Resolución de Problemas de Configuración, Autenticación y Otros Problemas de ASDM

Contenido

Introducción

Este documento describe el proceso de solución de problemas para la configuración, autenticación y otros problemas del Adaptive Security Appliance Device Manager (ASDM).

Background

El documento es parte de la serie de solución de problemas de ASDM junto con estos documentos:

Vínculo1<>

Vínculo2<>

Vínculo3<>

Resolución de Problemas de Configuración de ASDM

Problema 1. ASDM no muestra ninguna lista de control de acceso (ACL) aplicada a una interfaz

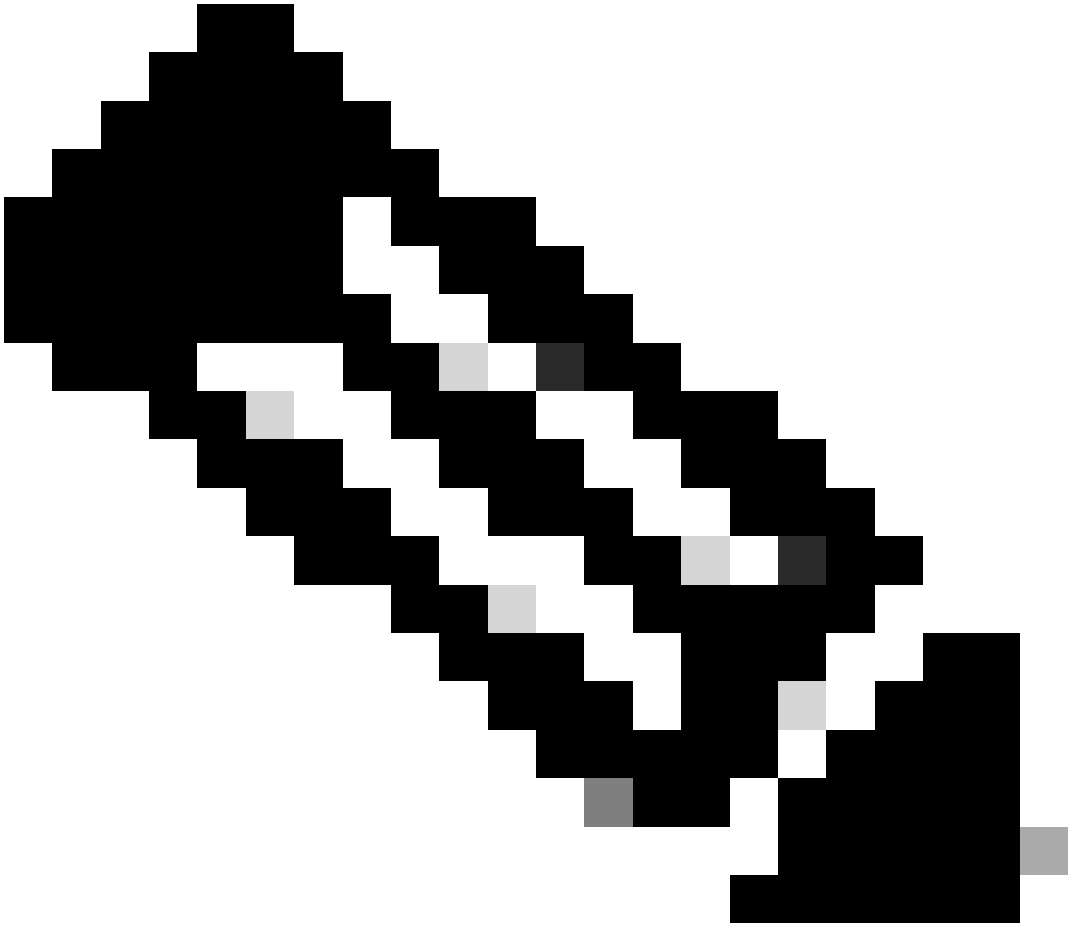
ASDM no muestra ninguna lista de control de acceso (ACL) aplicada a una interfaz, aunque haya un grupo de acceso válido aplicado a la interfaz en cuestión. El mensaje en su lugar dice "0 incoming rules". Estos síntomas se observan en ACL L3 y L2 configuradas en la configuración del grupo de acceso para una interfaz:

<#root>

```
firewall(config)#
access-list 1 extended permit ip any

firewall(config)#
any access-list 2 extended permit udp any any

firewall(config)#
access-list 3 ethertype permit dsap bpdu


firewall(config)#
access-group 3 in interface inside

firewall(config)#
access-group 1 in interface inside

firewall(config)#
access-group 2 in interface outside
```

Solución de problemas: acciones recomendadas

Consulte el ID de bug del software Cisco CSCwj14147 "ASDM no puede cargar la configuración del grupo de acceso si las ACL L2 y L3 están mezcladas.".



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

Problema 2. Incoherencia del recuento de visitas entre la CLI de ASA y la interfaz de usuario de ASDM

Las entradas de conteo de aciertos en el ASDM no son consistentes con los conteos de aciertos de la lista de acceso según lo informado por el comando show access-list en la salida del firewall.

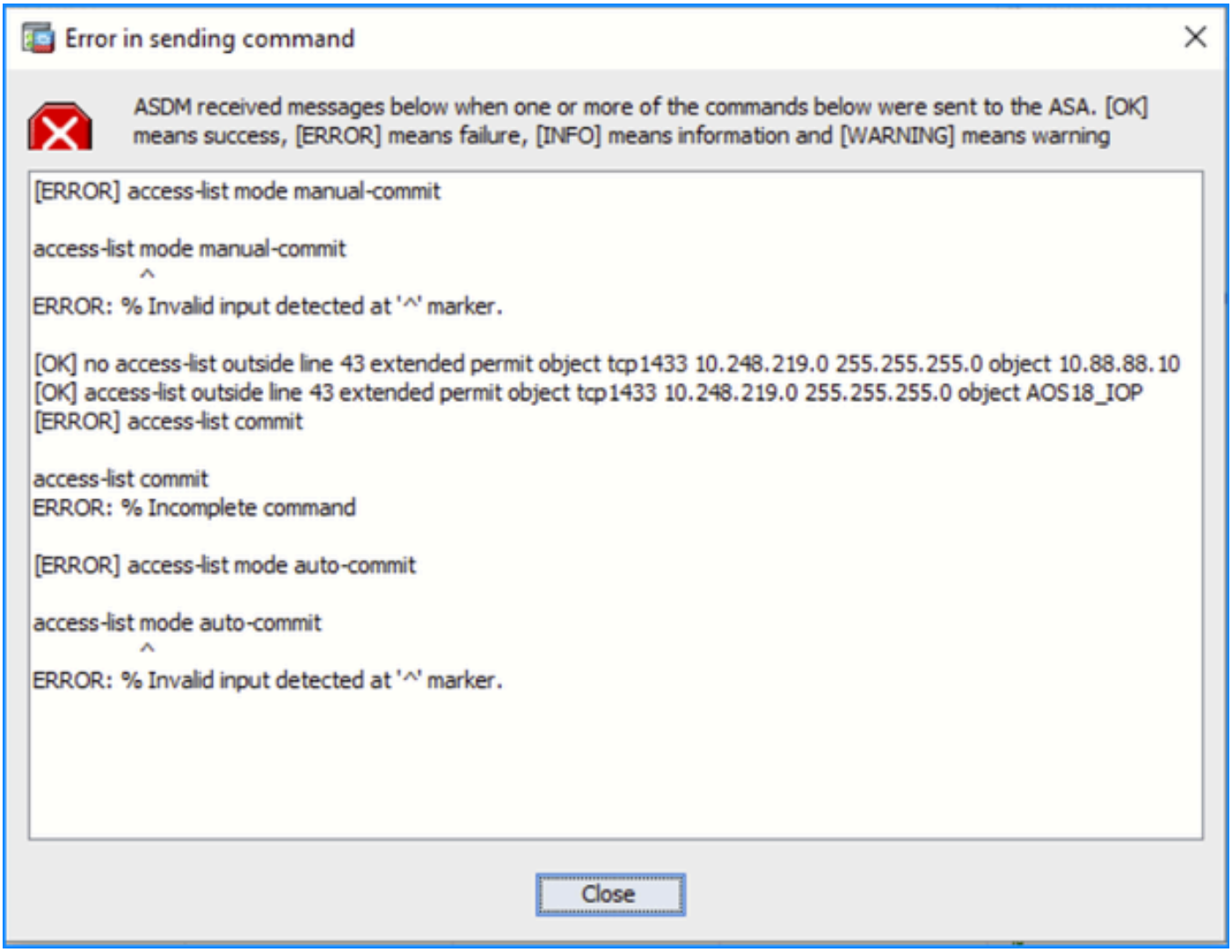
Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCtq38377 "ENH: ASDM debe utilizar el cálculo de hash de ACL en ASA y no el cálculo a nivel local" e ID de bug de Cisco CSCtq38405"ENH: ASA necesita un mecanismo para proporcionar información de hash de ACL a ASD"

Problema 3. "ERROR: % Se detectó una entrada no válida en el marcador '^'." mensaje de error al editar una ACL en ASDM

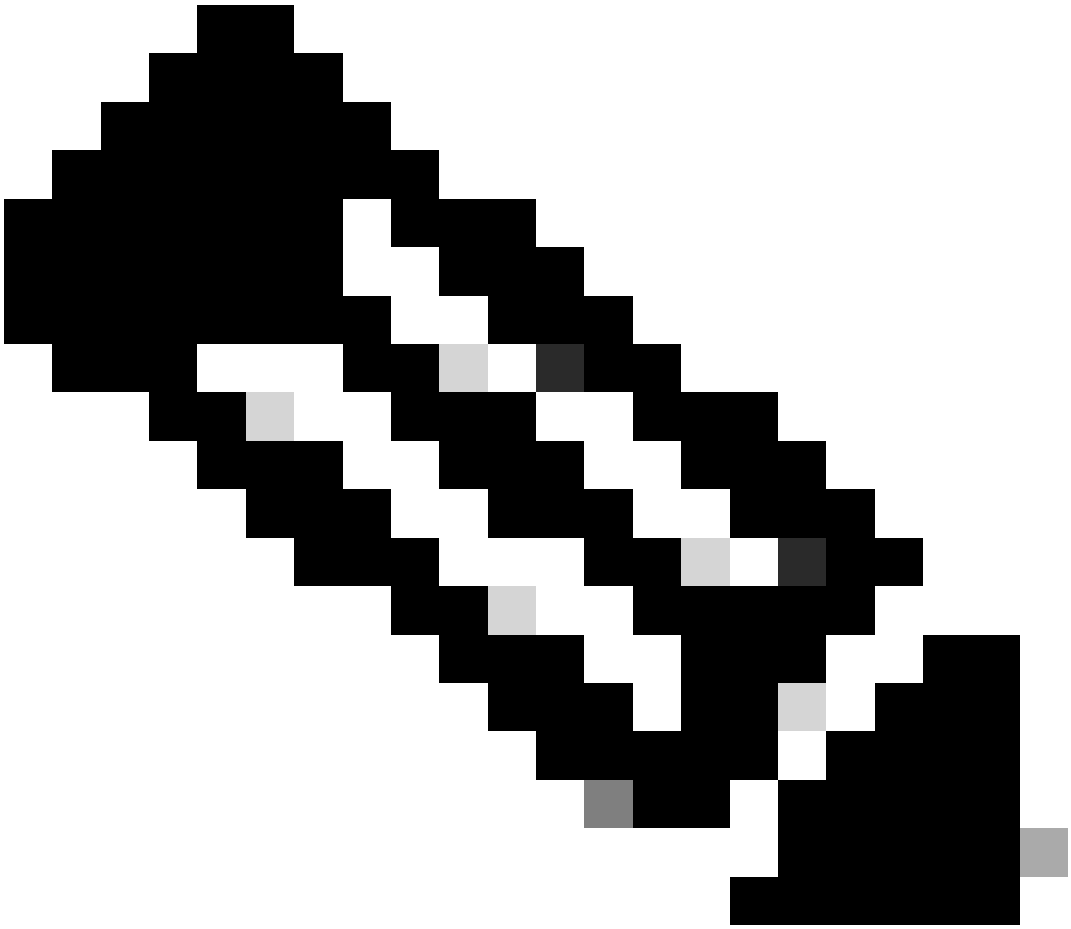
El mensaje de error "ERROR: % Se detectó una entrada no válida en el marcador '^'." se muestra un mensaje de error al editar una ACL en ASDM:

```
[ERROR] access-list mode manual-commit access-list mode manual-commit
                      ^
ERROR: % Invalid input detected at '^' marker.
[OK] no access-list ACL1 line 1 extended permit tcp object my-obj-1 object my-obj-2 eq 12345
[ERROR] access-list commit access-list commit
ERROR: % Incomplete command
[ERROR] access-list mode auto-commit access-list mode auto-commit
                      ^
ERROR: % Invalid input detected at '^' marker.
```



Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCvq05064 "Editar una entrada (ACL) de ASDM da un error. Cuando se utiliza ASDM con OpenJRE/Oracle - versión 7.12.2" y el ID de bug de Cisco CSCvp88926 "Envío de comandos de adición al eliminar la lista de acceso".



> Nota: Estos defectos se han corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

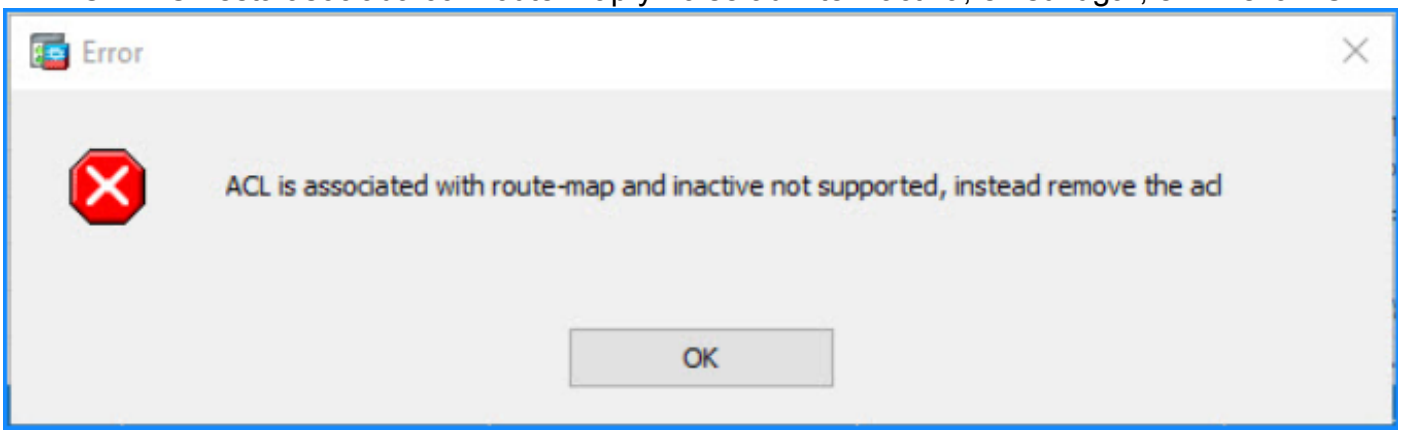
Problema 4. El mensaje de error "ERROR: ACL está asociado con route-map y no se admite inactivo; en su lugar, elimine el mensaje de error "acl" en casos específicos

El mensaje de error "ERROR: ACL está asociado con route-map y no se admite inactivo. En su lugar, se muestra el mensaje de error "acl" en uno de estos casos:

1. Edite una ACL en ASDM utilizada en una configuración de ruteo basada en políticas:

firewall (config)# access-list pbr line 1 permit ip any host 192.0.2.1

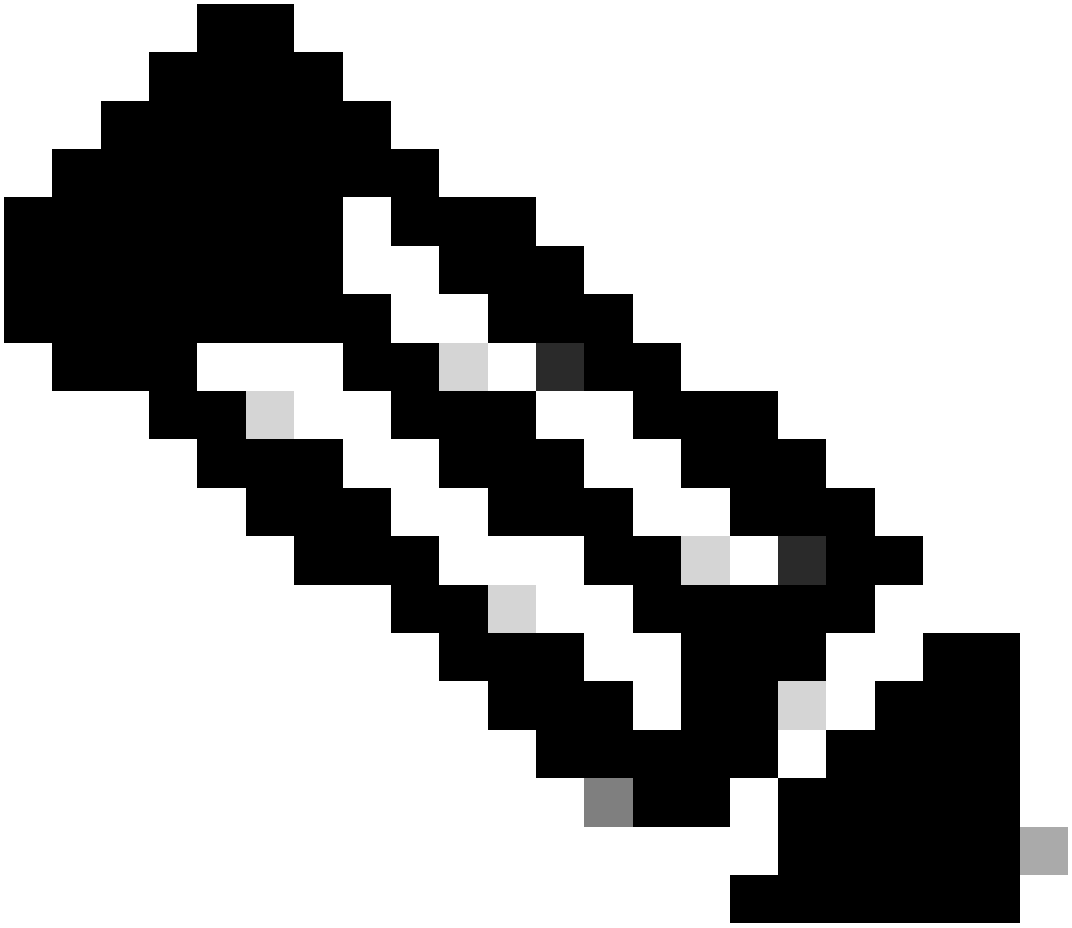
ERROR: ACL está asociada con route-map y no se admite inactiva; en su lugar, elimine la ACL



2. Edite una ACL ASDM > Configuration -> Remote Access VPN -> Network (Client) Access > Dynamic Access policy

Solución de problemas: acciones recomendadas

1. Consulte el ID de bug de software Cisco CSCwb57615 "Error al configurar la lista de acceso pbr con el número de línea". La solución alternativa es excluir el parámetro "line" de la configuración.
2. Consulte el software Cisco bug ID CSCwe3465 "No se pueden editar los objetos ACL si ya está en uso, obteniendo la excepción".



