

Solución de problemas de licencia, actualización y compatibilidad de ASDM

Contenido

[Introducción](#)

[Background](#)

[Problemas de actualización de ASDM](#)

[Problema 1. ¿Cómo actualizar ASA/ASDM de la versión X de origen a la versión Y de destino?](#)

[Problema 2. ¿Cuáles son las versiones recomendadas para ASA/ASDM?](#)

[Problema 3. Fallo de comprobación de actualización de ASA/ASDM en ASDM a través de Tools > Check for ASA/ASDM Updates](#)

[Problema 4. ¿Qué versiones contienen correcciones para vulnerabilidades específicas?](#)

[Problema 5. "% ERROR: El paquete ASDM no está firmado digitalmente. Rechazando configuración." mensaje de error](#)

[Problema 6. No se pueden comprobar las actualizaciones de ASA/ASDM en el modo de contexto múltiple](#)

[Problema 7. "El formulario de condiciones generales de Cisco no se ha aceptado o rechazado para continuar con la descarga". mensaje de error](#)

[Problema 8. No se puede descargar el software para el hardware específico](#)

[Problema 9. "Error al realizar la transferencia de archivos Código de respuesta HTTP -1" mensaje de error](#)

[Problemas de Compatibilidad con ASDM](#)

[Problema 1. Versión de Java incompatible](#)

[Problema 2. Versión de ASA y ASDM incompatible](#)

[Problema 3. Compatibilidad con ASDM y OpenJDK](#)

[Problema 4. Compatibilidad de ASDM y Java Azul Zulu](#)

[Problema 5. ADVERTENCIA: No se ha encontrado la firma en el archivo disk0:/asdm-xxx.bin](#)

[Problema 6. "% ERROR: El paquete ASDM no está firmado digitalmente. Rechazando configuración."](#)

[Problema 7. "%ERROR: Firma no válida para el disco de archivo0:/"](#)

[Problema 8. Compatibilidad con la condición de firewall seguro \(Hostscan\)](#)

[Problema 9. Última versión compatible](#)

[Problema 10. Soporte de ASDM en Linux](#)

[Problema 11. Fin de soporte de ASDM](#)

[Problemas de licencia de ASDM](#)

[Problema 1. Falta la licencia inteligente 3DES/AES](#)

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

[Problema 3. Advertencia de ASDM sobre licencia VPN de sitio a sitio en modo multicontexto](#)

[Referencias](#)

Introducción

Este documento describe el proceso de solución de problemas de licencia, actualización y compatibilidad de ASDM.

Background

El documento forma parte de la serie de solución de problemas del Administrador de dispositivos de seguridad adaptable (ASDM) junto con estos documentos:

- [Solucionar problemas de inicio de ASDM](#)
- [Resolución de Problemas de Configuración, Autenticación y Otros Problemas de ASDM](#)
- [Resolución de problemas de seguridad, certificados y vulnerabilidad de ASDM TLS](#)

Problemas de actualización de ASDM

Problema 1. ¿Cómo actualizar ASA/ASDM de la versión X de origen a la versión Y de destino?

El usuario necesita ayuda con una actualización de ASA/ASDM de la versión de origen X a la versión de destino Y.

Solución de problemas: acciones recomendadas

1. Asegúrese de que las versiones de ASA, ASDM, sistema operativo y Java sean compatibles con la versión de destino. Consulte la sección [Notas de la versión de Cisco Secure Firewall ASA](#), [Notas de la versión de Cisco Secure Firewall ASDM](#), [Compatibilidad con Cisco Secure Firewall ASA](#).

Las versiones de ASA, ASDM, sistema operativo y Java deben ser compatibles y las versiones de destino deben admitirse en hardware específico.

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

2. Para ASA que se ejecute en Firepower 4100/9300, asegúrese de que el sistema operativo extensible (FXOS) de Firepower y las versiones de software de ASA sean compatibles. Consulte [Compatibilidad con FXOS de Cisco Firepower 4100/9300](#).

3. Asegúrese de familiarizarse con los cambios en la versión de destino comprobando el [Notas de la versión de Cisco Secure Firewall ASA](#), [Notas de la versión de Cisco Secure Firewall ASDM](#). En el caso de Firepower 4100/9300, también familiarizarse con los cambios en FXOS comprobando el [Notas de la versión de FXOS](#).

4. Asegúrese de comprobar la ruta de actualización en las notas de la versión. En este ejemplo, la [Tabla 2 de las notas de la versión](#) para la versión 7.22 contiene la ruta de actualización de las versiones anteriores a la versión 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: → 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 vez cumplidos los requisitos de compatibilidad, descargue las versiones de ASA/ASDM y FXOS de destino (solo Firepower 4100/9300) desde la página de descarga de software. Asegúrese de seleccionar los modelos de hardware específicos como se muestra en este ejemplo. Las versiones sugeridas están marcadas con una estrella dorada:

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. Asegúrese de pasar por el [capítulo: Planificación de la actualización](#) y el [capítulo: Actualice el ASA](#) en la [Guía de actualización de ASA de Cisco Secure Firewall](#).

Referencias

- [Notas de la versión de Cisco Secure Firewall ASA](#)
- [Notas de la versión de Cisco Secure Firewall ASDM](#)
- [Compatibilidad con Cisco Secure Firewall ASA](#)
- [Compatibilidad con Cisco Firepower 4100/9300 FXOS](#)
- [Guía de actualización de Cisco Secure Firewall ASA](#)

Problema 2. ¿Cuáles son las versiones recomendadas para ASA/ASDM?

El usuario pregunta acerca de las versiones recomendadas para ASA/ASDM.

Solución de problemas: acciones recomendadas

El TAC de Cisco no proporciona recomendaciones sobre las versiones de software. Los usuarios pueden descargar la versión sugerida por Cisco en función de la calidad, estabilidad y longevidad del software. Las versiones sugeridas están marcadas con una estrella dorada como se muestra a continuación:

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

Search...

