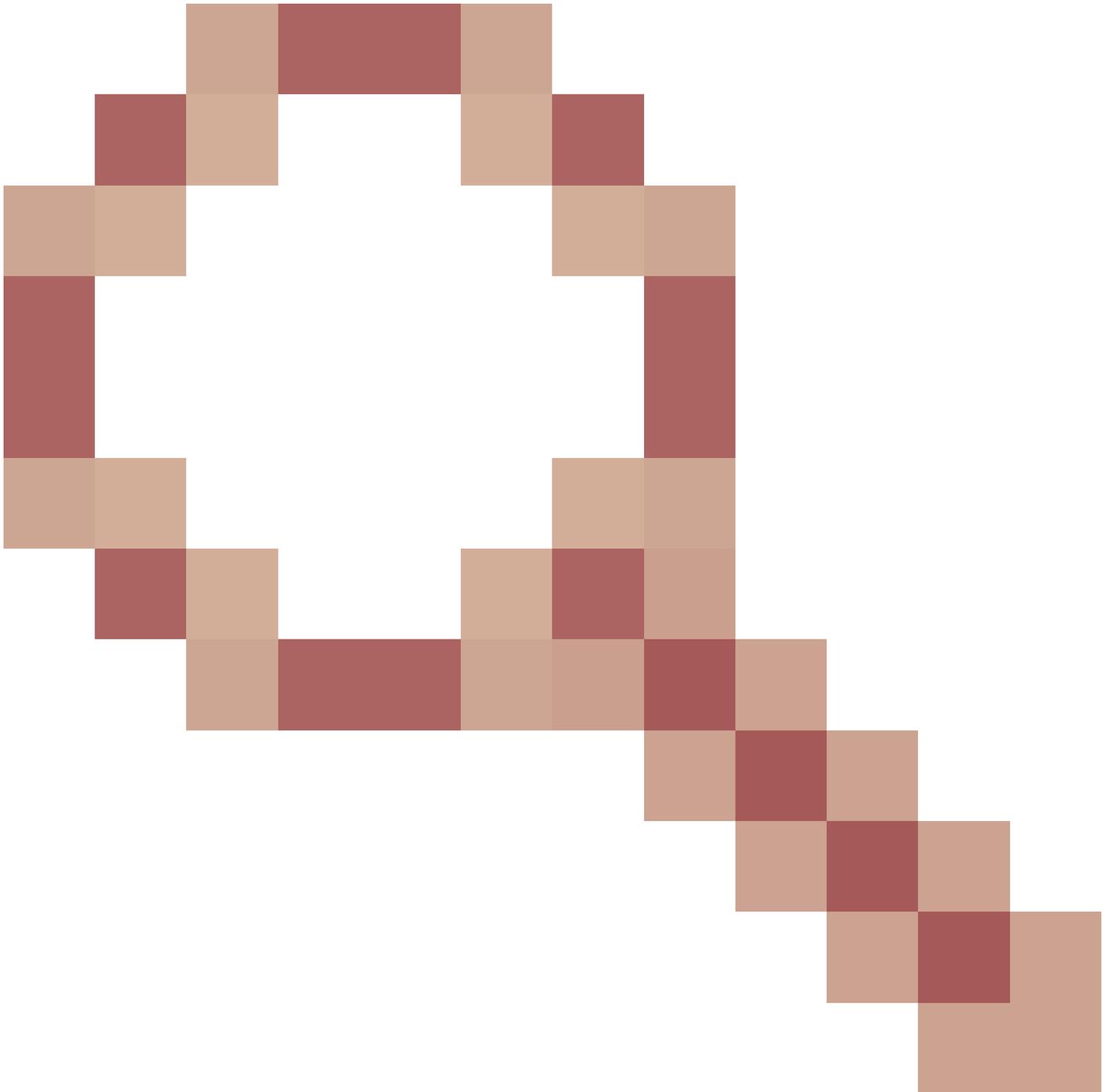
Type	Active	Cumulative
AnyConnect Client		76
SSL/TLS/DTLS		76
Site-to-Site VPN		12
IKEv2 IPsec		11
IKEv1 IPsec		1

At the bottom of the screenshot, there are filter options: "Filter By: IPsec Site-to-Site" and "-- All Sessions --", along with a "Filter" button.

Solução de problemas - Ações recomendadas

Este é um defeito de software cosmético monitorado por:

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



Erro persistente L2L multicontexto do ASDM 7.9(2) ASA 9.6(4)8

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

Você pode se inscrever no defeito para receber uma notificação sobre suas atualizações.

## Referências

- [Guias de configuração do ASDM](#)
- [Compatibilidade do Cisco ASA e ASDM por modelo](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.