Nota: Estos defectos se han corregido en las últimas versiones del software ASA. Consulte los detalles del defecto para obtener más información.

Problema 5. No hay registros en el visor de registro en tiempo real de ASDM para conexiones denegadas implícitamente

El visor de registro en tiempo real de ASDM no muestra registros de conexiones denegadas implícitamente.

Solución de problemas: acciones recomendadas

La negación implícita al final de la lista de acceso no genera syslog. Si desea que todo el tráfico denegado genere syslog, agregue una regla con la palabra clave log al final de la ACL.

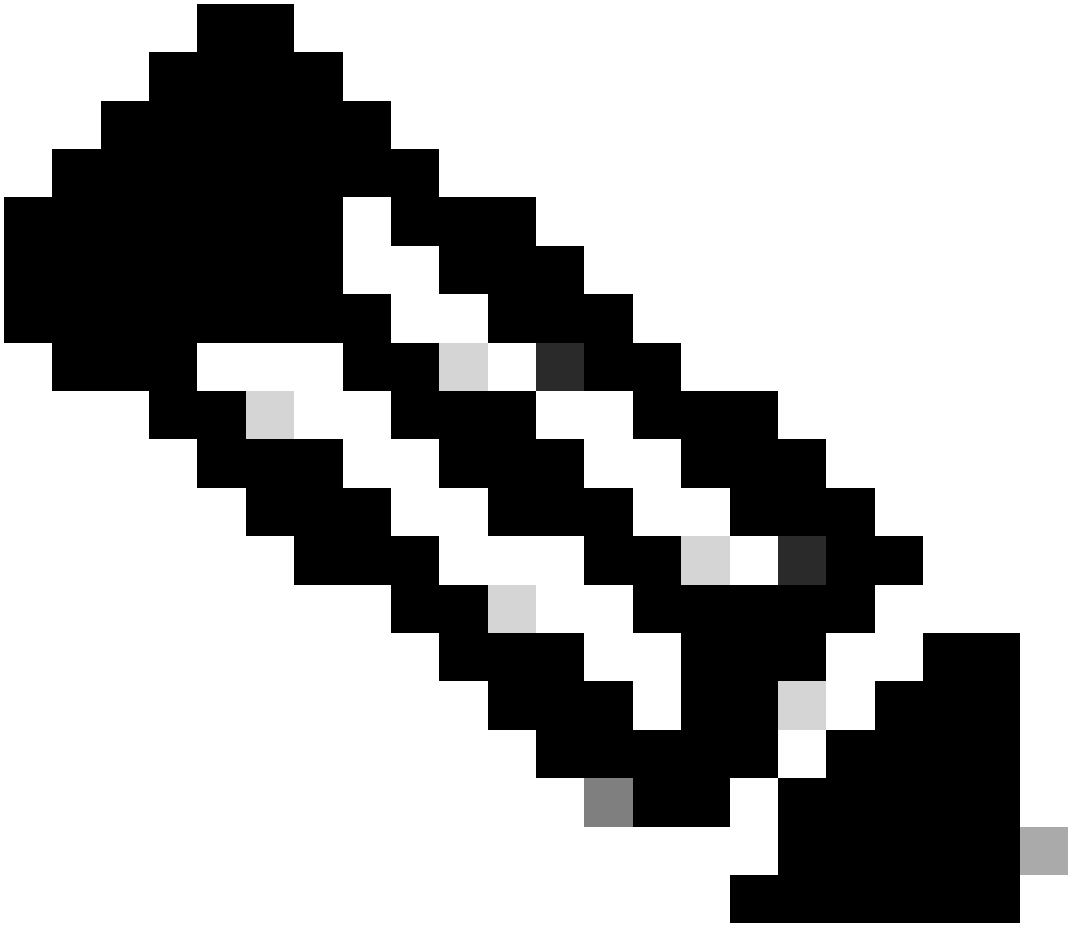
Problema 6. ASDM se congela cuando se intenta modificar cualquier objeto de red o grupo de objetos

ASDM se congela cuando se intenta modificar cualquier objeto de red o grupo de objetos desde la página Configuration > Firewall > Access Rules bajo la pestaña Addresses. El usuario no podrá editar ninguno de los parámetros de la ventana de objetos de red cuando se produzca este problema.

Solución de problemas: acciones recomendadas

Consulte el ID de bug de software Cisco CSCwj1250 "ASDM se congela al editar objetos de red o grupos de objetos de red". La solución alternativa es inhabilitar la recopilación de estadísticas del host topN:

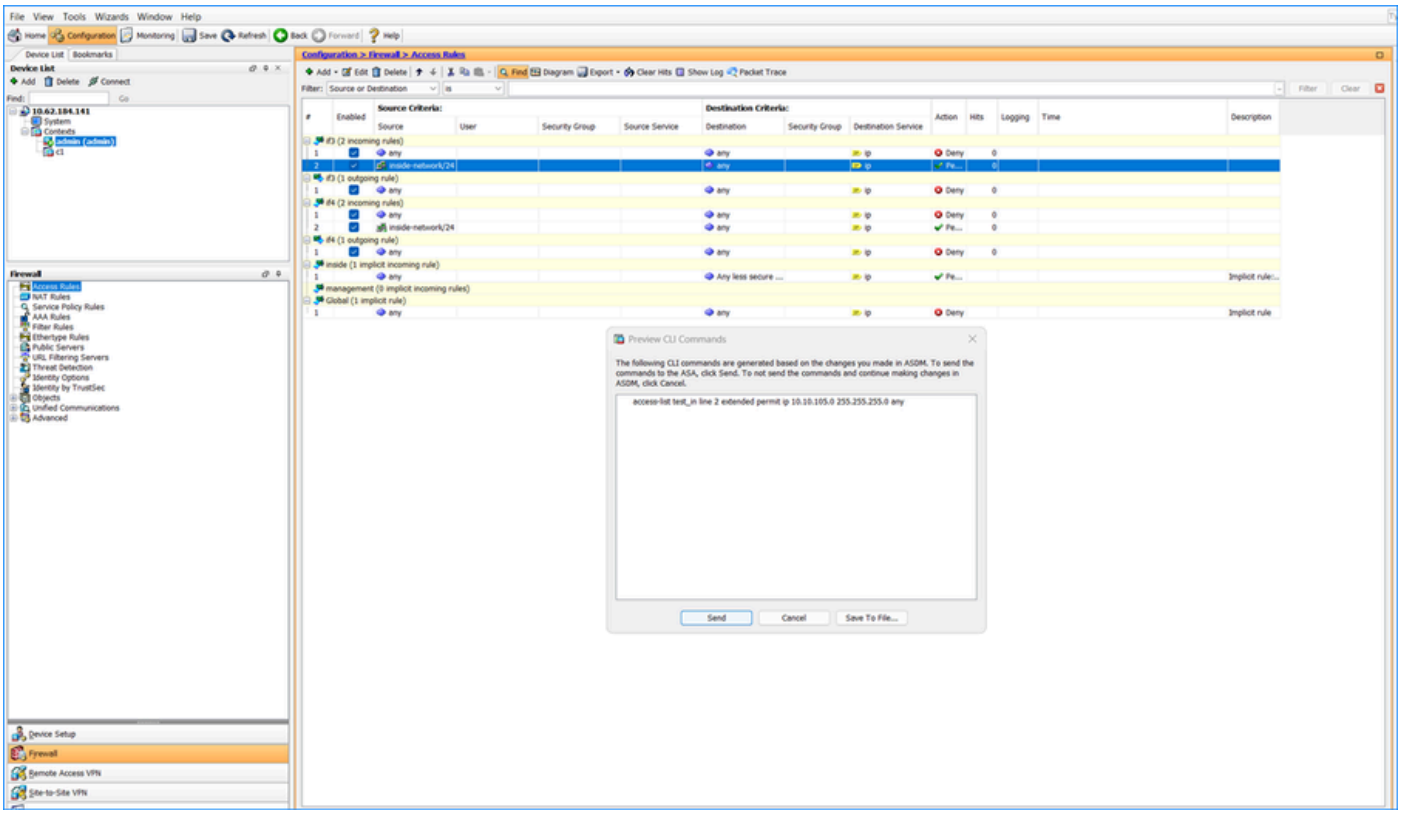
```
<#root>

ASA(config)#

no hpm topN enable
```



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

Problema 7. ASDM puede mostrar reglas adicionales de la lista de control de acceso para diferentes interfaces

ASDM puede mostrar reglas adicionales de la lista de control de acceso para diferentes interfaces si se modifica una lista de control de acceso de nivel de interfaz. En este ejemplo, se agregó una regla entrante nº 2 a la interfaz if3 ACL. ASDM también muestra #2 para la interfaz if4, mientras que esta regla no fue configurada por el usuario. La vista previa del comando muestra correctamente un solo cambio pendiente. Este es un problema de visualización de la interfaz de usuario.



Solución de problemas: acciones recomendadas

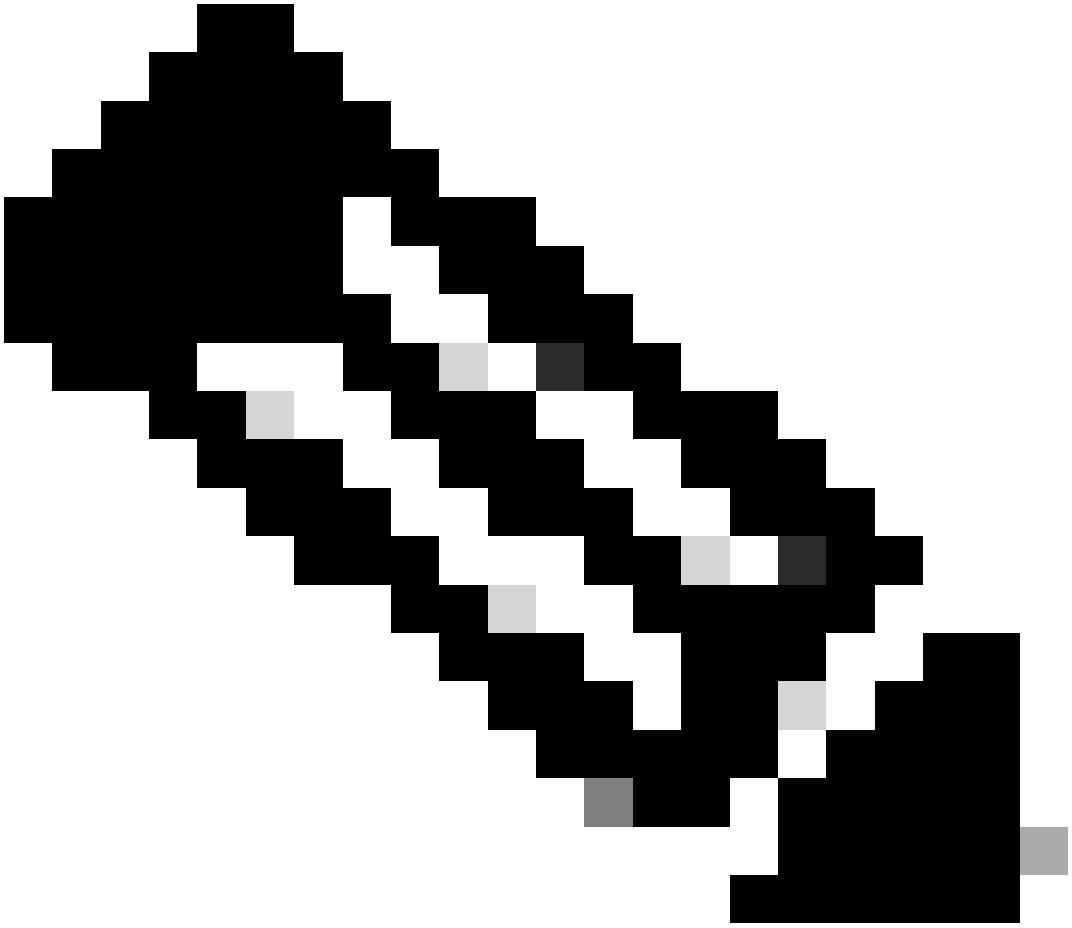
Consulte el ID de bug del software Cisco CSCwm71434 "ASDM puede mostrar entradas duplicadas de la lista de acceso de la interfaz".

Problema 8. Los registros en tiempo real no están disponibles en el Visualizador de registros en tiempo real

No se muestra ningún registro en el visor de registros en tiempo real

Solución de problemas: acciones recomendadas

1. Asegúrese de que el registro esté configurado. Consulte el libro 1 de ASDM: Guía de Configuración de ASDM de Operaciones Generales de la Serie ASA de Cisco, 7.22, Capítulo: Registro.
2. Consulte el software Cisco bug ID CSCvf82966 "ASDM - Logging: No se pueden ver los registros en tiempo real".

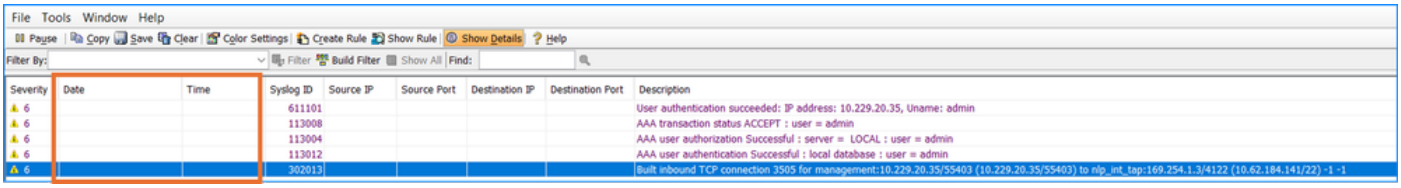


Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Referencias

- Libro 1 de ASDM: Guía de Configuración de ASDM de Operaciones Generales de la Serie ASA de Cisco, 7.22, Capítulo: Registro.

Problema 9. Las columnas de fecha y hora están vacías en el visor de registros en tiempo real



Solución de problemas: acciones recomendadas

1. Compruebe si se utiliza el formato de registro de hora RFC5424:

<#root>

#

show run logging

logging enable

logging timestamp rfc5424

2. Si se utiliza el formato de registro de fecha y hora RFC5424, consulte el ID de bug de Cisco CSCvs52212 "ASDM ENH: capacidad para que los visores de registro de eventos muestren los registros del sistema ASA con el formato de marca de tiempo rfc5424". La solución alternativa es evitar el uso del formato RFC5424:

<#root>

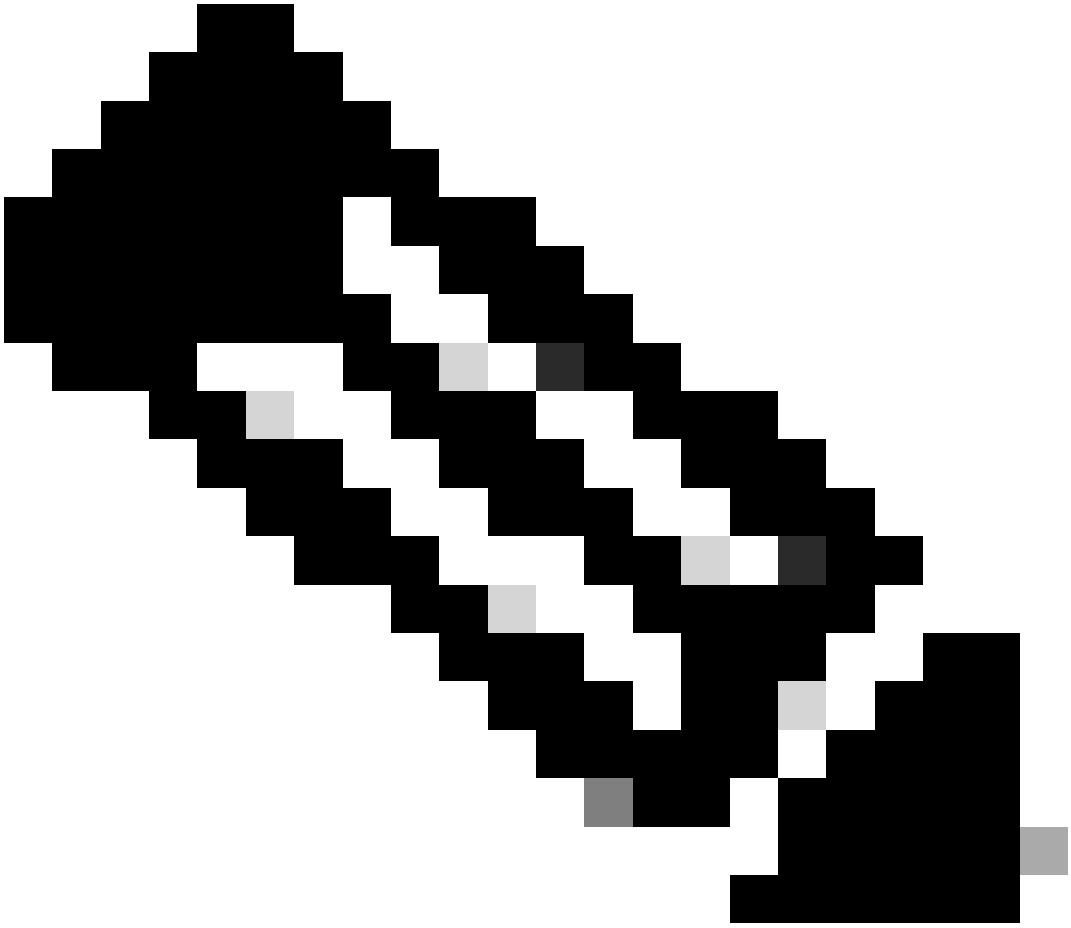
firewall(config)#

no logging timestamp rfc5424

firewall(config)#

logging timestamp

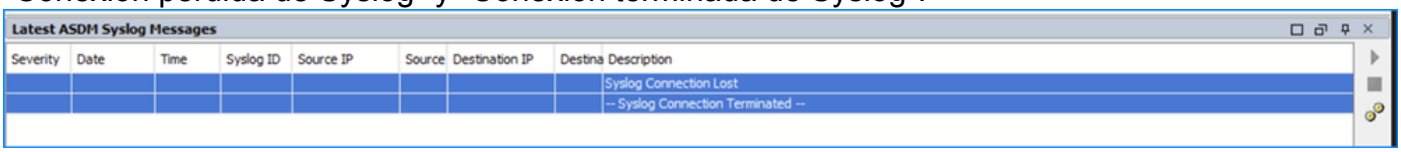
3. Además, consulte el defecto de software ID de bug Cisco CSCwh70323 "Falta entrada de registro de hora para algunos mensajes de syslog enviados al servidor syslog".