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](#)

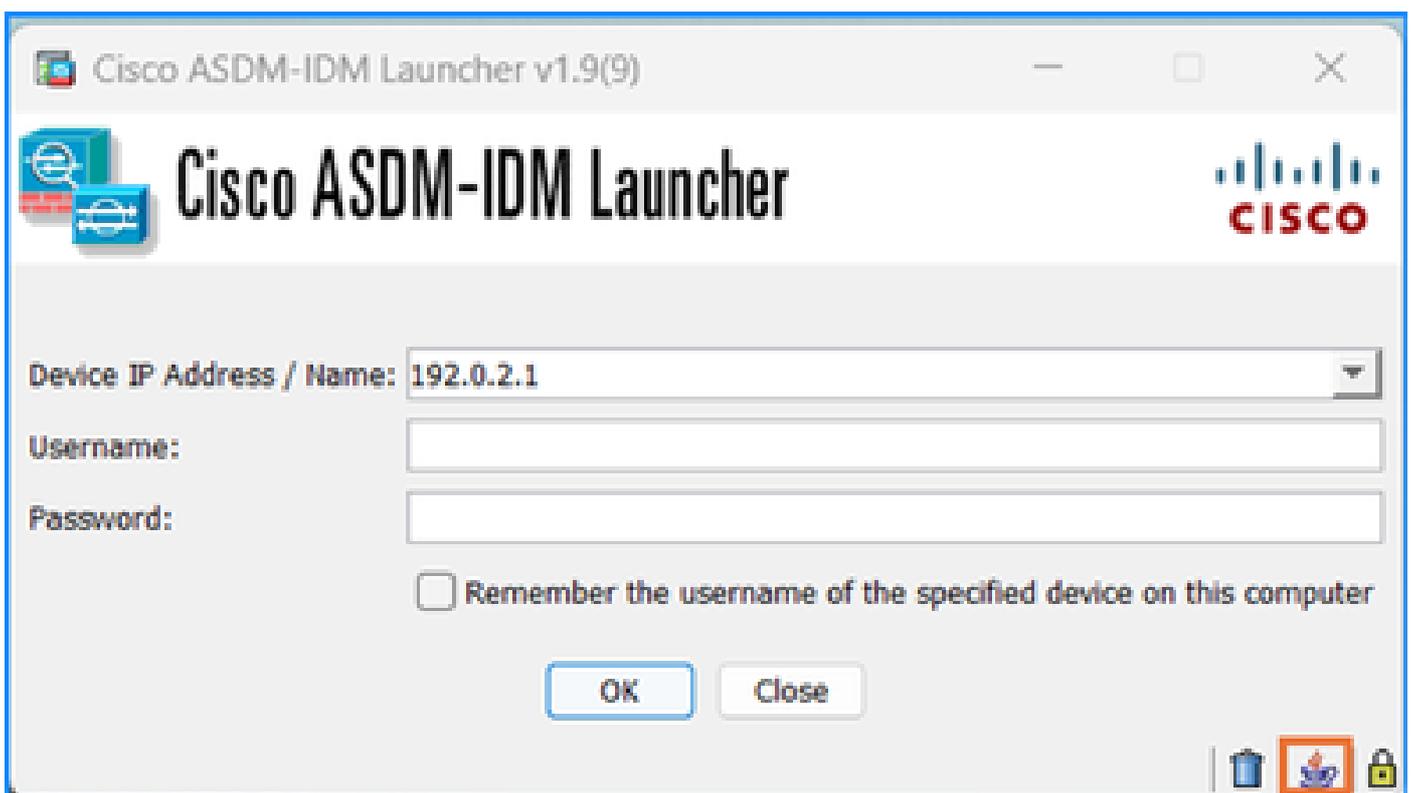
Warning: Interim releases contain bug fixes which address specific issues found since the last Feature or Maintenance release. These images are fully supported by Cisco TAC, and will remain on the download site at least until the next Maintenance release is available.

File Information	Release Date	Size	
Cisco Adaptive Security Appliance for the Cisco Firepower 3100 Series. cisco-asa-fp3k.9.20.3.7.SPA Advisories	21-Oct-2024	664.32 MB	Download Cart Share
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 Cart Share

Problema 3. Fallo de comprobación de actualización de ASA/ASDM en ASDM a través de Tools > Check for ASA/ASDM Updates

La comprobación de las actualizaciones de ASA/ASDM en ASDM vía Tools > Check for ASA/ASDM Updates falla. Específicamente, se observan estos síntomas:

1. La ventana Introducir Contraseña de Red vuelve a aparecer después de hacer clic en el botón Conectar, aunque se hayan proporcionado las credenciales correctas.
2. En los registros de la consola Java, se muestra el error "Error en la solicitud de metadatos":