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

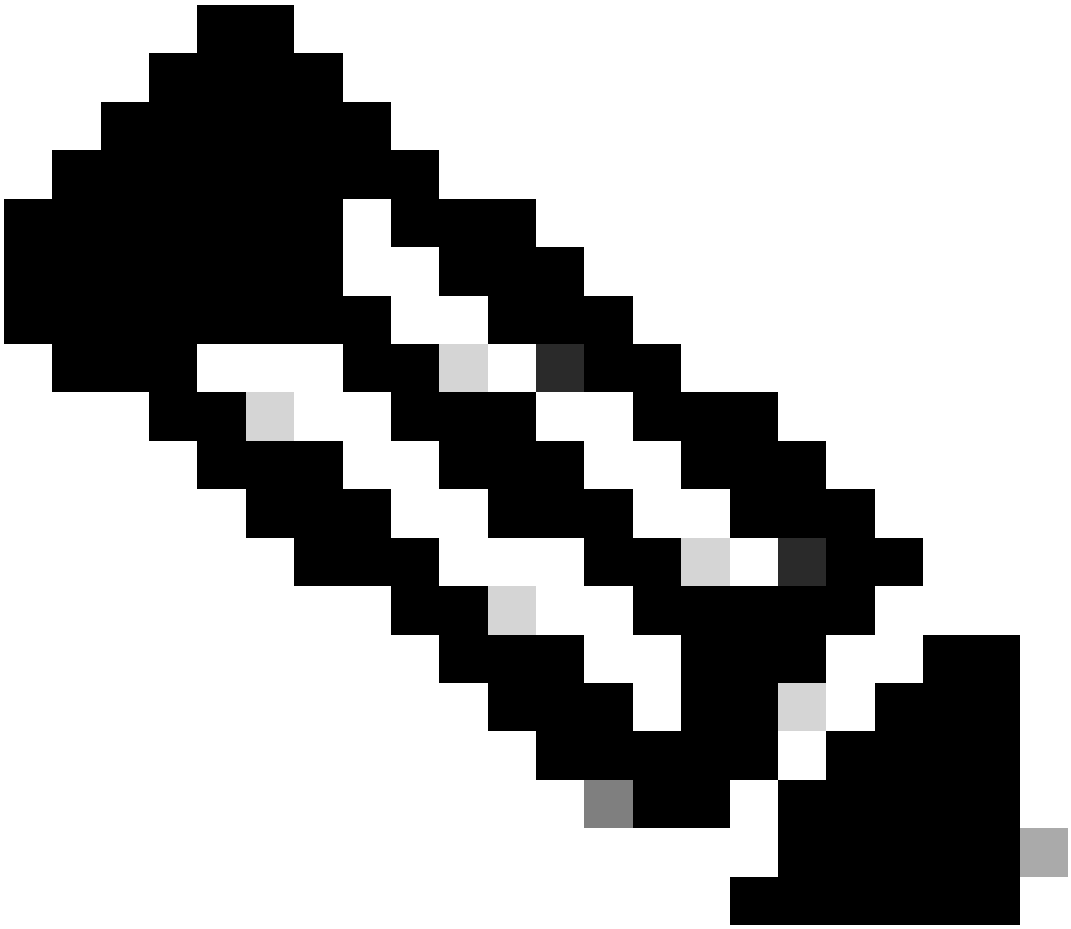
Problema 10. El registro en ASDM puede fallar después de cambiar a un contexto diferente en un ASA multicontexto

La pestaña Últimos Mensajes de Syslog de ASDM en la página Inicio muestra los mensajes "Conexión perdida de Syslog" y "Conexión terminada de Syslog":



Solución de problemas: acciones recomendadas

Asegúrese de que el registro esté configurado. Consulte el software Cisco bug ID CSCvz15404 "ASA: Modo de contexto múltiple: El registro de ASDM se detiene cuando se conmuta a un contexto diferente".



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

Problema 11. La sesión de ASDM finaliza abruptamente cuando se cambia entre diferentes contextos

La sesión de ASDM finaliza abruptamente cuando se conmuta entre diferentes contextos con el mensaje de error "El número máximo de sesiones de administración para el protocolo http o el usuario ya existe. Inténtelo de nuevo más tarde". Estos registros se muestran en los mensajes de syslog:

```
%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5

%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5
```

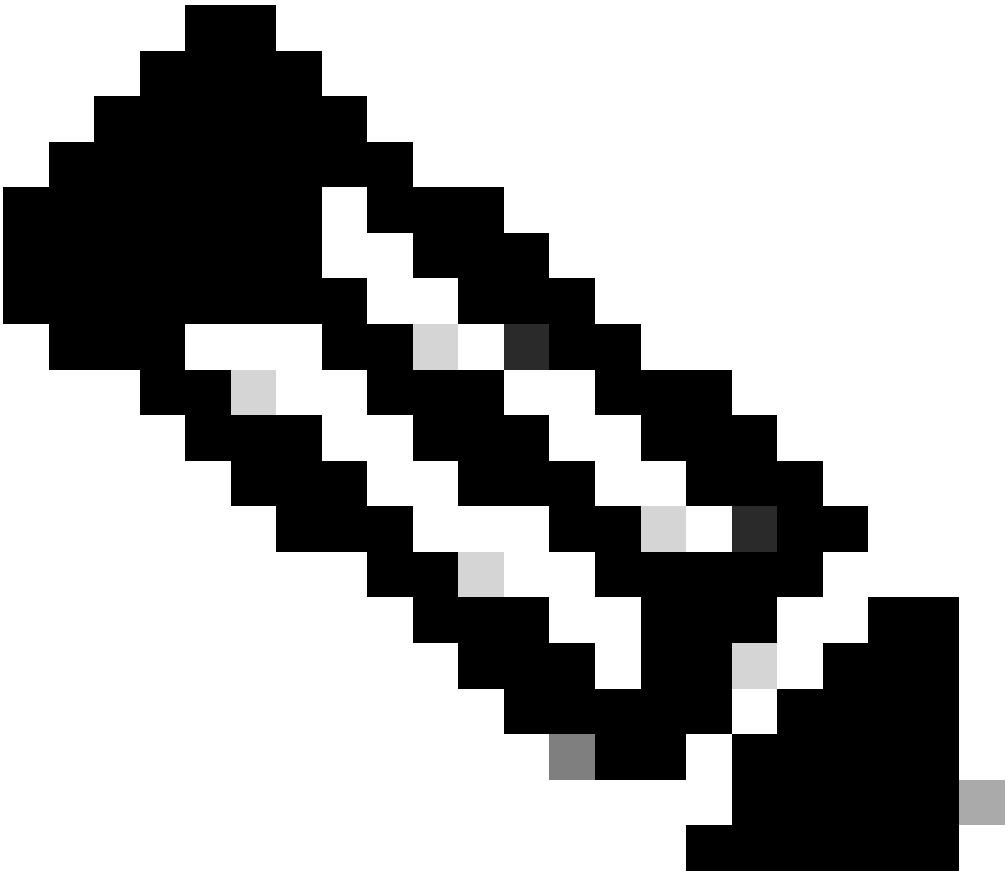
Solución de problemas: acciones recomendadas

1. Verifique si el uso de recursos Current ASDM ha alcanzado el Límite. En este caso, el contador Denied aumenta:

<#root>

```
firewall #

show resource usage resource ASDM


Resource                Current        Peak      Limit        Denied Context
ASDM

5

           5

5


10

 admin
```

2. Consulte el software Cisco bug ID CSCvs72378 "La sesión de ASDM se termina abruptamente cuando se conmuta entre diferentes contextos".



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

3. Si la versión de software tiene la corrección para el ID de bug de Cisco CSCvs72378, y el recurso actual alcanzó el límite, desconecte algunas de las sesiones ASDM existentes. Puede cerrar el ASDM o, alternativamente, borrar las conexiones HTTPS para la dirección IP del host que ejecuta el ASDM. En este ejemplo, se supone que el servidor HTTP en ASDM se ejecuta en el puerto HTTPS predeterminado 443:

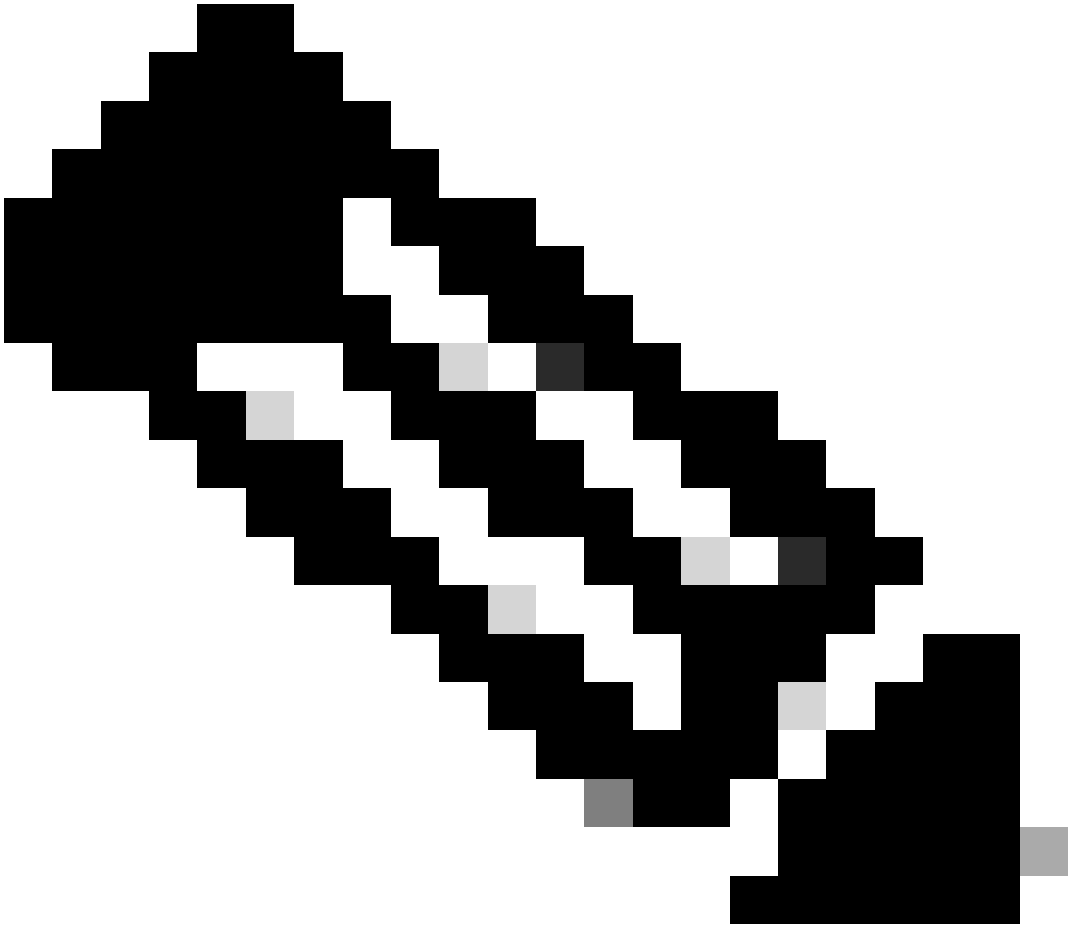
```
<#root>

#

show conn all protocol tcp port 443


TCP management  192.0.2.35:55281 NP Identity Ifc  192.0.2.1:443, idle 0:00:01, bytes 33634, flags UOB
TCP management  192.0.2.36:38844 NP Identity Ifc  192.0.2.1:443, idle 0:00:08, bytes 1629669, flags UOB
#

clear conn all protocol tcp port 443 address 192.0.2.35
```

Problema 12. ASDM sale/termina aleatoriamente con el mensaje "ASDM recibió un mensaje del dispositivo ASA para desconectarse. El ASDM se cerrará ahora".

En ASA multicontexto, el ASDM sale/termina aleatoriamente con el mensaje "ASDM recibió un mensaje del dispositivo ASA para desconectarse. El ASDM se cerrará ahora.".

Solución de problemas: acciones recomendadas

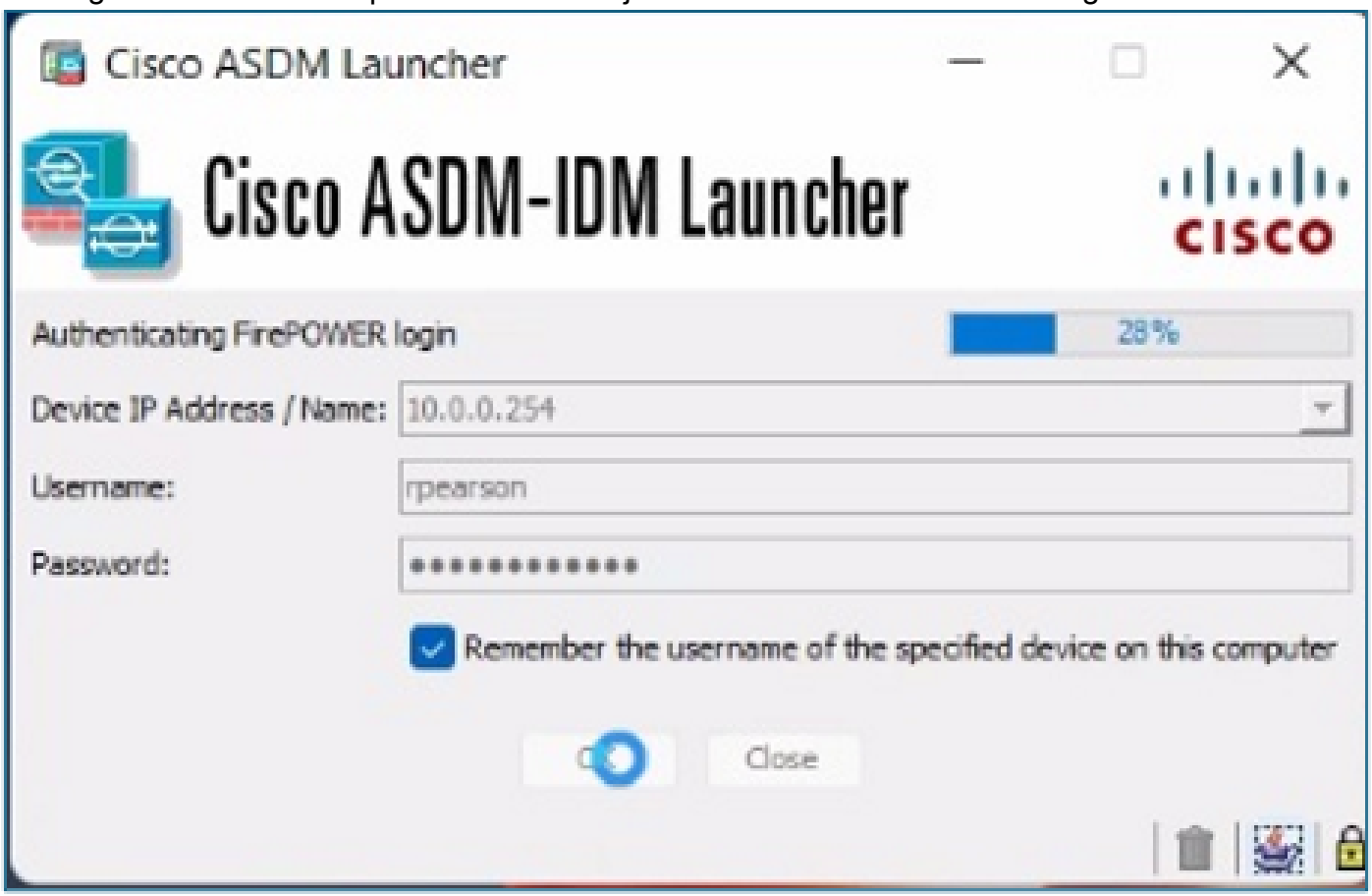
Consulte el defecto de software ID de bug Cisco CSCwh04395 "La aplicación ASDM sale/termina aleatoriamente con un mensaje de alerta en la configuración multi-contexto".



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

Problema 13. La carga de ASDM se bloquea con el mensaje "Authentication FirePOWER login"

La carga de ASDM se bloquea con el mensaje "Authentication FirePOWER login":

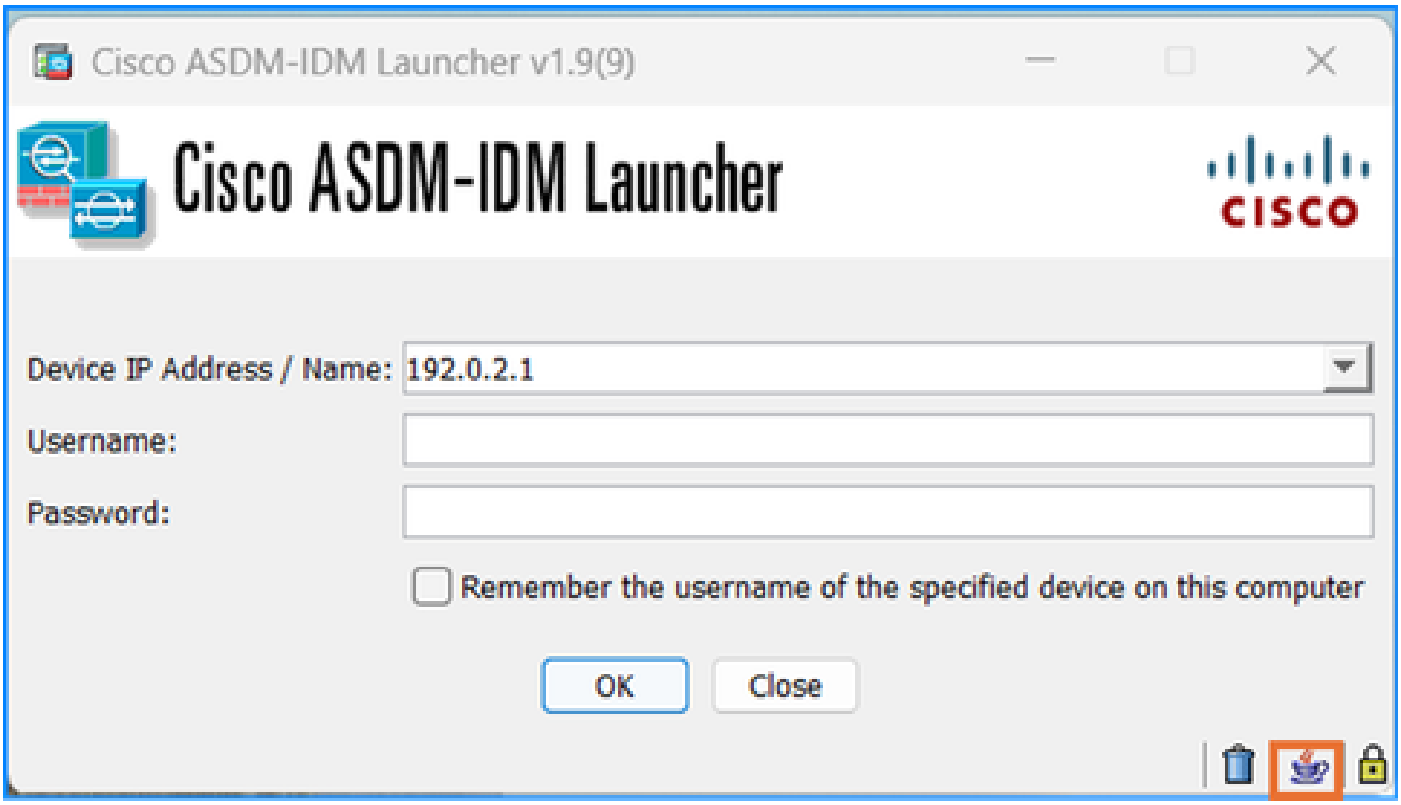


Los registros de la consola Java muestran el mensaje "Error al conectarse a FirePower, continuar sin él":

<#root>

```
2023-05-08 16:55:10,564 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
0 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup  - CLI-PASSTHROUGH-DEBUG Inside do
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
2023-05-08 16:55:10,657 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cpl@18c4cb7
93 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup  - CLI-PASSTHROUGH-DEBUG Inside d
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cpl@18c4cb75
com.jidesoft.plaf.LookAndFeelFactory not loaded.
2023-05-08 17:15:31,419 [ERROR]  Unable to login to DC-Lite. STATUS CODE IS 502
1220855 [SGZ Loader: launchSgzApplet] ERROR com.cisco.dmcommon.util.DMCommonEnv  -  Unable to login to
May 08, 2023 10:15:31 PM vd cx

INFO: Failed to connect to FirePower, continuing without it.
May 08, 2023 10:15:31 PM vd cx
INFO: If the FirePower is NATed, clear the cache (C:/Users/user1/.asdm/data/firepower.conf) and try agai
Env.isAsdmInHeadlessMode()------------->false
java.lang.InterruptedException
        at java.lang.Object.wait(Native Method)
```

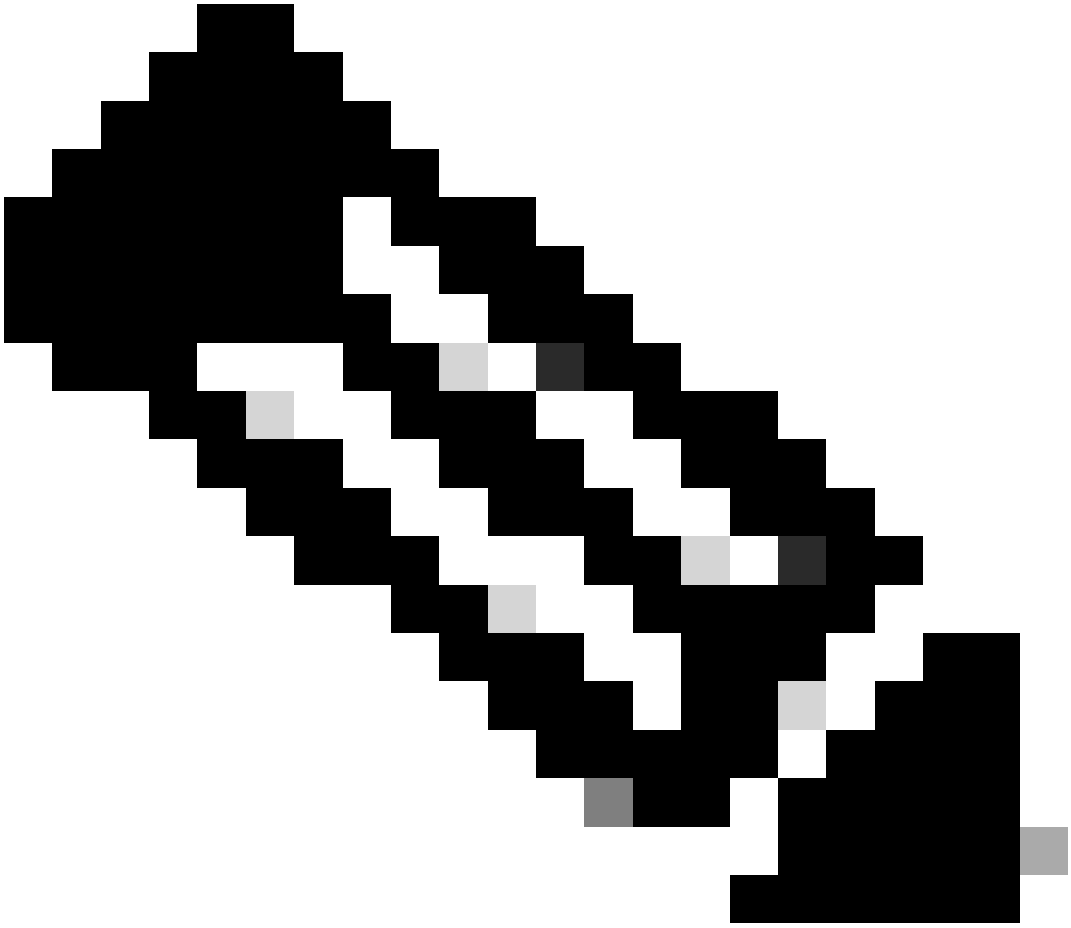
Para verificar este síntoma, habilite los registros de la consola Java:



Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCwe15164 "ASA: ASDM no puede mostrar las pestañas de SFR hasta que se "active" a través de su CLI." Pasos de la solución alternativa:

1. Cierre el administrador ASDM.
2. Obtenga acceso SSH al SFR y cambie el usuario a root (sudo su).
3. Después de realizar los pasos anteriores, vuelva a iniciar el ASDM y podrá cargar las pestañas de Firepower (SFR).



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

Problema 14. ASDM no muestra la administración/configuración del módulo Firepower

La configuración del módulo Firepower no está disponible en ASDM.

Solución de problemas: acciones recomendadas

1. Asegúrese de que las versiones del módulo ASA, ASDM, Firepower y del sistema operativo sean compatibles. Consulte Notas de la versión de Cisco Secure Firewall ASA, Notas de la versión de Cisco Secure Firewall ASDM, Compatibilidad de Cisco Secure Firewall ASA:

- ASA 9.14/ASDM 7.14/Firepower 6.6 es la versión final para el módulo ASA FirePOWER en

ASA 5525-X, 5545-X y 5555-X.
- ASA 9.12/ASDM 7.12/Firepower 6.4.0 es la versión final para el módulo ASA FirePOWER en ASA 5515-X y 5585-X.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 es la versión final para el módulo ASA FirePOWER en ASA serie 5506-X y 5512-X.
- Las versiones de ASDM son compatibles con versiones anteriores de ASA, a menos que se indique lo contrario. Por ejemplo, ASDM 7.13(1) puede administrar un ASA 5516-X en ASA 9.10(1).
- ASDM no es compatible con la gestión del módulo FirePOWER con ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ y 9.16(3.19)+; debe utilizar FMC para gestionar el módulo con estas versiones. Estas versiones de ASA requieren ASDM 7.18(1.152) o posterior, pero la compatibilidad con ASDM para el módulo ASA FirePOWER finalizó con 7.16.
- ASDM 7.13(1) y ASDM 7.14(1) no eran compatibles con ASA 5512-X, 5515-X, 5585-X y ASASM; debe actualizar a ASDM 7.13(1.101) o 7.14(1.48) para restaurar la compatibilidad con ASDM.

2. Si las versiones son compatibles, verifique si el módulo está en funcionamiento:

<#root>

```
firewall#
```

show module sfr details

```
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5508
Hardware version:   N/A
Serial Number:      AAAABBBB1111
Firmware version:   N/A
Software version:   7.0.6-236
MAC Address Range:  006b.f18e.dac6 to 006b.f18e.dac6
App. name:          ASA FirePOWER
```

App. Status: Up

```
App. Status Desc:   Normal Operation
App. version:       7.0.6-236
```

Data Plane Status: Up

Console session: Ready

Status: Up

```
DC addr:            No DC Configured
Mgmt IP addr:       192.0.2.1
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt web ports:     443
```

```
Mgmt TLS enabled:   true
```

Si el módulo está inactivo, el comando sw-module module module reset se puede utilizar para reiniciar el módulo y luego recargar el software del módulo.

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

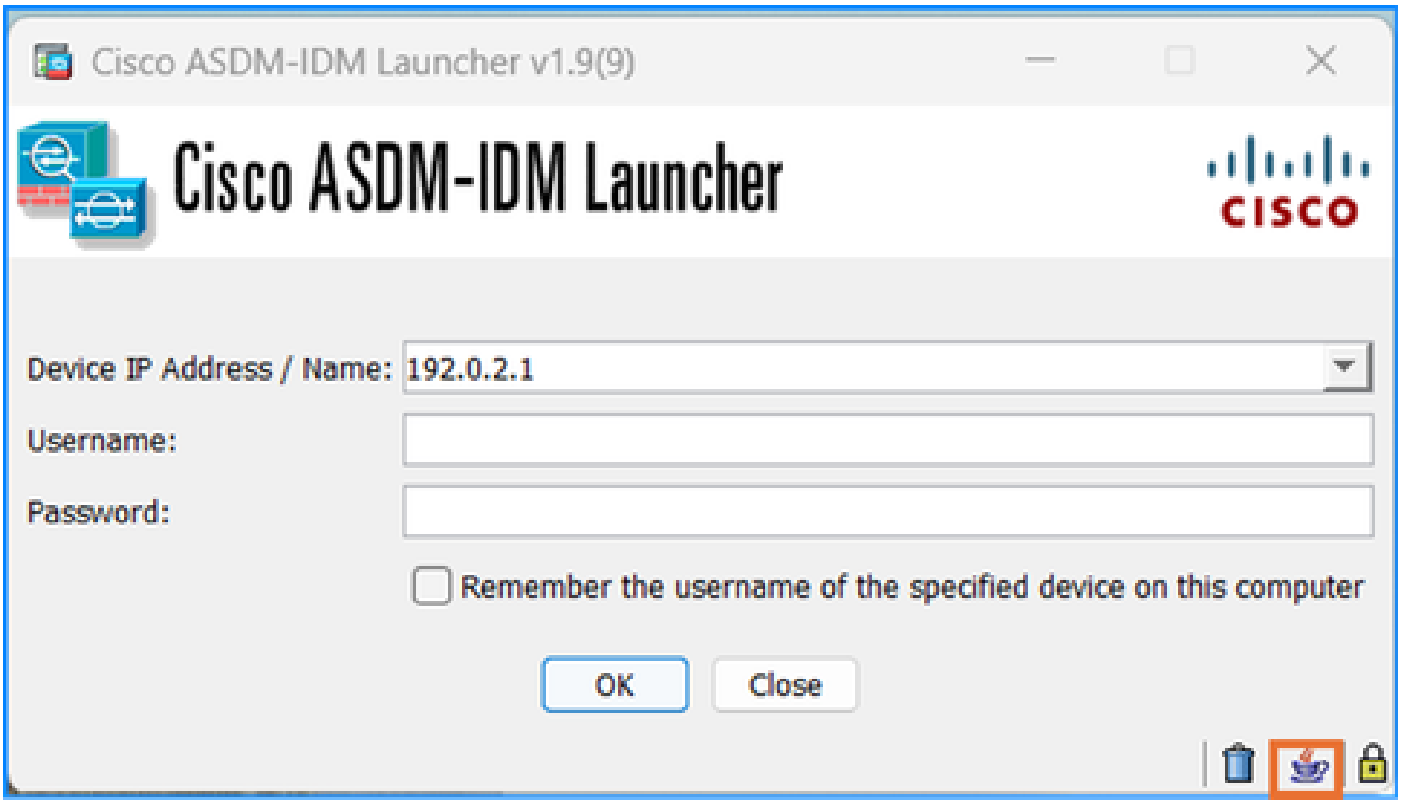
Problema 15. No se puede acceder a los perfiles de Secure Client en ASDM

Los registros de la consola Java muestran la excepción "java.lang.ArrayIndexOutOfBoundsException: Mensaje de error de 3":

<#root>

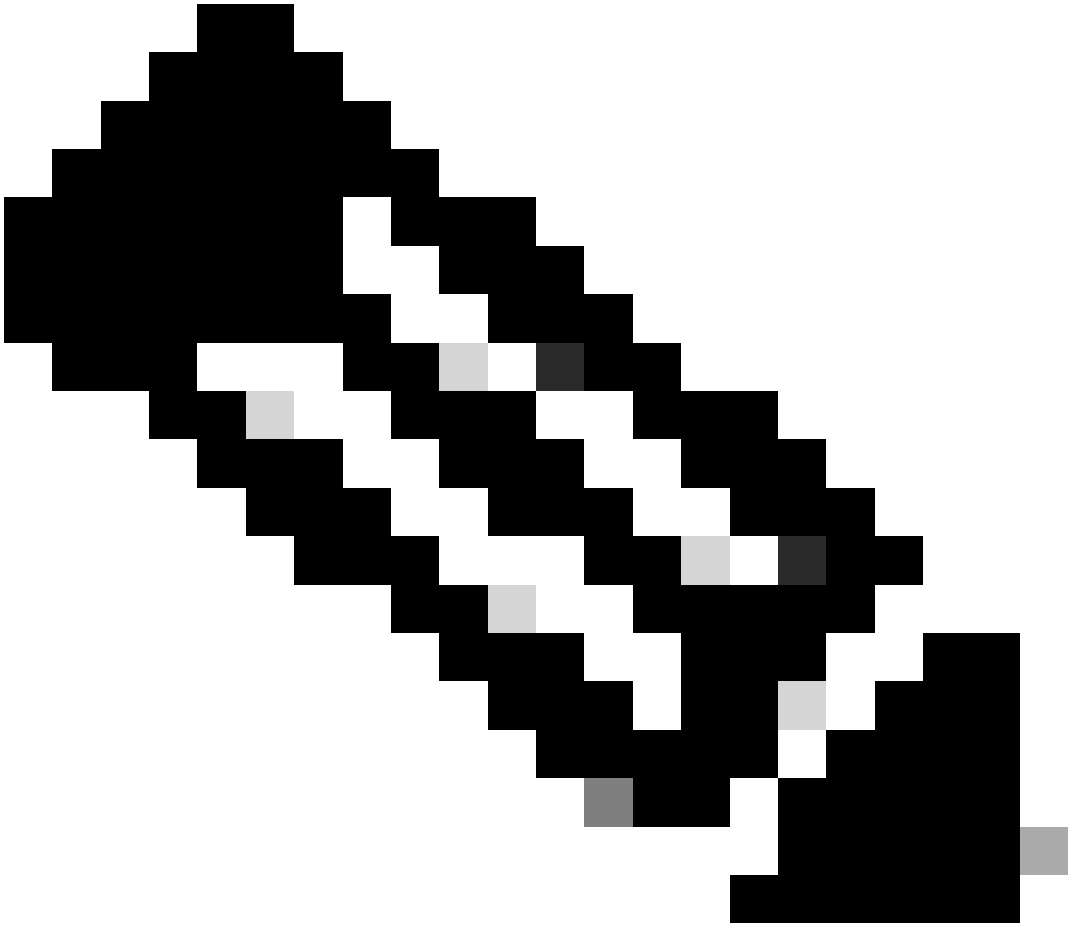
```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige

java.lang.ArrayIndexOutOfBoundsException: 3


   at doz.a(doz.java:1256)
   at doz.a(doz.java:935)
   at doz.l(doz.java:1100)
```

Para verificar este síntoma, habilite los registros de la consola Java:



Solución de problemas: acciones recomendadas

Consulte el ID de bug de software Cisco CSCwi56155 "Imposible acceder al perfil de cliente seguro en ASDM".