<#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.
```

Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID [CSCvf91260](#) "ASDM: La actualización de CCO no funciona debido a campos que no se pueden ignorar. "Error en la solicitud de metadatos". La solución alternativa es descargar imágenes directamente desde la página de descarga y cargarlas en el firewall.



Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Problema 4. ¿Qué versiones contienen correcciones para vulnerabilidades específicas?

El usuario pregunta acerca de las versiones fijas de vulnerabilidades específicas.

Solución de problemas: acciones recomendadas

1. Asegúrese de comprobar el aviso de seguridad de los productos afectados.
2. En el aviso de seguridad, proporcione la versión de hardware y software existente al comprobador de software y haga clic en Comprobar:

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.

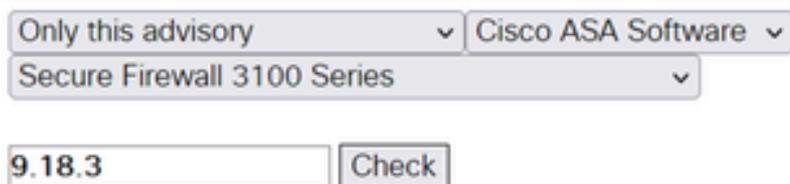
In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical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

3. Si la versión fija está disponible, anote las versiones de la columna FIRST FIXED OR NOT AFFECTED:

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. Siga los pasos del "Problema 1. ¿Cómo actualizar ASA/ASDM de la versión X de origen a la versión Y de destino?" para actualizar el software.

Problema 5. "% ERROR: El paquete ASDM no está firmado digitalmente. Rechazando configuración." mensaje de error

El "% DE ERROR: El paquete ASDM no está firmado digitalmente. Rechazando configuración." mensaje de error cuando se configura una nueva imagen ASDM mediante el comando `asdm image <ruta de la imagen>`.

Solución de problemas: acciones recomendadas

1. ASA valida si la imagen ASDM es una imagen firmada digitalmente por Cisco. Si intenta ejecutar una imagen ASDM anterior con una versión de ASA con esta corrección, ASDM se bloquea y aparece el mensaje "%ERROR: La firma no válida para el archivo disk0:/<filename>" se muestra en la CLI de ASA. ASDM versión 7.18(1.152) y posteriores son compatibles con todas las versiones de ASA, incluso las que no tienen esta corrección. Consulte la sección Notas Importantes en [Release Notes para Cisco ASDM, 7.17\(x\)](#).

2. Para ASA que se ejecuta en Secure Firewall 3100, verifique el software Cisco bug ID [CSCwc12322](#) "Digitally signed ASDM image verification error on FPR3100 platform".

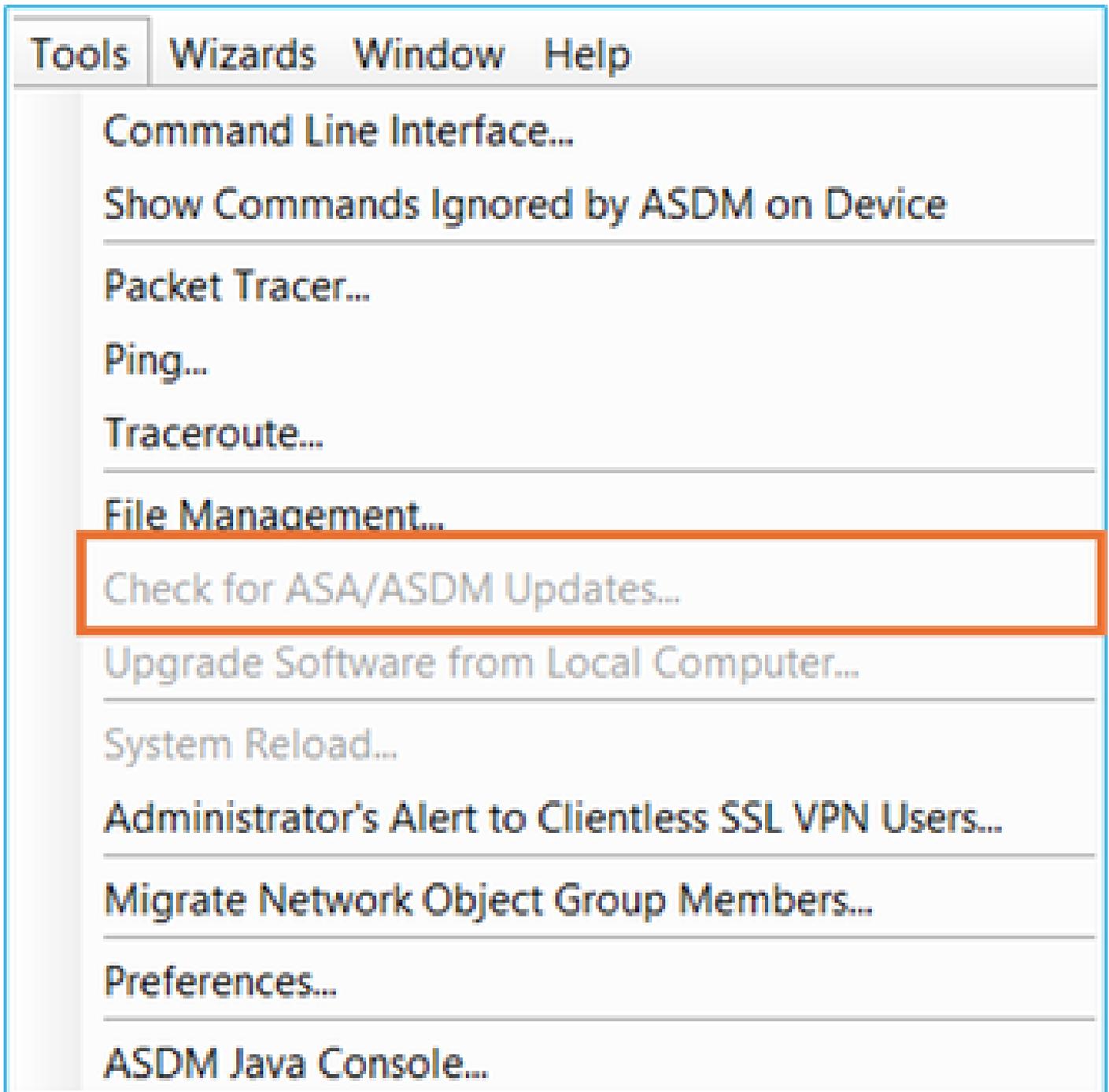
 Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Referencias

- [Notas de la versión de Cisco ASDM, 7.17\(x\)](#)

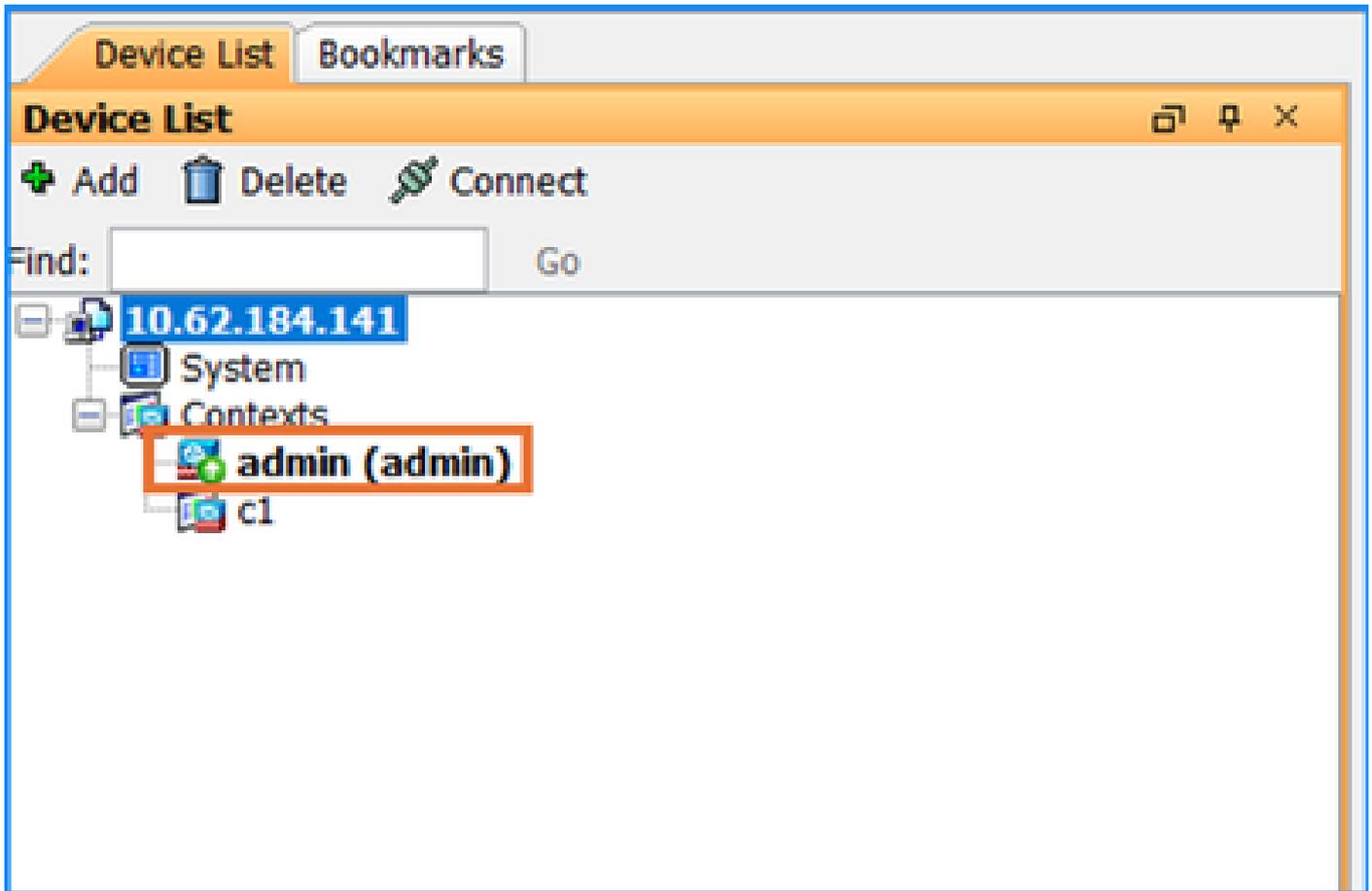
Problema 6. No se pueden comprobar las actualizaciones de ASA/ASDM en el modo de contexto múltiple

La opción Tools > Check for ASA/ASDM Updates aparece atenuada en el modo de contexto múltiple:

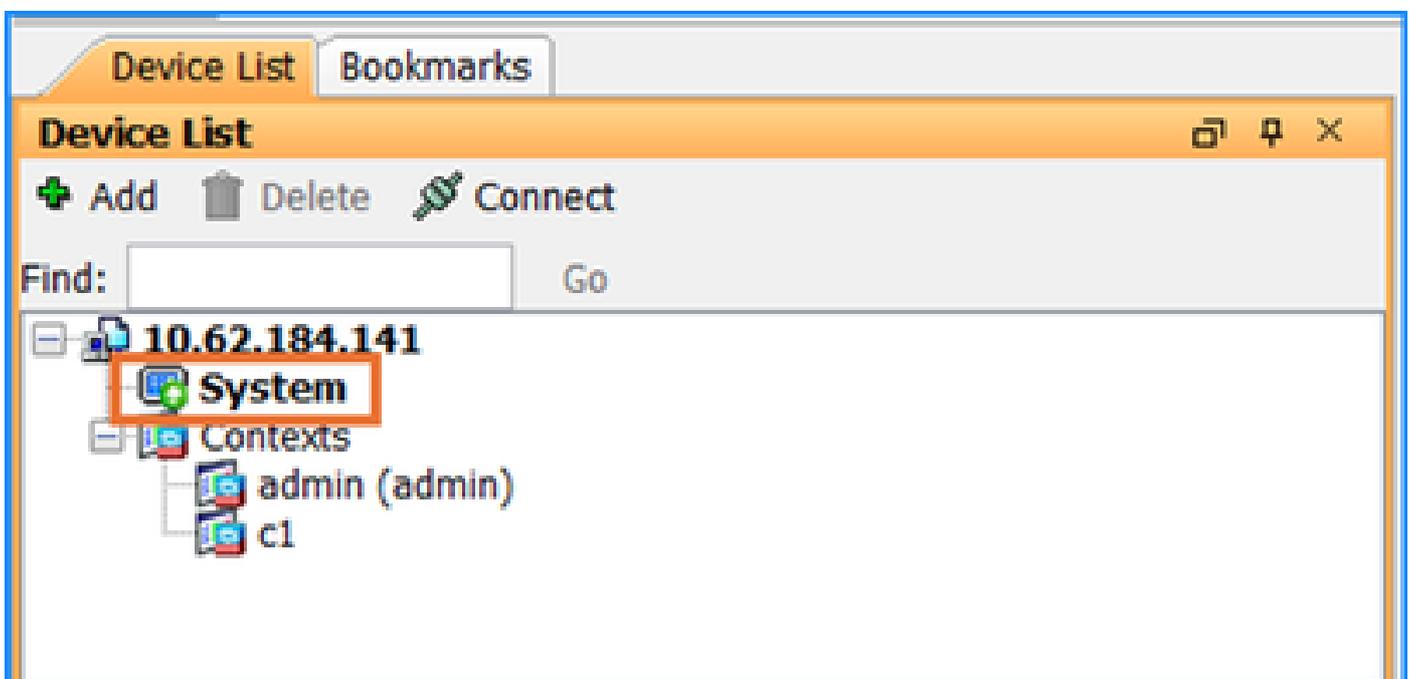


Solución de problemas: acciones recomendadas

Normalmente, esta opción aparece atenuada porque en la pestaña Device List el contexto de selección actual es el contexto admin:



En este caso, asegúrese de cambiar al contexto del sistema haciendo doble clic en el icono System:



Problema 7. "El formulario de condiciones generales de Cisco no se ha aceptado o rechazado para continuar con la descarga". mensaje de error

"El formulario de condiciones generales de Cisco no se ha aceptado o rechazado para continuar con la descarga". Se muestra un mensaje de error cuando el usuario intenta actualizar las imágenes de ASA/ASDM a través del menú Tools > Check for ASA/ASDM Updates.

Solución de problemas: acciones recomendadas

Este mensaje de error aparece si el usuario no acepta el [acuerdo de licencia del usuario final \(CLUF\)](#). Para continuar, asegúrese de aceptar el CLUF.

Referencias

- [Contrato de licencia para el usuario final \(CLUF\)](#)

Problema 8. No se puede descargar el software para el hardware específico

La página de descarga de software no muestra algunas versiones de software de ASA/ASDM para hardware específico.

Solución de problemas: acciones recomendadas

La disponibilidad de software para hardware específico depende principalmente de la compatibilidad y de los hitos de fin de vida útil (EoL). En caso de incompatibilidad, productos EoL o aplazamientos de versiones, las versiones de software no suelen estar disponibles para su descarga.

Asegúrese de seguir estos pasos para verificar la compatibilidad y las versiones compatibles:

1. Compruebe la compatibilidad entre las versiones de software y hardware. Consulte [Compatibilidad con Cisco Secure Firewall ASA](#).
 2. Compruebe la fecha de fin de versiones de mantenimiento de software y la fecha final de soporte técnico en los [avisos de fin de vida útil y fin de venta](#)
- Fecha final para las versiones de mantenimiento de software - La fecha final en la que el Departamento de Ingeniería de Cisco puede publicar versiones finales de mantenimiento de software o correcciones de errores. Después de esta fecha, el departamento de ingeniería de Cisco dejará de desarrollar, reparar, mantener o probar el software del producto.
 - Fecha final de soporte técnico - La fecha final en la que se podrá recibir el servicio y soporte aplicables al producto, según lo estipulado en los contratos de servicio activos o en los términos y condiciones de la garantía. Después de esta fecha, todos los servicios de soporte técnico para el producto no estarán disponibles y el producto pasará a estar 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. Consulte [Notas de la versión de Cisco Secure Firewall ASA](#) y [Notas de la versión de Cisco Secure Firewall ASDM](#) para obtener información sobre el aplazamiento o la eliminación de la versión.

Referencias

- [Compatibilidad con Cisco Secure Firewall ASA](#)

- [Avisos de fin de venta y fin del ciclo de vida](#)