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

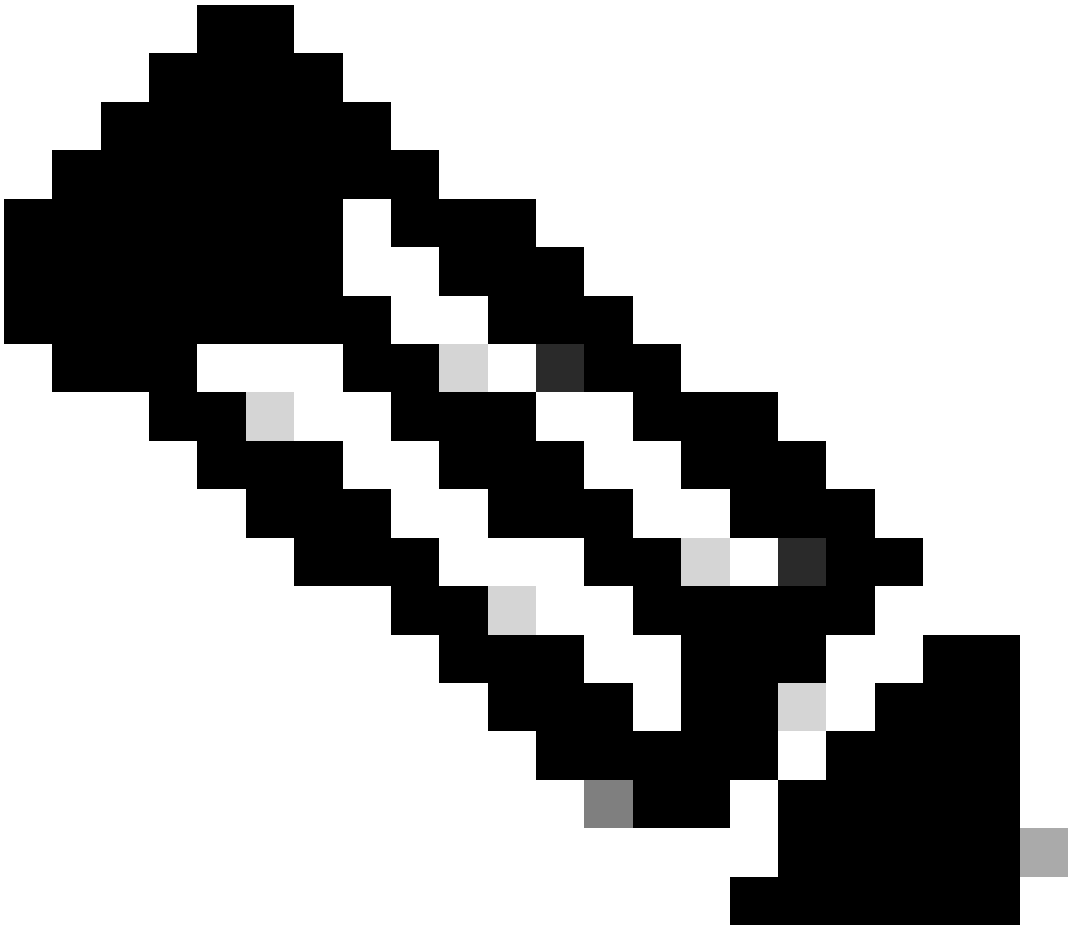
Problema 16. No se pueden editar los perfiles XML del perfil de cliente seguro en ASDM

Los perfiles XML del perfil de cliente seguro en ASDM Configuration > Remote Access VPN > Network (Client) Access no se pueden editar en un dispositivo ASA si hay una imagen de AnyConnect presente en el disco que es anterior a la versión 4.8.

El mensaje de error "There is no profile editor plugin in your Secure Client Image on the device. Vaya a Network (Client) Access > Secure Client Software e instale Secure Client Image versión 2.5 o posterior y vuelva a intentarlo".

Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCwk64399 "ASDM- No se puede editar el perfil de Secure Client". La solución alternativa es establecer otra imagen de AnyConnect con una prioridad más baja.



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

Problema 17. Faltan imágenes de Secure Client después de los cambios de configuración

Después de realizar cambios en ASDM Configuration > Network (Client) Access > Secure Client Profile, las imágenes en Configuration > Network (Client) Access > Secure Client Software faltan.

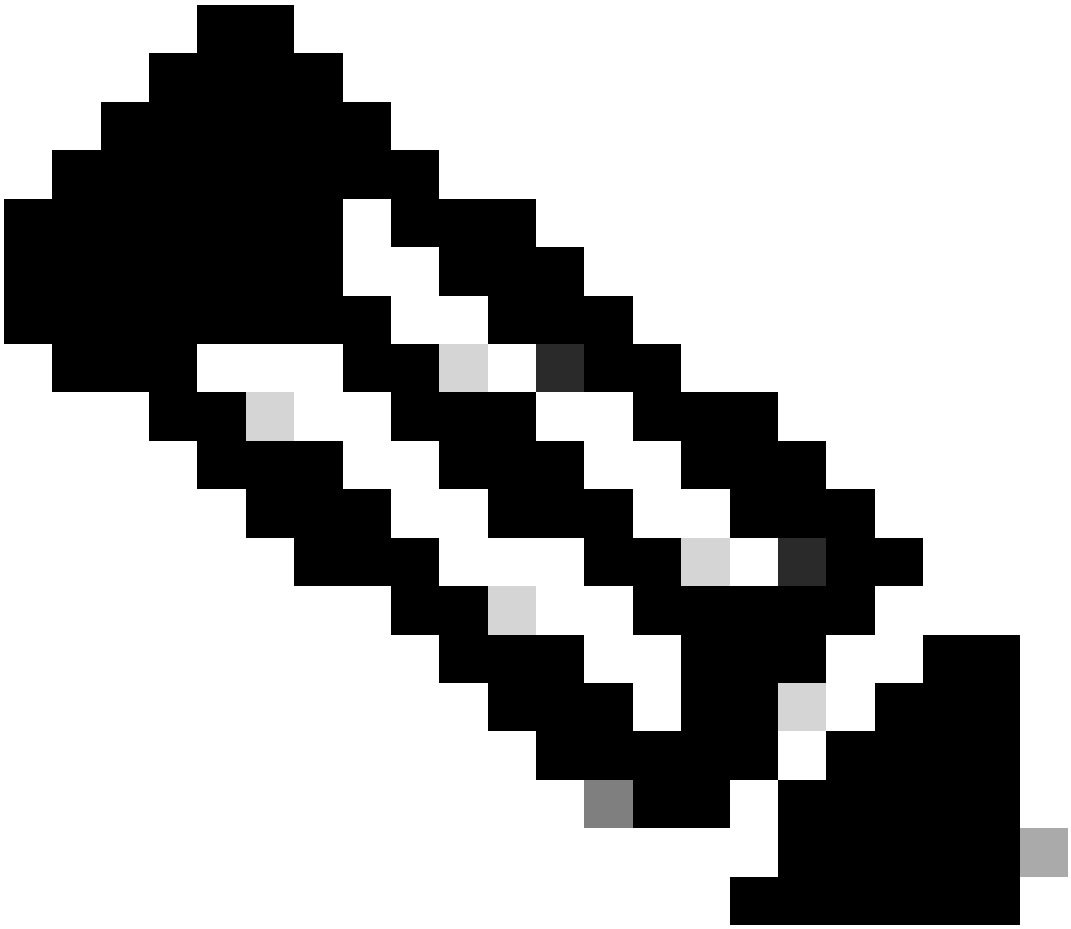
Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCwf23826 "Secure Client Software no se muestra después de modificar el Secure Client Profile Editor en ASDM". Las opciones de solución alternativa:

- Haga clic en el icono Actualizar en ASDM

O bien

- Cierre y vuelva a abrir ASDM



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

Problema 18. Comandos http server session-timeout y http server idle-timeout ineficaces

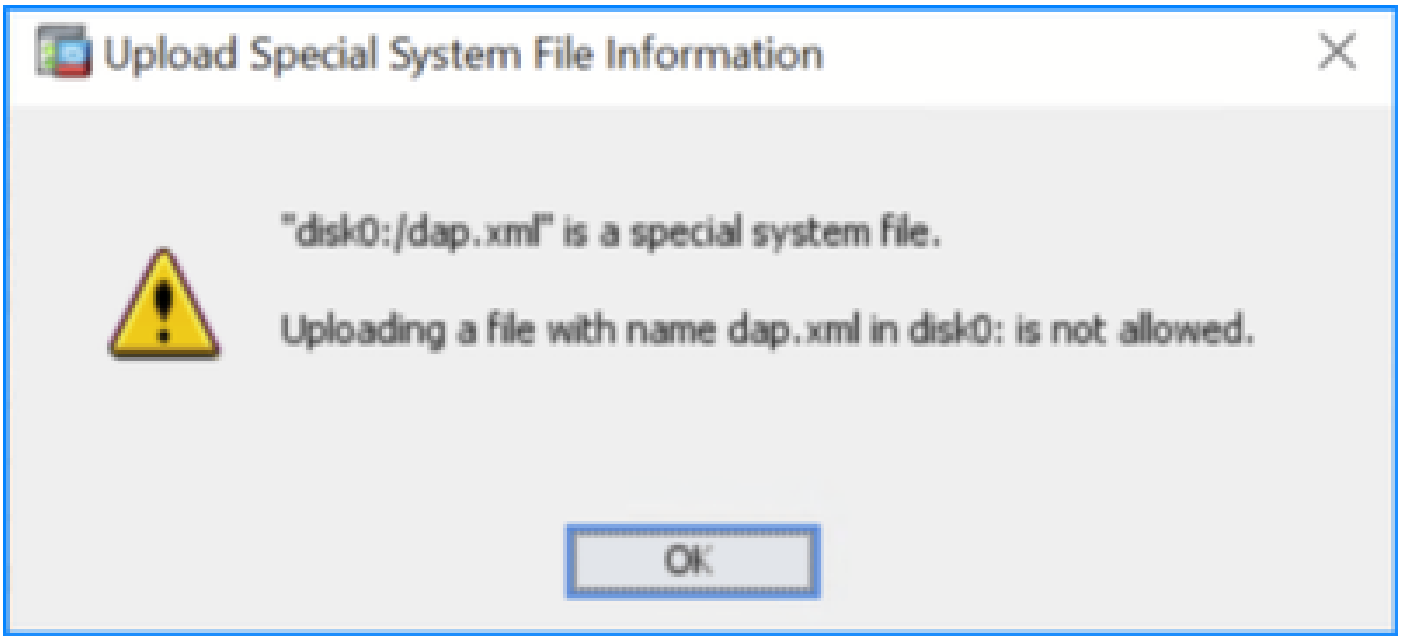
Los comandos http server session-timeout y http server idle-timeout no tienen efecto en el modo multicontexto ASA.

Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCtx41707 "Support for http server timeout command in multi-context mode". Los comandos son configurables, pero los valores no tienen ningún efecto.

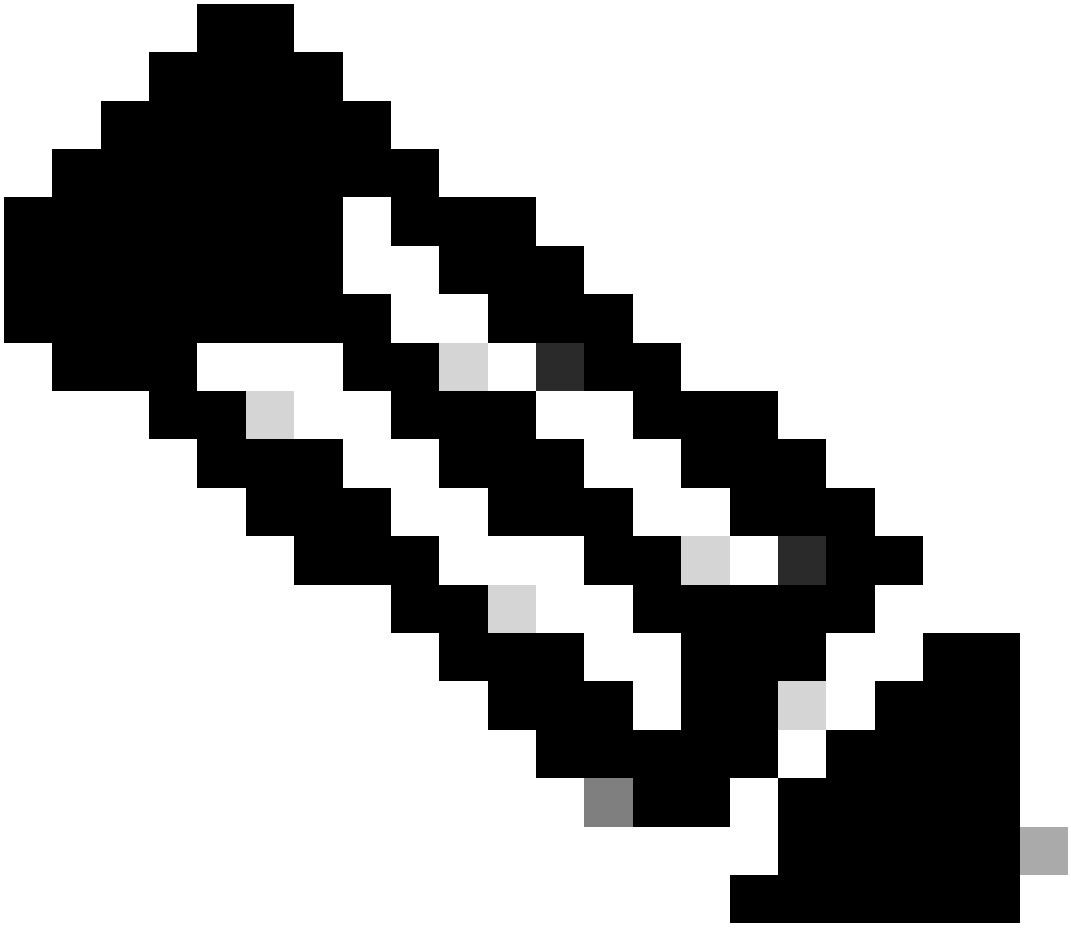
Problema 19. Error de copia de Dap.xml en ASDM

La copia de dap.xml a ASA a través de la ventana Administración de archivos en ASDM falla con el error "disk0:/dap.xml es un archivo de sistema especial. Cargando un archivo con el nombre dap.xml en disk0: no está permitido":



Solución de problemas: acciones recomendadas

Consulte el ID de bug de software Cisco CSCvt62162 "No se puede copiar dap.xml mediante la administración de archivos en ASDM 7.13.1". La solución alternativa es copiar el archivo directamente al ASA usando protocolos como FTP o TFTP.



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

Problema 20. No hay políticas IKE ni propuestas IPSEC visibles en ASDM

ASDM no muestra las políticas IKE y las propuestas IPSEC en la ventana Configuraciones > VPN de sitio a sitio.

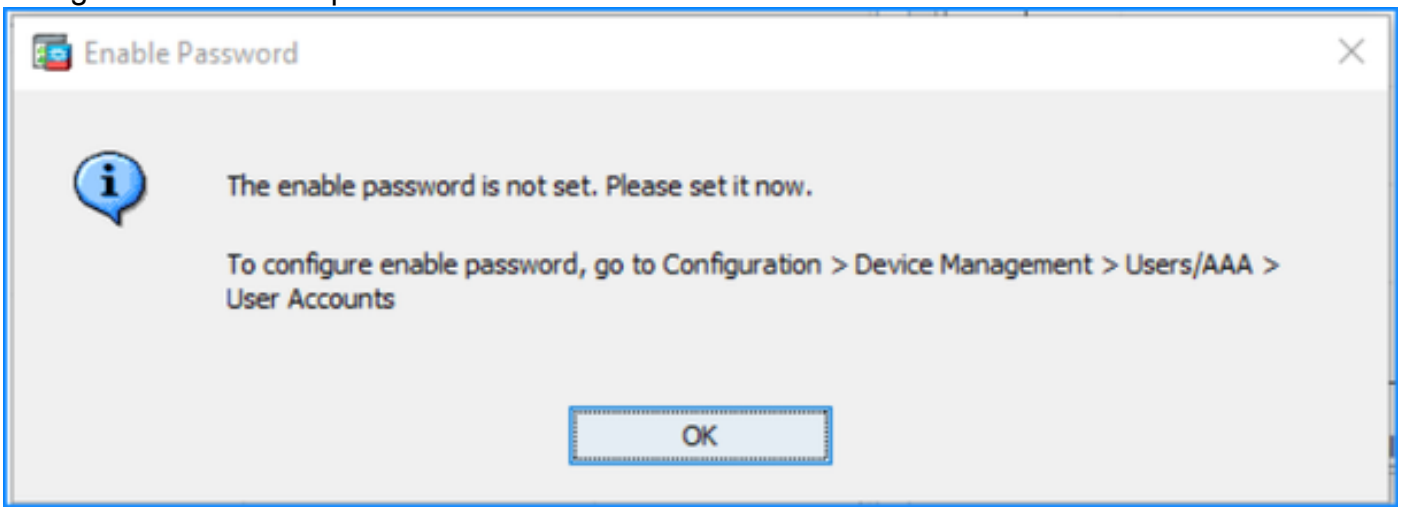
Solución de problemas: acciones recomendadas

Consulte la identificación de error de software Cisco CSCwm42701 "ASDM display blank in IKE policies and IPSEC projects tab" (Visualización de ASDM en blanco en las políticas IKE y la ficha de propuestas IPSEC).

Problema 21. ASDM muestra el mensaje "La contraseña de habilitación no está

establecida. Por favor, configúrelo ahora."