- [Notas de la versión de Cisco Secure Firewall ASA](#)
- [Notas de la versión de Cisco Secure Firewall ASDM](#)

Problema 9. "Error al realizar la transferencia de archivos Código de respuesta HTTP -1" mensaje de error

El mensaje de error "Error al realizar la transferencia de archivos con el código de respuesta HTTP -1" se muestra cuando el usuario carga un archivo en el firewall mediante la opción Herramientas de ASDM > Administración de archivos.

Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID [CSCvf85831](#) "Error ASDM "Error al realizar el código de respuesta HTTP de transferencia de archivos -1" durante la carga de la imagen".

Problemas de Compatibilidad con ASDM

Esta sección cubre los problemas más comunes relacionados con la compatibilidad de ASDM.

En general, ASDM debe ser compatible con estos componentes:

- ASA
- Java
- Sistema operativo (OS)
- Navegador
- Módulo SFR (si se utiliza)

Por lo tanto, antes de instalar o actualizar ASDM, se recomienda verificar siempre primero esta tabla:

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"> • 11 • 10 Note See Windows 10 in ASDM Compatibility Notes if you have problems with the ASDM shortcut. <ul style="list-style-type: none"> • 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

Y luego la tabla Compatibilidad por modelo de ASA y ASDM, por ejemplo:

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

Notas:

Las nuevas versiones de ASA requieren la versión de ASDM de coordinación o una versión posterior; no puede utilizar una versión antigua de ASDM con una nueva versión de ASA.

Ejemplo 1

No puede utilizar ASDM 7.17 con ASA 9.18. Para los intervalos de ASA, puede continuar utilizando la versión actual de ASDM, a menos que se indique lo contrario. Por ejemplo, puede utilizar ASA 9.2(1.2) con ASDM 7.2(1).

Ejemplo 2

Tiene ASDM 9.8(4)32. Puede utilizar ASDM 7.19(1) para gestionarlo, ya que ASDM es compatible con versiones anteriores, a menos que se indique lo contrario en las notas de la versión de ASDM.

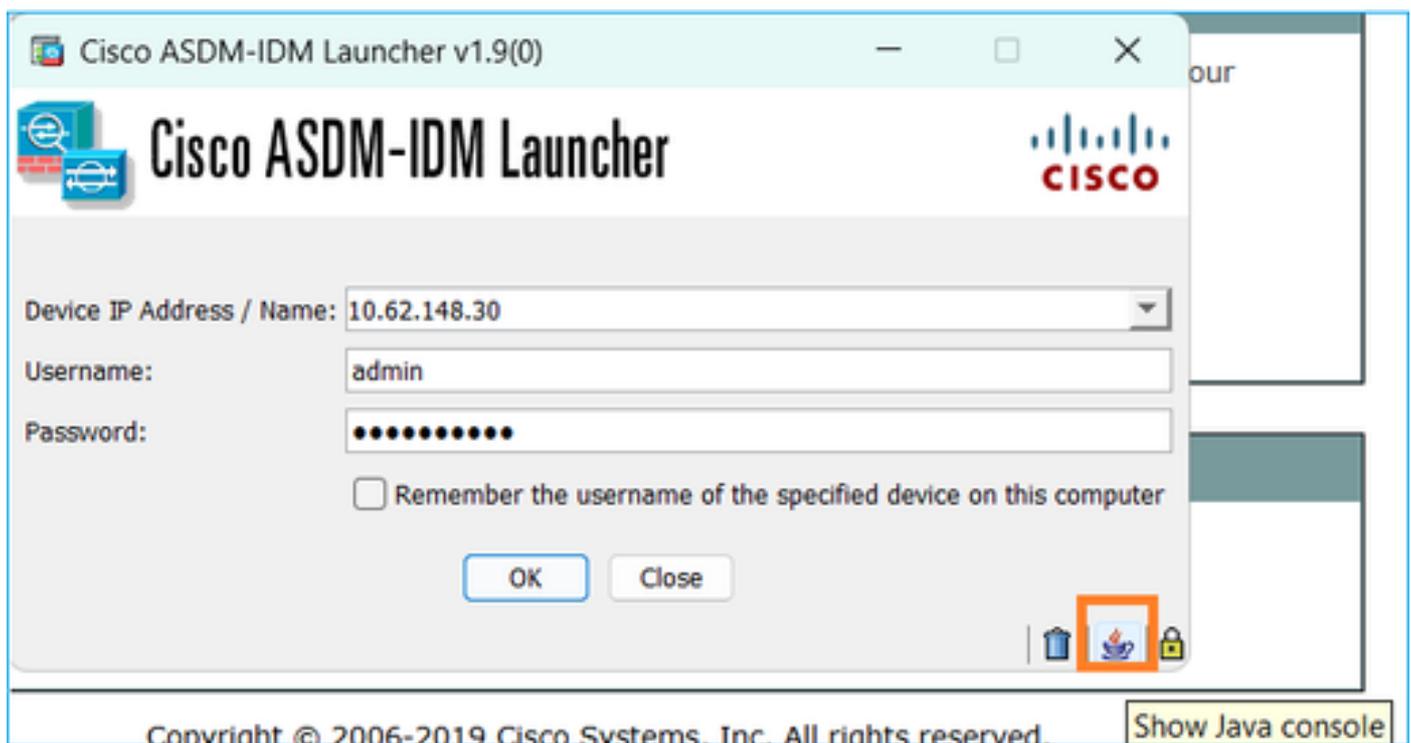
Referencias

- 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

Problema 1. Versión de Java incompatible

Solución de problemas: pasos recomendados

Verifique los registros de la consola Java:



A continuación, consulte las guías de compatibilidad de Java y 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/asamatrix.html#id_65776

Problema 2. Versión de ASA y ASDM incompatible

Si se encuentra con versiones de ASA y ASDM incompatibles, puede perder el acceso a la interfaz de usuario de ASDM.

Solución de problemas: pasos recomendados

Debe instalar la versión de ASDM desde la CLI del dispositivo, copiar la imagen en la memoria flash del ASA a través del TFTP y configurar la imagen ASDM usando el comando "asdm image" como se explica en la guía a continuación:

<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>

Ejemplo:

```
<#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. Compatibilidad con ASDM y OpenJDK

La imagen de Cisco ASDM no admite OpenJDK oficialmente. Por lo tanto, hay 2 opciones disponibles:

- JRE de Oracle: Contiene el tiempo de ejecución de Java Web Start para iniciar ASDM en el equipo host. Para utilizar este método, necesita que Oracle JRE de 64 bits esté instalado en el equipo local. Puede descargarlo en el sitio web oficial de Java.

- OpenJRE: La imagen abierta de JRE es la misma que la de Oracle, pero la diferencia es que no es necesario instalar Oracle JRE de 64 bits en el equipo local, ya que la propia imagen tiene la función Java Web Start para iniciar el ASDM. Esta es la razón por la que el tamaño de la imagen de OpenJRE es mayor que el de Oracle JRE. Tenga en cuenta que se espera ver el OpenJRE utilizando una versión de Java un poco más antigua, ya que se compilan con la última versión estable disponible al principio del ciclo de desarrollo de ASDM openJRE.

Oracle JRE frente a OpenJRE

	Oracle JRE	OpenJRE
Requiere que Java esté instalado en el host final	Yes	No (tiene su propio Java integrado)
Patente	Yes	No (código abierto)
Tamaño de imagen	Medio	Más grande, ya que también tiene Java integrado
Nombre de la imagen	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

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
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin Advisories	16-Sep-2024	195.09 MB

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

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

Consejo: Si decide cambiar la versión del punto de ejecución de ASDM, desinstale primero el punto de ejecución de ASDM existente y, a continuación, instale el nuevo mediante la conexión al ASA a través de HTTPS.

Referencias

- https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472
- OpenJDK: Entorno completo de desarrollo y tiempo de ejecución, código abierto, licencia GPL.
- JRE de Oracle: Sólo el entorno de tiempo de ejecución, licencia propietaria, requiere una licencia comercial para el uso en producción.
- OpenJRE: Solo entorno de tiempo de ejecución, código abierto, licencia GPL.
- <https://www.oracle.com/java/technologies/javase/jre8-readme.html>

Problema 4. Compatibilidad de ASDM y Java Azul Zulu

Las imágenes ASDM basadas en Oracle JRE no admiten Java Azul Zulu. Por otro lado, las imágenes basadas en ASDM OpenJRE vienen con la integración Azul Zulu. Consulte las recomendaciones del 'Problema 3' para ver las opciones disponibles.

Problema 5. ADVERTENCIA: No se ha encontrado la firma en el archivo disk0:/asdm-xxx.bin

Ejemplo:

```
<#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.
```

Solución de problemas: pasos recomendados

Normalmente se trata de un problema de compatibilidad de ASA frente a ASDM. Consulte la guía de compatibilidad de ASDM y asegúrese de que su ASDM sea compatible con la imagen ASA. Puede encontrar la matriz de compatibilidad de ASA y ASDM en:

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

Problema 6. "% ERROR: El paquete ASDM no está firmado digitalmente. Rechazando configuración."

Este mensaje de error se puede mostrar cuando se configura una nueva imagen ASDM mediante el comando `asdm image <image path>` comando.

Solución de problemas: acciones recomendadas

1. ASA valida si la imagen ASDM es una imagen firmada digitalmente por Cisco. Si intenta ejecutar una imagen ASDM anterior con una versión de ASA con esta corrección, ASDM se bloquea y aparece el mensaje "%ERROR: La firma no válida para el archivo disk0:/<filename>" se muestra en la CLI de ASA. ASDM versión 7.18(1.152) y posteriores son compatibles con todas las versiones de ASA, incluso las que no tienen esta corrección. Consulte la sección Notas Importantes en [Notas de la versión de Cisco ASDM, 7.17\(x\)](#).
2. Actualice la versión de Java en el PC host.
3. Para ASA que se ejecuta en Secure Firewall 3100, verifique el ID de bug de Cisco del software [CSCwc12322](#) "Error de verificación de imagen ASDM firmado digitalmente en plataformas FPR3100"

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



Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Problema 7. "%ERROR: La firma no es válida para el archivo disk0:/<filename>"

El error se muestra durante la copia del archivo, por ejemplo:

```
<#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.
```

Solución de problemas: acciones recomendadas

ASA 9.14(4.14) y posterior requiere ASDM 7.18(1.152) o posterior. ASA ahora valida si la imagen ASDM es una imagen firmada digitalmente de Cisco. Si intenta ejecutar una imagen ASDM anterior a la 7.18(1.152) con una versión de ASA con esta corrección, ASDM se bloquea y aparece el mensaje "%ERROR: La firma no válida para el archivo disk0:/<filename>" se muestra en la CLI de ASA.

Este cambio se introdujo debido a la vulnerabilidad de ejecución de código arbitrario en el lado del cliente del software Cisco ASDM y ASA (ID de CVE CVE-2022-20829)

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

En caso de que el dispositivo funcione en el modo de plataforma, siga las instrucciones de este documento para cargar la imagen:

https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_zp4_dzj_cjb

Referencias

- Notas de la versión de ASDM:
https://www.cisco.com/c/en/us/td/docs/security/asdm/7_14/release/notes/rn714.html#reference_yw3
- Guía de actualización de ASA:
https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#task_E9EE51964590499999B1D976F66E2771

Problema 8. Compatibilidad con la condición de firewall seguro (Hostscan)

La versión de Hostscan depende más de la versión de AnyConnect que de la versión de ASA. Puede encontrar las dos versiones aquí: Descarga de software - Cisco Systems:

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

Problema 9. Última versión compatible

Solución de problemas: acciones recomendadas

Si desea conocer la última versión de ASDM soportada para su firewall, hay principalmente dos documentos para verificar:

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

En concreto, la tabla de modelos 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

El segundo documento es la página de descarga 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

Puede encontrar las últimas versiones de ASDM por tren de SW admitidas por su hardware, por ejemplo:

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

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](#)