ASDM muestra el mensaje "La contraseña de habilitación no está configurada. Por favor, configúrelo ahora." después de cambiar la contraseña de habilitación en la línea de comandos:



Solución de problemas: acciones recomendadas

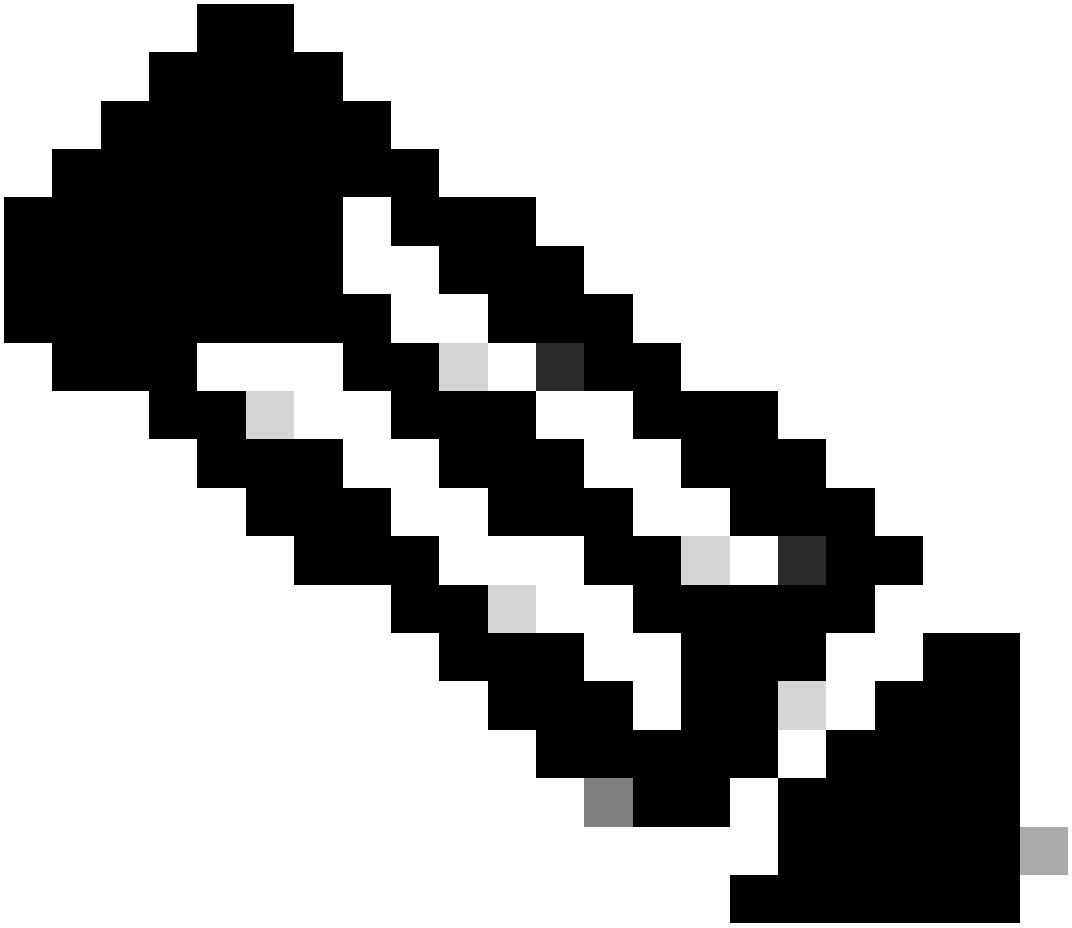
Consulte el ID de bug de software Cisco CSCvq42317 "ASDM pide cambiar la contraseña de habilitación después de que se estableció en CLI".

Problema 22. El objeto ASDN desaparece después de actualizar la interfaz de usuario ASDM

Al agregar un grupo de objetos y un host de objetos a un grupo de objetos existente y después de actualizar el ASDM, el grupo de objetos desaparece de la lista ASDM. Los nombres de objeto deben comenzar con números para que este defecto coincida.

Solución de problemas: acciones recomendadas

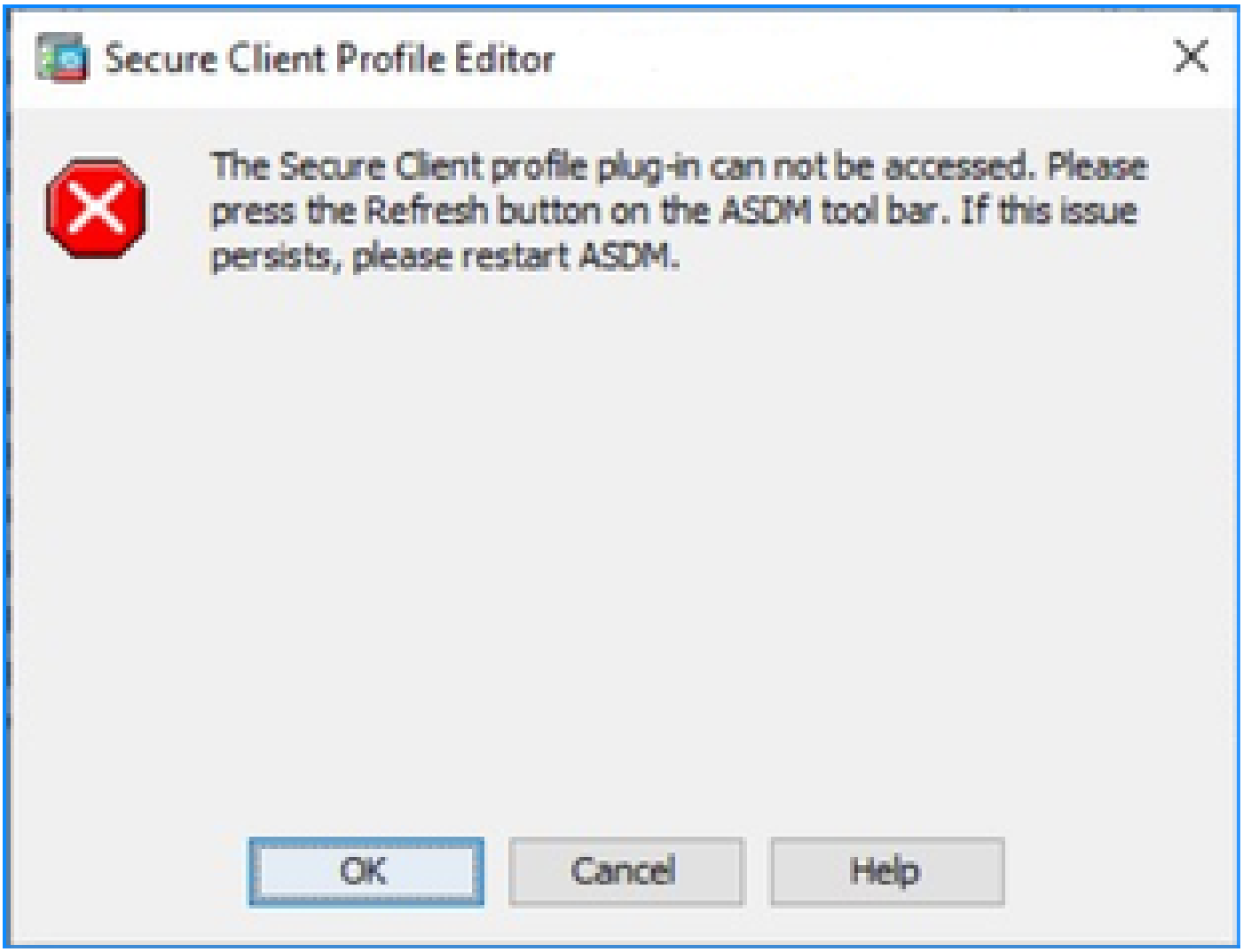
Consulte el ID de bug de software Cisco CSCwf71723 "ASDM perder objetos configurados/grupos de objetos".



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

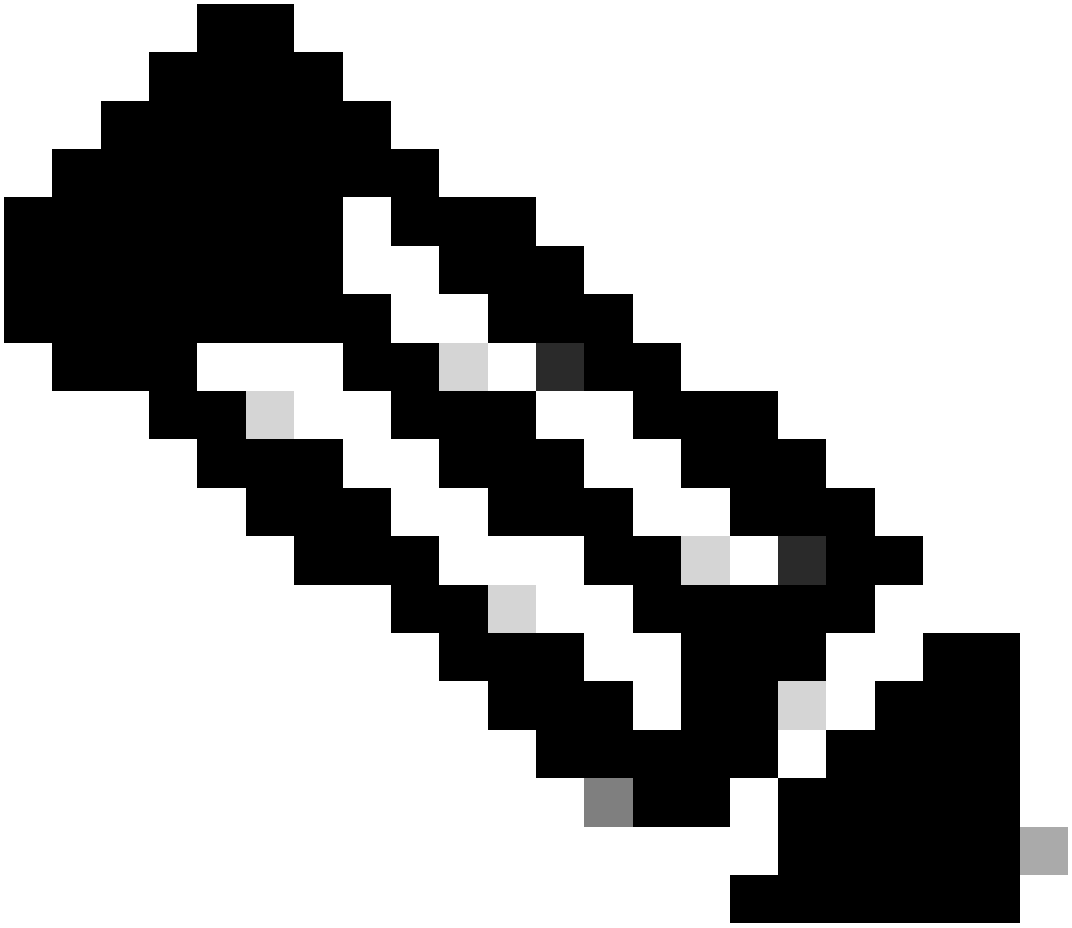
Problema 23. No se pueden editar los perfiles de cliente de AnyConnect para las versiones anteriores a la 4.5

Los perfiles de cliente de AnyConnect no se pueden editar para AnyConnect Profile anterior a la versión 4.5. El mensaje de error es "No se puede acceder al plug-in de perfil de cliente seguro. Pulse el botón Actualizar en la barra de herramientas de ASDM. Si el problema continúa, reinicie ASDM.":



Solución de problemas: acciones recomendadas

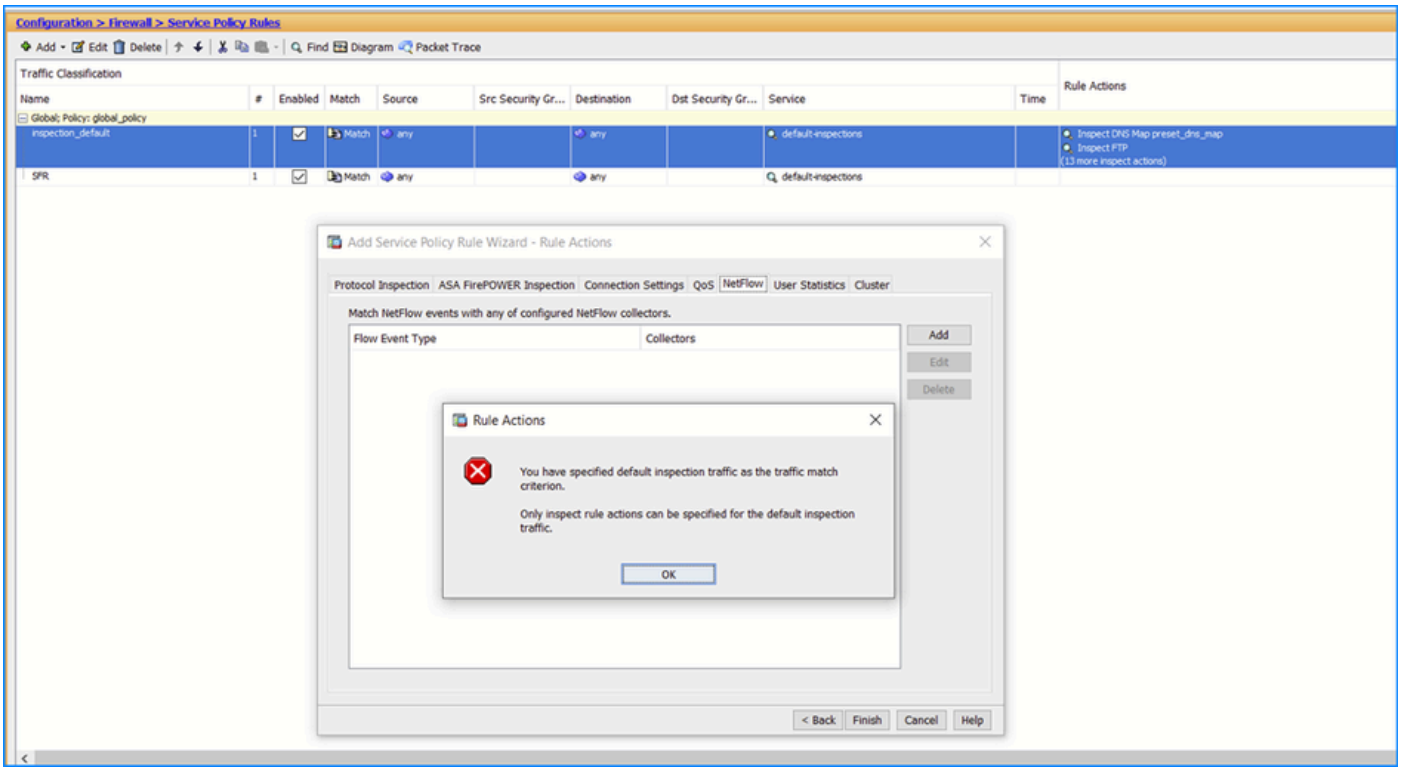
Consulte el software Cisco bug ID CSCwf16947 "ASDM - No se puede cargar Anyconnect Profile Editor".



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

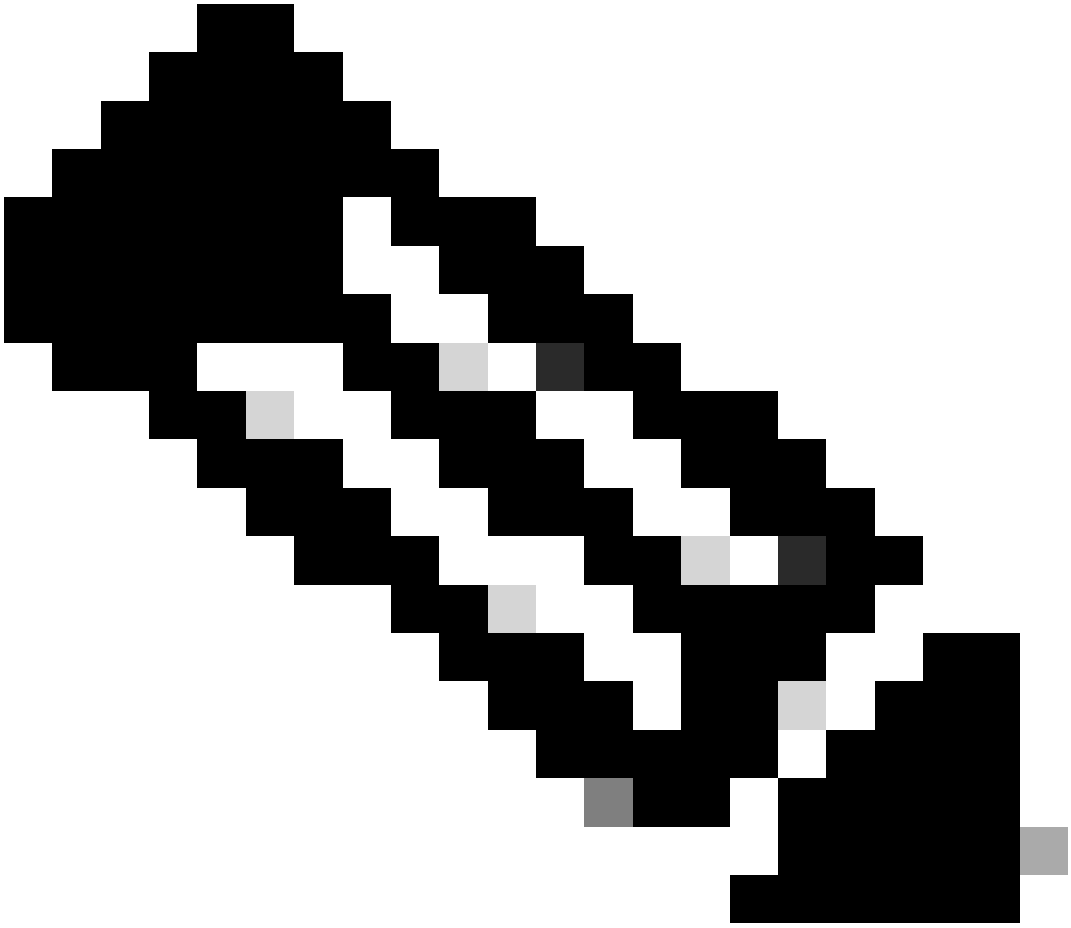
Problema 24. No se puede acceder a la ficha Editar política de servicio > Acciones de regla > Inspección de ASA FirePOWER

En la versión 7.8.2 de ASDM, los usuarios no pueden navegar a la pestaña Edit Service Policy > Rule Actions > ASA FirePOWER Inspection y se muestra el error: "Ha especificado el tráfico de inspección predeterminado como criterio de coincidencia de tráfico. Solo se pueden especificar acciones de regla de inspección para el tráfico de inspección predeterminado." Esto ocurre incluso cuando se ha seleccionado una ACL para la redirección:



Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCvg15782 "ASDM - No se puede ver o modificar el redireccionamiento del tráfico SFR después de actualizar a la versión 7.8(2)". La solución alternativa es utilizar la CLI para editar la configuración de policy-map.