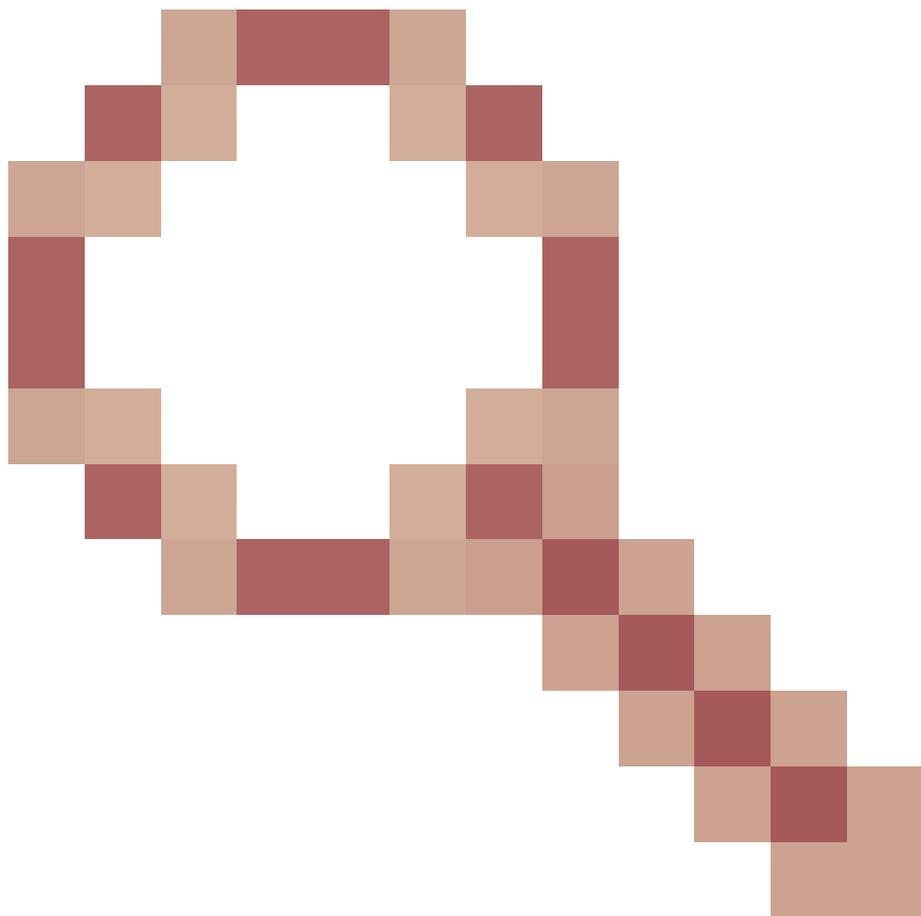
File Information	Release Date	Size	Download
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 requires Oracle JRE. asdm-7221.bin Advisories	16-Sep-2024	120.79 MB	↓
Cisco Adaptive Security Device Manager for ASA 9.8-9.22 integrated with OpenJRE. asdm-openjre-7221.bin Advisories	16-Sep-2024	195.09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

Problema 10. Soporte de ASDM en Linux

Solución de problemas: acciones recomendadas

Linux no es oficialmente compatible.

Mejora relacionada:



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

ENH: Incluir Linux en la lista de sistemas operativos compatibles

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

Problema 11. Fin de soporte de ASDM

Solución de problemas: acciones recomendadas

Consulte los avisos de fin de vida útil y fin de venta de ASA/ASDM:

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

Problemas de licencia de ASDM

Esta sección trata los problemas más comunes relacionados con la licencia de ASDM.

El modelo de licencia inteligente lo utiliza:

- Registro de chasis de Firepower 4100/9300: Gestión de licencias para ASA
- ASAv, Firepower 1000, Firepower 2100, Firepower 9300 y Firepower 4100: Licencias:

Licencia de software inteligente (ASAv, ASA en Firepower)

Todos los demás modelos utilizan licencias de clave de autorización de producto (PAK)

Referencias

- Licencias de funciones de Cisco Secure Firewall ASA Series - Directrices del modelo

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

Problema 1. Falta la licencia inteligente 3DES/AES

ASDM requiere una licencia de cifrado avanzado (3DES/AES) en ASA a menos que acceda a ella mediante la interfaz de gestión. Para habilitar el acceso ASDM sobre una interfaz de datos, necesita obtener la licencia 3DES/AES.

Para solicitar una licencia 3DES/AES de Cisco:

1. Dirijase a <https://www.cisco.com/go/license>
2. Haga clic en Continuar para registrar la licencia del producto.
3. En el portal de licencias, haga clic en Obtener otras licencias junto al campo de texto.
4. Elija IPS, Crypto, Other... en la lista desplegable.
5. Escriba ASA en el campo Buscar por palabra clave.
6. Seleccione Cisco ASA 3DES/AES License en la lista Product y haga clic en Next.
7. Introduzca el número de serie del ASA y consulte las indicaciones para solicitar una licencia 3DES/AES para el ASA.

Solución de problemas: acciones recomendadas

Para habilitar la licencia y registrarse en el portal de Cisco Smart Licensing, asegúrese de que estos elementos estén en su lugar:

- El reloj ASA muestra la hora correcta. Se recomienda utilizar un servidor NTP.
- Routing hacia el portal de Cisco Smart Licensing.
- El tráfico HTTPS no se bloquea desde el firewall al portal de licencias. Una recopilación de capturas en el firewall puede confirmar esto.
- Si necesita utilizar un servidor proxy HTTP, incluya el comando necesario, por ejemplo:

```
<#root>
```

```
ciscoasa(config)#
```

```
call-home
```

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

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

Problema 2. Requisitos de licencia de Oracle Java JRE

Solución de problemas: acciones recomendadas

El archivo de imagen .bin de ASDM se presenta en dos tipos:

- JRE de Oracle: Contiene el tiempo de ejecución de Java Web Start para iniciar ASDM en el equipo host. Para utilizar este método, necesita que Oracle JRE de 64 bits esté instalado en el equipo local. Puede descargarlo en el sitio web oficial de Java.
- OpenJRE: La imagen abierta de JRE es la misma que la de Oracle, pero la diferencia es que no es necesario instalar Oracle JRE de 64 bits en el equipo local, ya que la propia imagen tiene la función Java Web Start para iniciar el 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.

En caso de que decida utilizar la imagen ASDM basada en Oracle, debe disponer de una licencia Java cuando la utilice para usos no personales. Preguntas frecuentes sobre licencias de Oracle Java SE:

El uso personal consiste en utilizar Java en un equipo de escritorio o portátil para realizar tareas como jugar o ejecutar otras aplicaciones personales. Si utiliza Java en un equipo de escritorio o portátil como parte de cualquier operación empresarial, no es un uso personal. Por ejemplo, podría usar una aplicación de productividad Java para hacer sus propios deberes o sus impuestos personales, pero no podría usarla para hacer su contabilidad empresarial.

Si no desea aplicar ninguna licencia de Java, puede utilizar la imagen ASDM basada en OpenJRE.