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

Problema 25. AnyConnect Image versión 5.1 y editor de perfiles de AnyConnect en ASDM

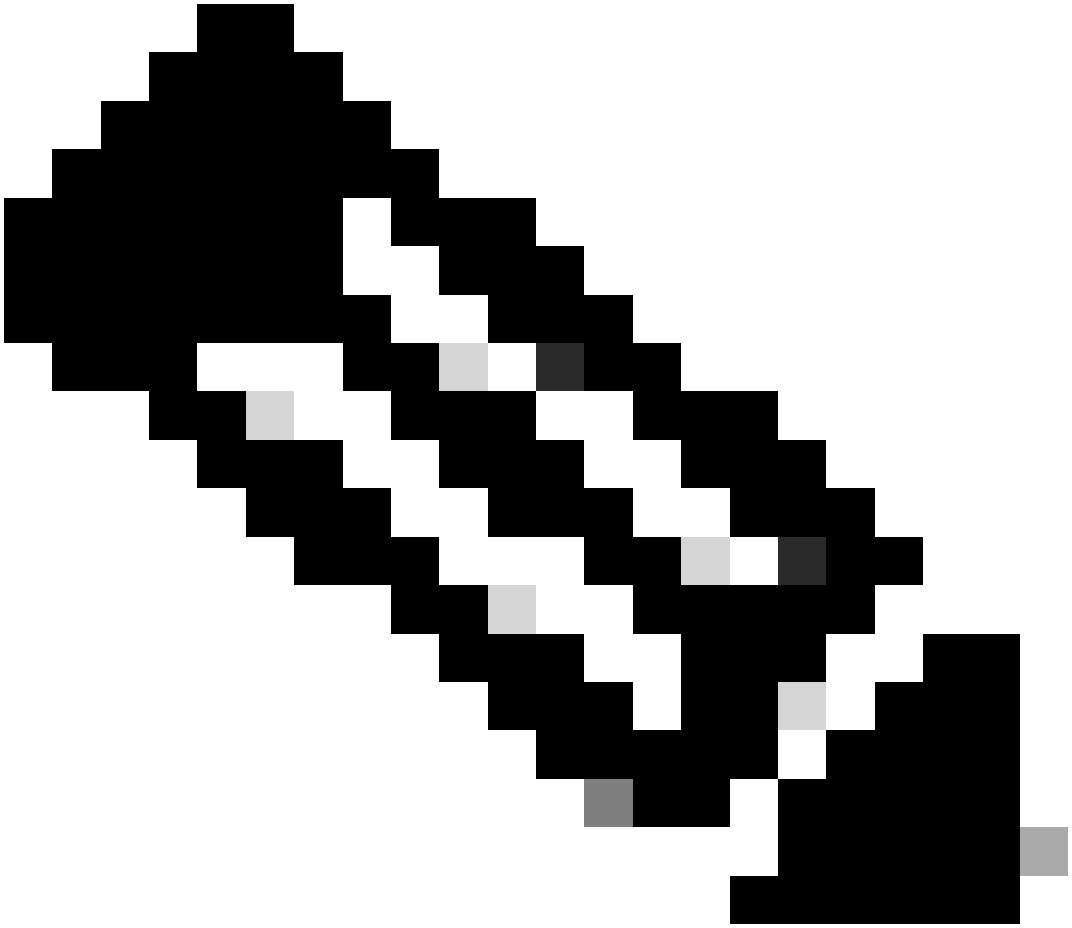
Estos síntomas se observan para la versión 5.1 del software Secure Client:

1. Los nombres de los módulos de políticas de grupo no aparecen al cargar los paquetes Win/Mac/Linux
2. ASDM no puede abrir el Editor de perfiles de AnyConnect.

Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCwh7417 "ASDM : No se pueden cargar el Editor de perfiles

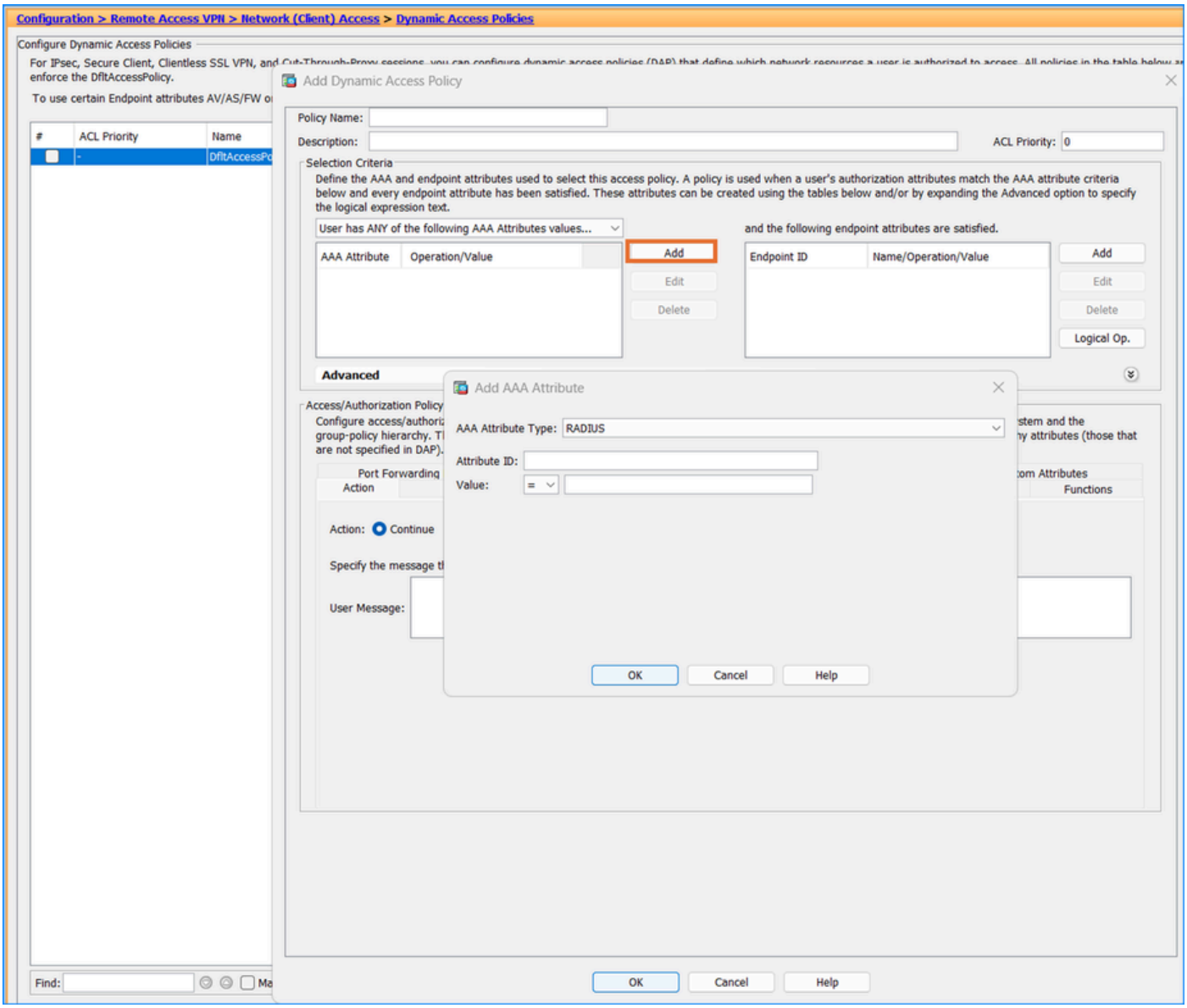
y la Directiva de grupo de AnyConnect cuando se usa la imagen de CSC 5.1". La solución alternativa es utilizar versiones más bajas de Secure Client.



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

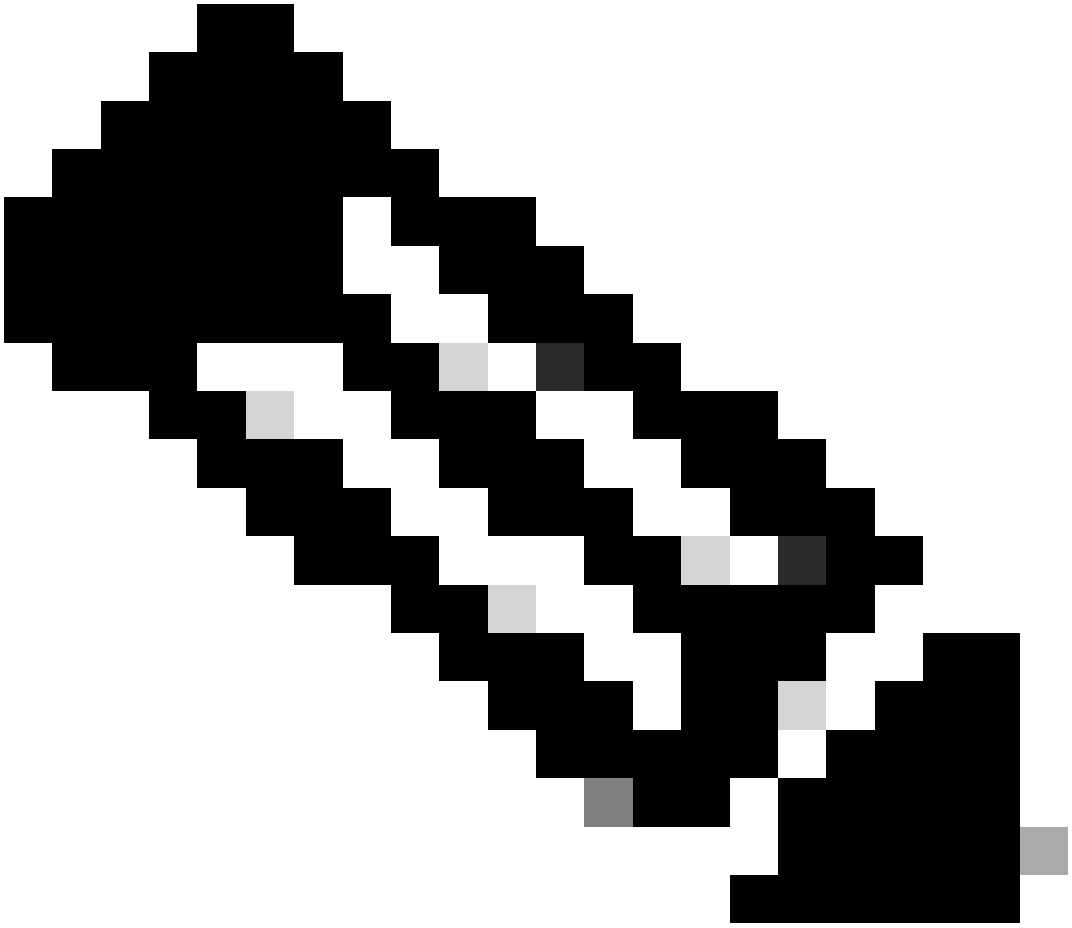
Problema 26. El tipo de atributos AAA (RADIUS/LDAP) no está visible en ASDM

El tipo de atributos AAA (Radius/LDAP) no está visible en ASDM > Configuración > VPN de acceso remoto > Acceso de red (cliente) > Políticas de acceso dinámico<Agregar > En el campo de atributo AAA > Agregar > Seleccionar RADIUS o LDAP:



Solución de problemas: acciones recomendadas

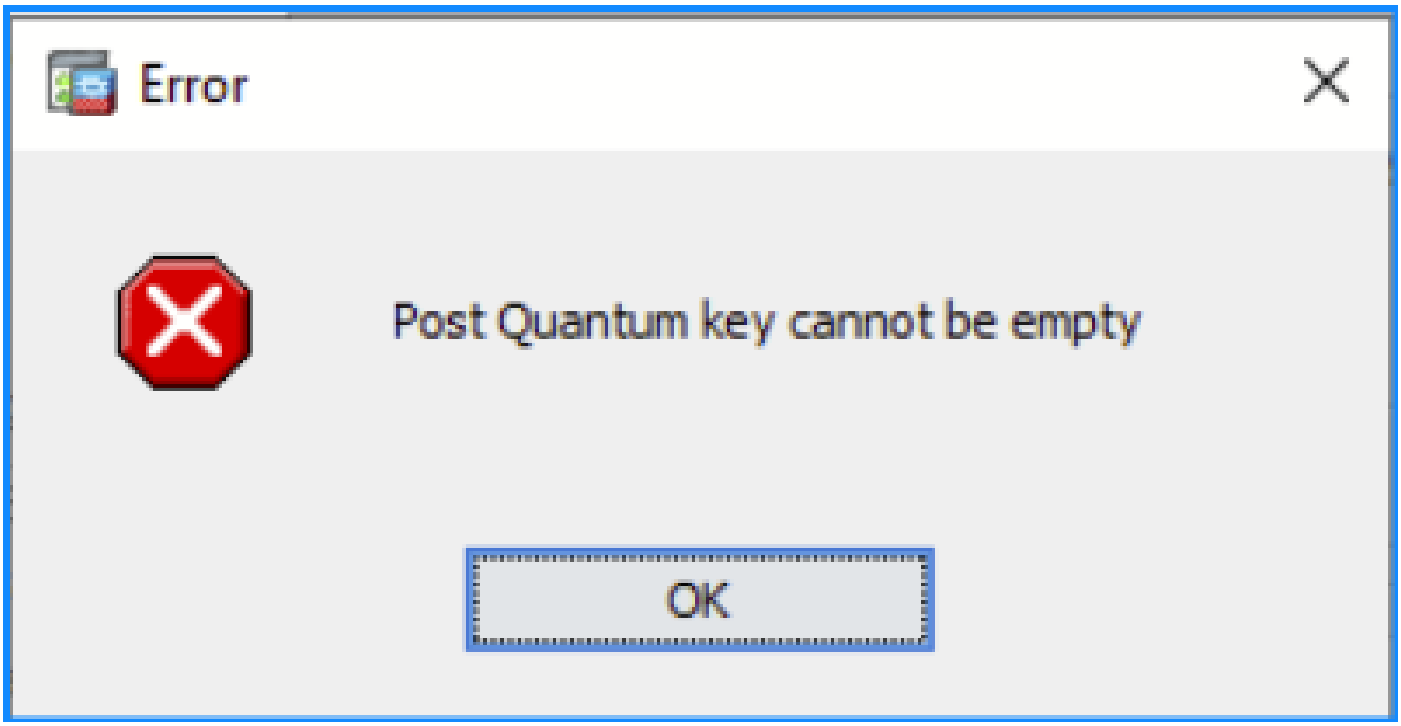
Consulte el software Cisco bug ID CSCwa9370 "ASDM : ASDM:DAP config missing AAA Attributes type (Radius/LDAP)" y Cisco bug ID CSCwd16386 "ASDM:DAP config missing AAA Attributes type (Radius/LDAP)".



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

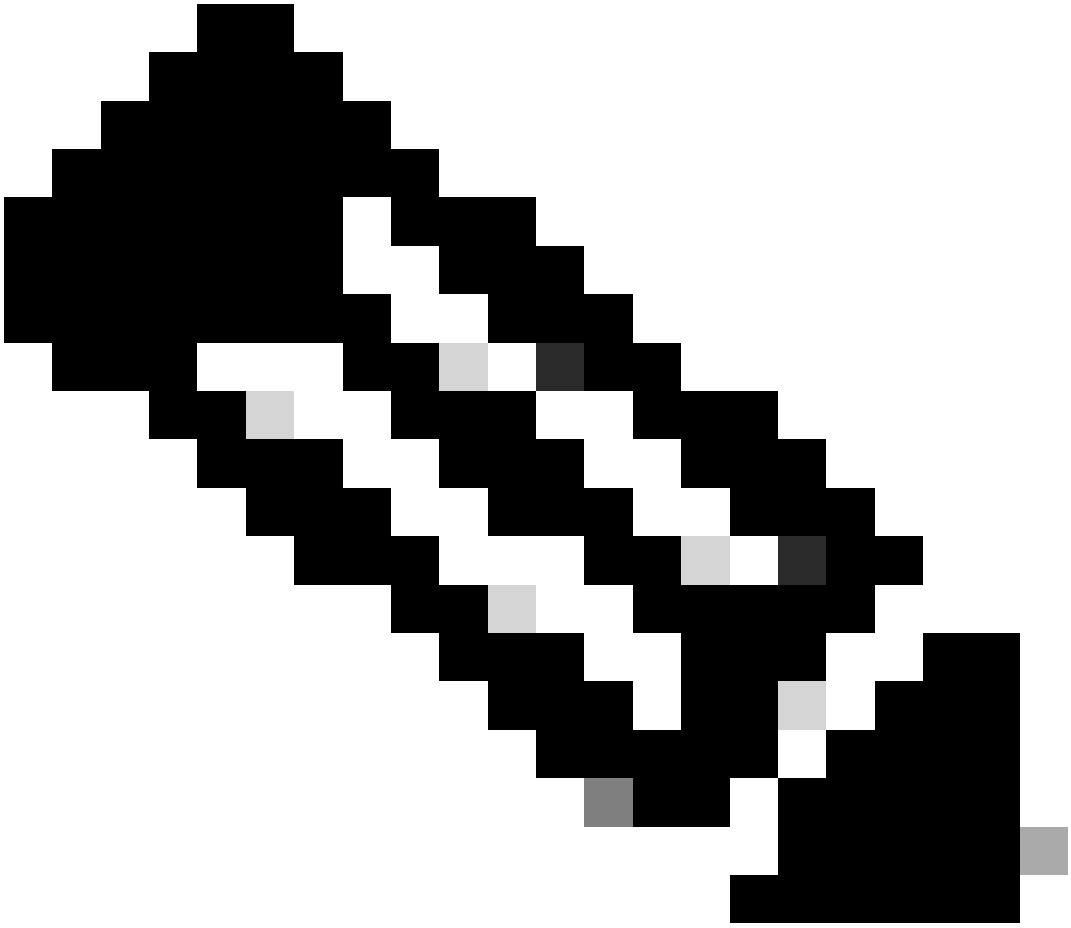
Problema 27. Se muestra el error 'La clave posterior a la cuántica no puede estar vacía' en ASDM

El error 'La clave posterior a la cuántica no puede estar vacía' se muestra al editar la sección Avanzadas en ASDM > Configuración > VPN de acceso remoto > Perfiles de conexión de red (cliente) e IPsec (IKEv2):



Solución de problemas: acciones recomendadas

Consulte el software Cisco bug ID CSCwe58266 "ASDM IKev2 configuration - Post Quantum Key cannot be empty error message".