Referencias

- <https://www.oracle.com/java/technologies/javase/jdk-faqs.html>
- Requisitos de ASDM Java para ASDM 7.2:

https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25472

- Notas de compatibilidad de ASDM para ASDM 7.22:

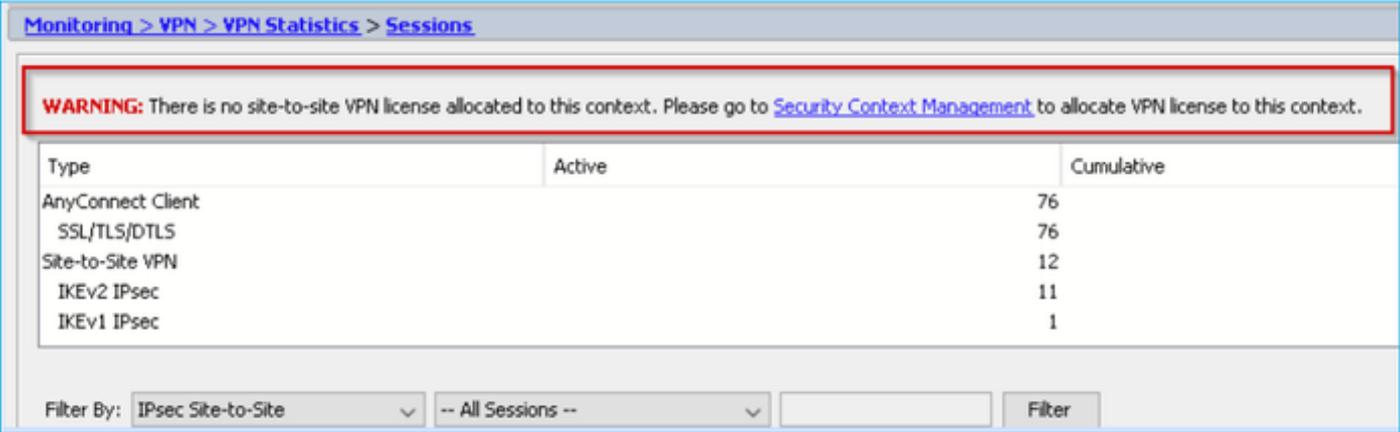
https://www.cisco.com/c/en/us/td/docs/security/asdm/7_22/release/notes/rn722.html#id_25476

 Nota: Verifique las notas de la versión para la versión de ASDM que utiliza.

Problema 3. Advertencia de ASDM sobre licencia VPN de sitio a sitio en modo multicontexto

El ASDM muestra lo siguiente:

ADVERTENCIA: No hay ninguna licencia VPN de sitio a sitio asignada a este contexto. Vaya a Administración del contexto de seguridad para asignar una licencia VPN a este contexto.



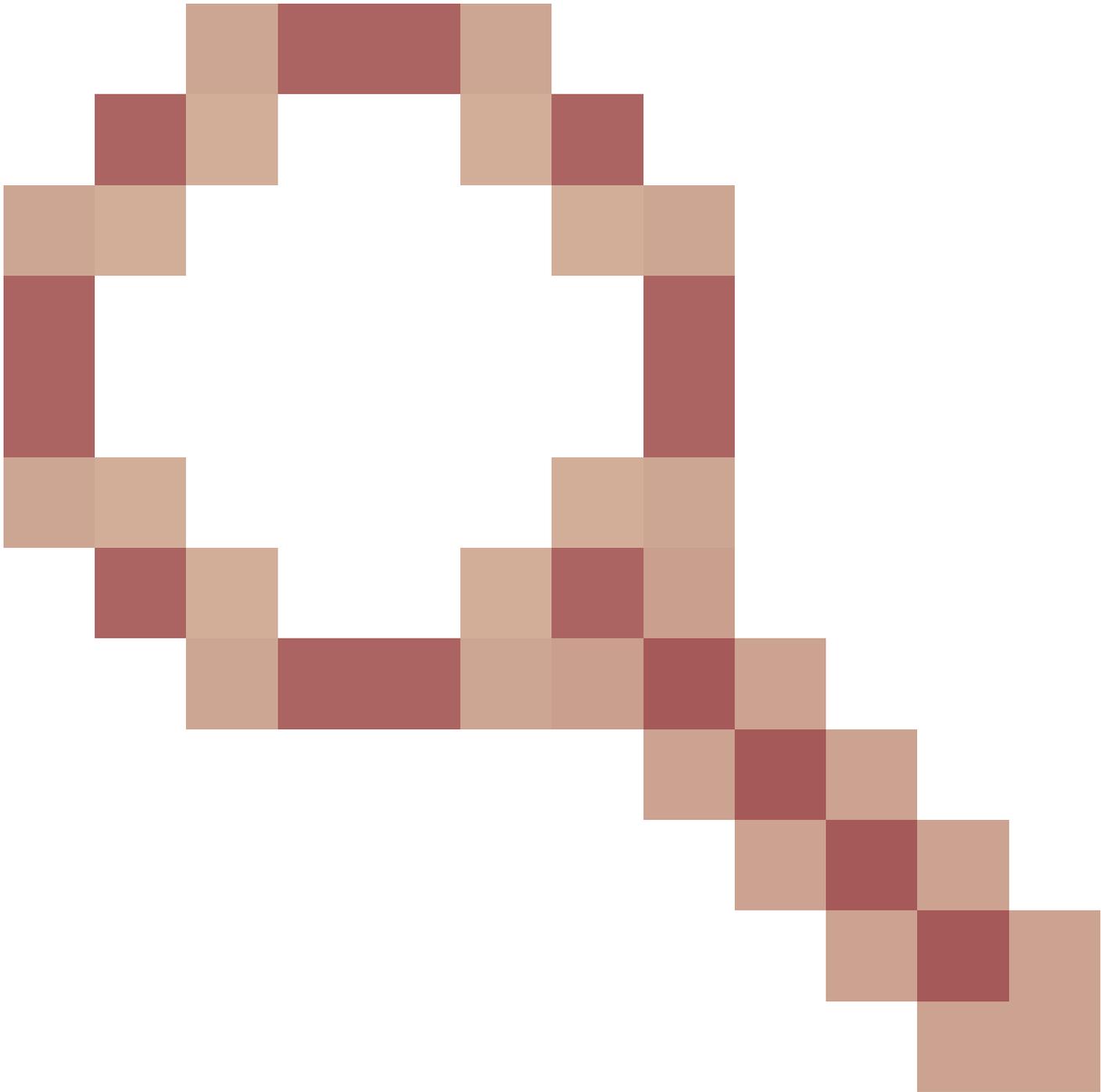
The screenshot shows the ASDM interface for monitoring VPN sessions. At the top, there is a breadcrumb trail: Monitoring > VPN > VPN Statistics > Sessions. A red-bordered warning box contains the following text: "WARNING: There is no site-to-site VPN license allocated to this context. Please go to [Security Context Management](#) to allocate VPN license to this context." Below the warning is a table with three columns: Type, Active, and Cumulative. The table lists various VPN types and their session counts. At the bottom, there are filter options: "Filter By: IPsec Site-to-Site" and "-- All Sessions --", along with a "Filter" button.

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

Solución de problemas: acciones recomendadas

Este es un defecto de software cosmético rastreado por:

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



Error persistente de L2L multicontexto ASDM 7.9(2) ASA 9.6(4)8

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

Puede suscribirse al defecto para recibir una notificación sobre las actualizaciones de defectos.

Referencias

- [Guías de Configuración de ASDM](#)
- [Compatibilidad de Cisco ASA y ASDM por modelo](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).