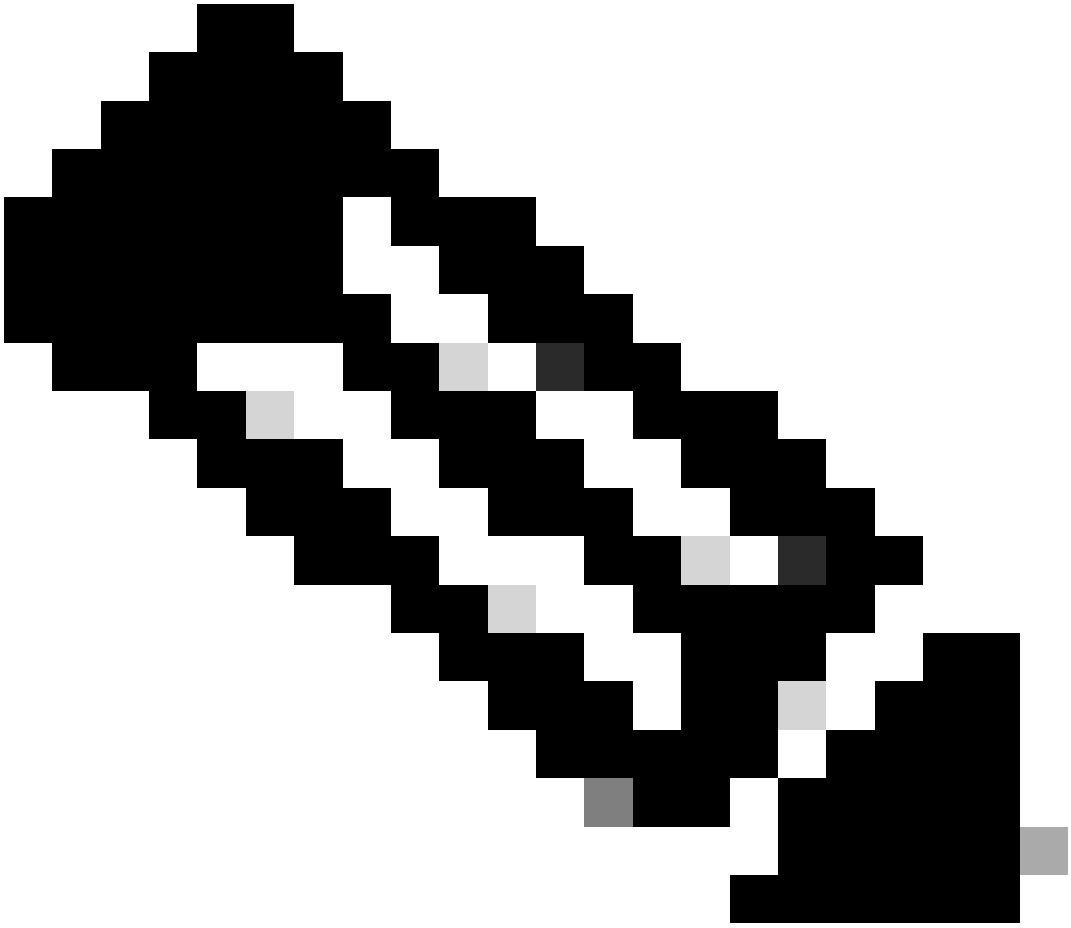
Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Problema 28. ASDM no muestra ningún resultado cuando utiliza la opción "where used"

ASDM no muestra ningún resultado cuando se utiliza la opción "where used" que se encuentra en Configuration > Firewall > Objects > Network Objects/Groups y al hacer clic con el botón derecho del ratón en un objeto.

Solución de problemas: acciones recomendadas

Consulte la opción "Where used" (Uso) de la opción CSCwd98702 "Where used" (Uso) en ASDM not working (ASDM no funciona) del software de ID de bug Cisco.



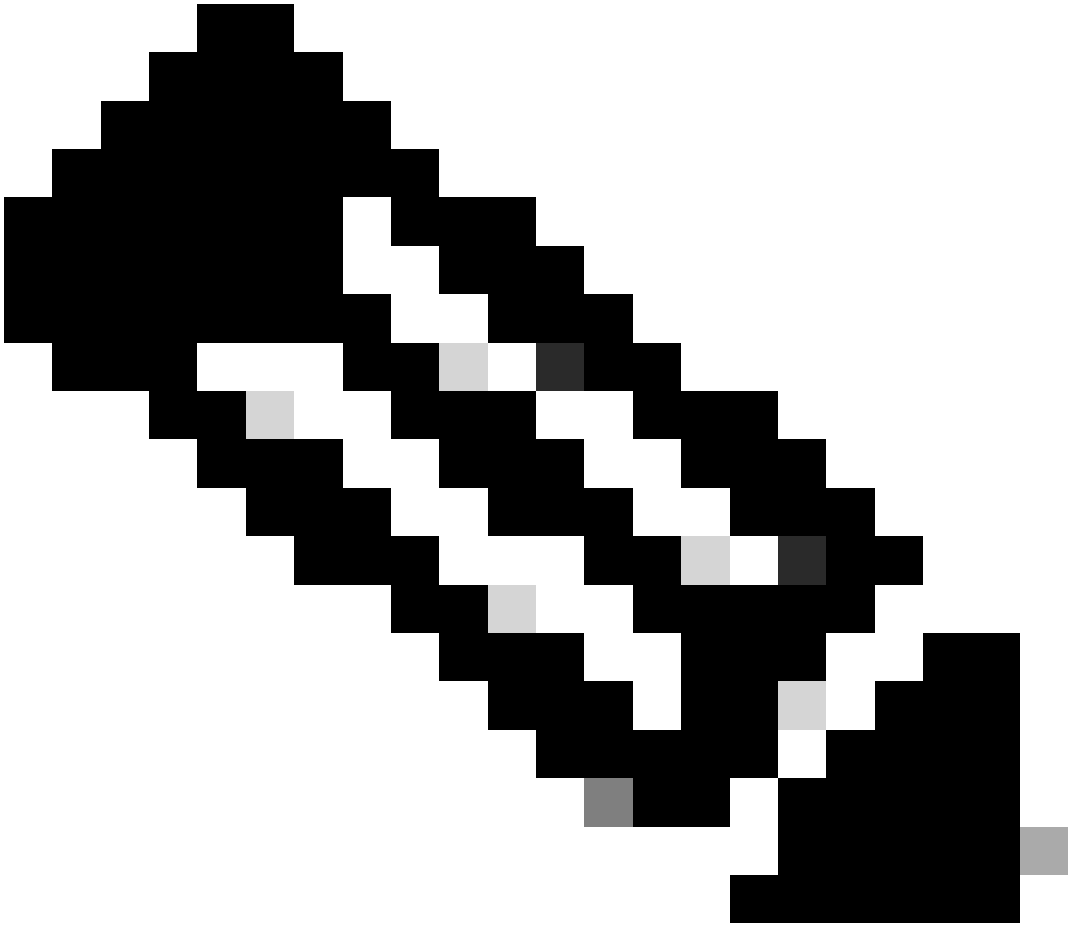
Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

Problema 29. El mensaje de advertencia "[Objeto de red] no se puede eliminar porque se utiliza en los siguientes elementos" al eliminar un objeto de red

ASDM no muestra el mensaje de advertencia "[Objeto de red] no se puede eliminar porque se utiliza en lo siguiente" cuando se elimina un objeto de red al que se hace referencia en un grupo de red en Configuración > Firewall > Objetos > Network Objects/Groups.

Solución de problemas: acciones recomendadas

Consulte el ID de bug de software Cisco CSCwe67056 "[Objeto de red] no se puede eliminar porque se utiliza en la siguiente advertencia" no aparece".



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

Problema 30. Problemas de usabilidad con la ficha Network Objects/Group en ASDM

Se observan uno o más de estos síntomas:

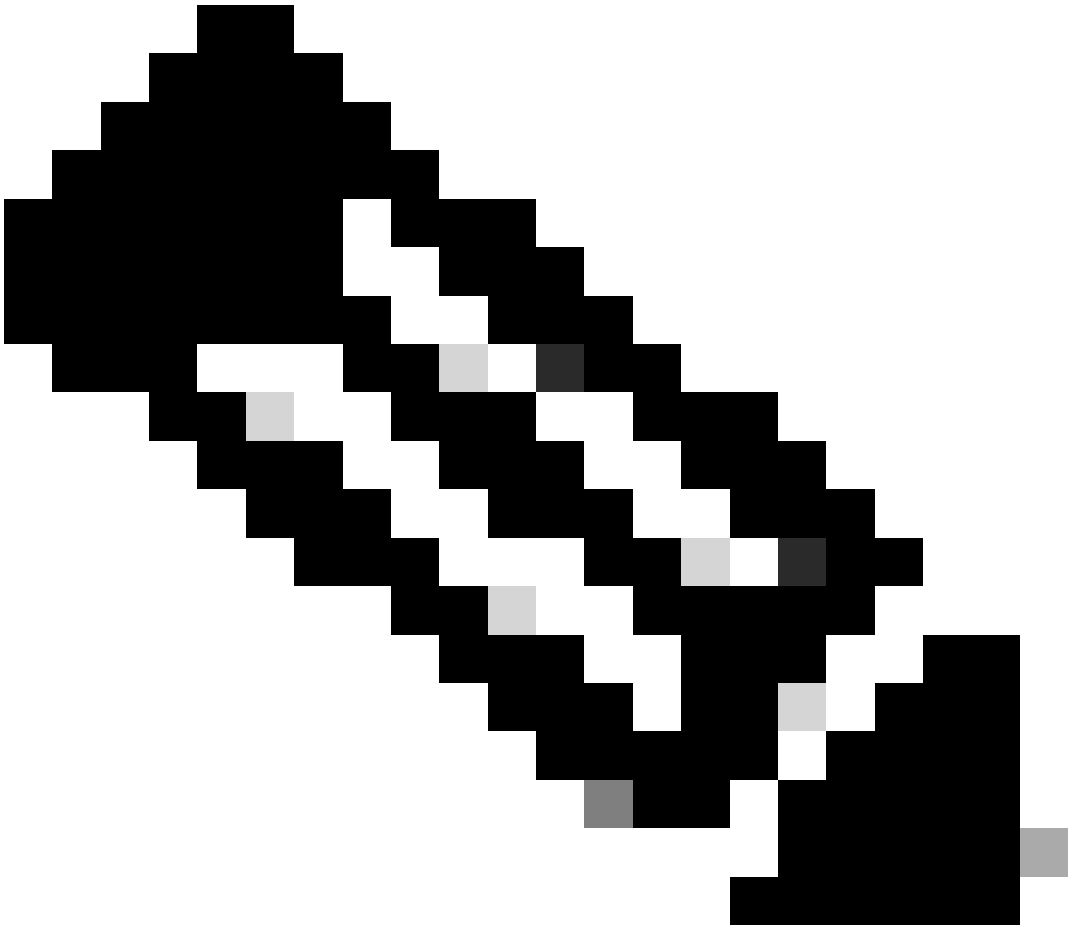
- La entrada de texto "Nombre" de la sección "Crear nuevo miembro de objeto" de "Agregar/editar ventanas de grupo de objetos" se marca como "opcional". Sin embargo, el botón "Agregar>>" para crear y agregar el objeto está deshabilitado a menos que se especifique un nombre.
- La ficha "Usos" que se abre cuando un usuario hace clic en la opción "Uso..." El menú contextual sólo enumera las entidades (ACL, mapas de ruta, grupos de objetos) que hacen referencia directamente al objeto. También debe enumerar recursivamente segundo, tercero, etc. Referencias de orden (es decir, una ACL que utiliza un grupo de objetos que

contiene un objeto también debe aparecer como "uso" del objeto).
- La operación "Eliminar" disponible en el menú contextual también muestra este comportamiento. Elimina automáticamente cualquier entidad que haga referencia directa al objeto (si la entidad quedaría vacía al eliminar el objeto). No funciona de esta manera cuando un segundo, un tercero, etc. order reference quedaría vacía al eliminar el objeto y la primera referencia de orden.

Se puede hacer creer al usuario que el ASDM evita que las entidades que quedarían vacías debido a la eliminación de objetos del resto de la configuración. Sin embargo, esto no es necesariamente así.

Solución de problemas: acciones recomendadas

Consulte la identificación de error de software Cisco CSCwe86257 "Usabilidad de la ficha Network Objects/Group en ASDM".



Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte

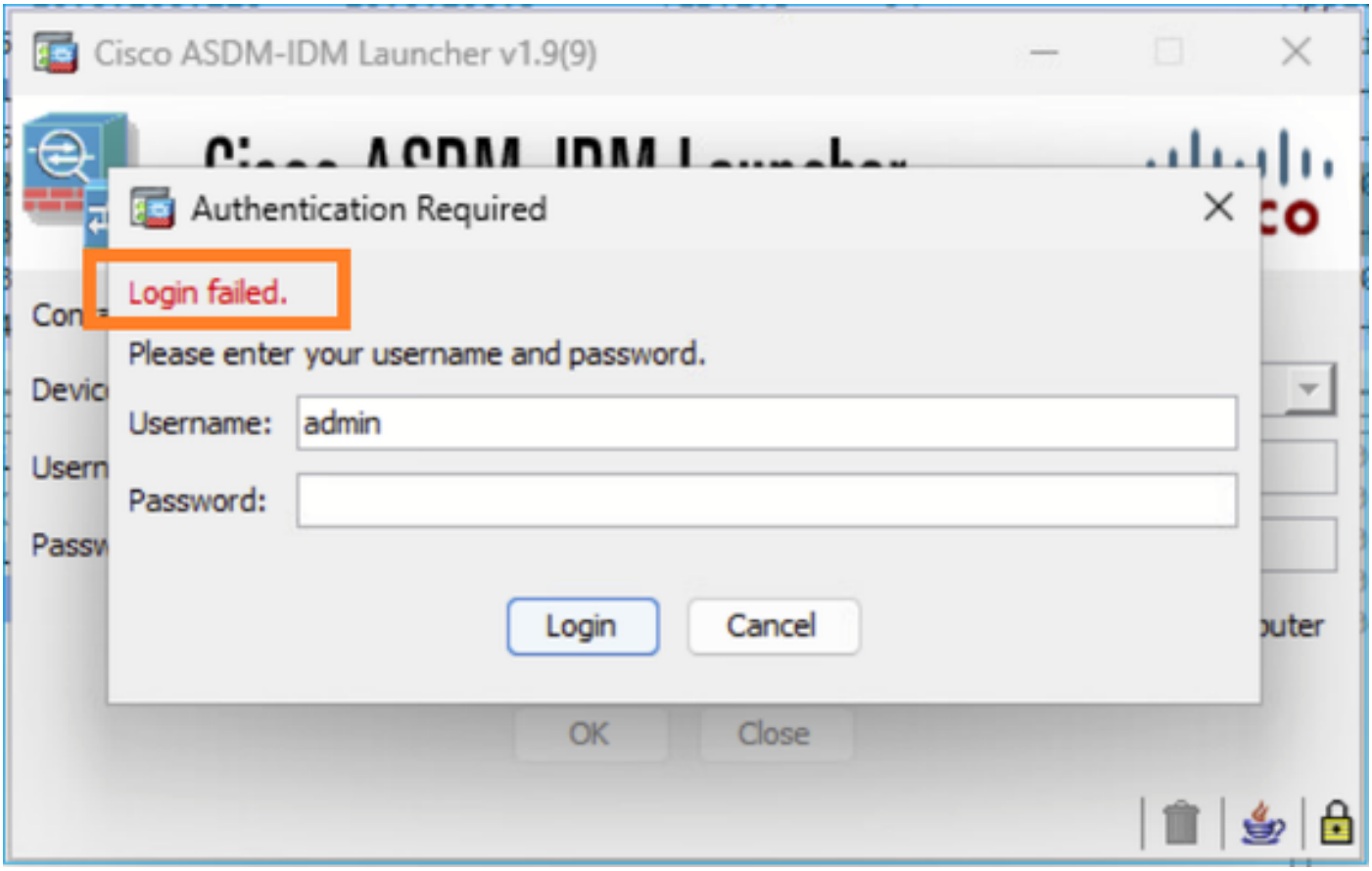
---

los detalles del defecto para obtener más información.

Resolución de Problemas de Autenticación ASDM

Problema 1. Error de inicio de sesión de ASDM

El error que se muestra en la IU de ASDM es:



Solución de problemas: acciones recomendadas

Este error se puede ver cuando tiene HTTP y Webvpn Cisco Secure Client (AnyConnect) habilitados en la misma interfaz. Por lo tanto, deben cumplirse todas las condiciones:

1. AnyConnect/Cisco Secure Client está activado en una interfaz
2. El servidor HTTP está habilitado en la misma interfaz y en el mismo puerto que AnyConnect/Cisco Secure Client

Ejemplo:

<#root>

```
asa#
configure terminal
```

```
asa(config)#
webvpn

asa(config-webvpn)#
enable outside  <-
 default port in use (443)

and
asa(config)#
http server enable
 <-
 default port in use (443)

asa(config)#
http 0.0.0.0 0.0.0.0 outside
 <- HTTP server configured on the same interface as Webvpn
```

Sugerencia de solución de problemas: Habilite 'debug http 255' y podrá ver el conflicto entre ASDM y Webvpn:

<#root>

```
ciscoasa#
debug http 255

debug http enabled at level 255.
ciscoasa# ewaURLHookVCARedirect
...addr: 192.0.2.5
ewaURLHookHTTPRedirect: url = /+webvpn+/index.html
HTTP: ASDM request detected [ASDM/] for [/+webvpn+/index.html]   <--------

webvpnhook: got '/+webvpn+' or '/+webvpn+/': Sending back "/+webvpn+/index.html"    <-----

HTTP 200 OK (192.0.2.110)HTTP: net_handle->standalone_client [1]
webvpn_admin_user_agent: buf: ASDM/ Java/1.8.0_431
ewsStringSearch: no buffer
Close 0
```

Como nota al margen, a pesar de la falla de login, los syslogs de ASA muestran que la Autenticación es exitosa:

<#root>

asa#

show logging

Oct 28 2024 07:42:44: %ASA-6-113012: AAA user authentication Successful : local database : user = user2
Oct 28 2024 07:42:44: %ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user
Oct 28 2024 07:42:44: %ASA-6-113008: AAA transaction status ACCEPT : user = user2
Oct 28 2024 07:42:44: %ASA-6-605005: Login permitted from 192.0.2.110/60316 to NET50:192.0.2.5/https fo
Oct 28 2024 07:42:44: %ASA-6-611101:

User authentication succeeded: IP address: 192.0.2.110, Uname: user2

Soluciones alternativas

Solución alternativa 1

Cambie el puerto TCP para el servidor HTTP ASA, por ejemplo:

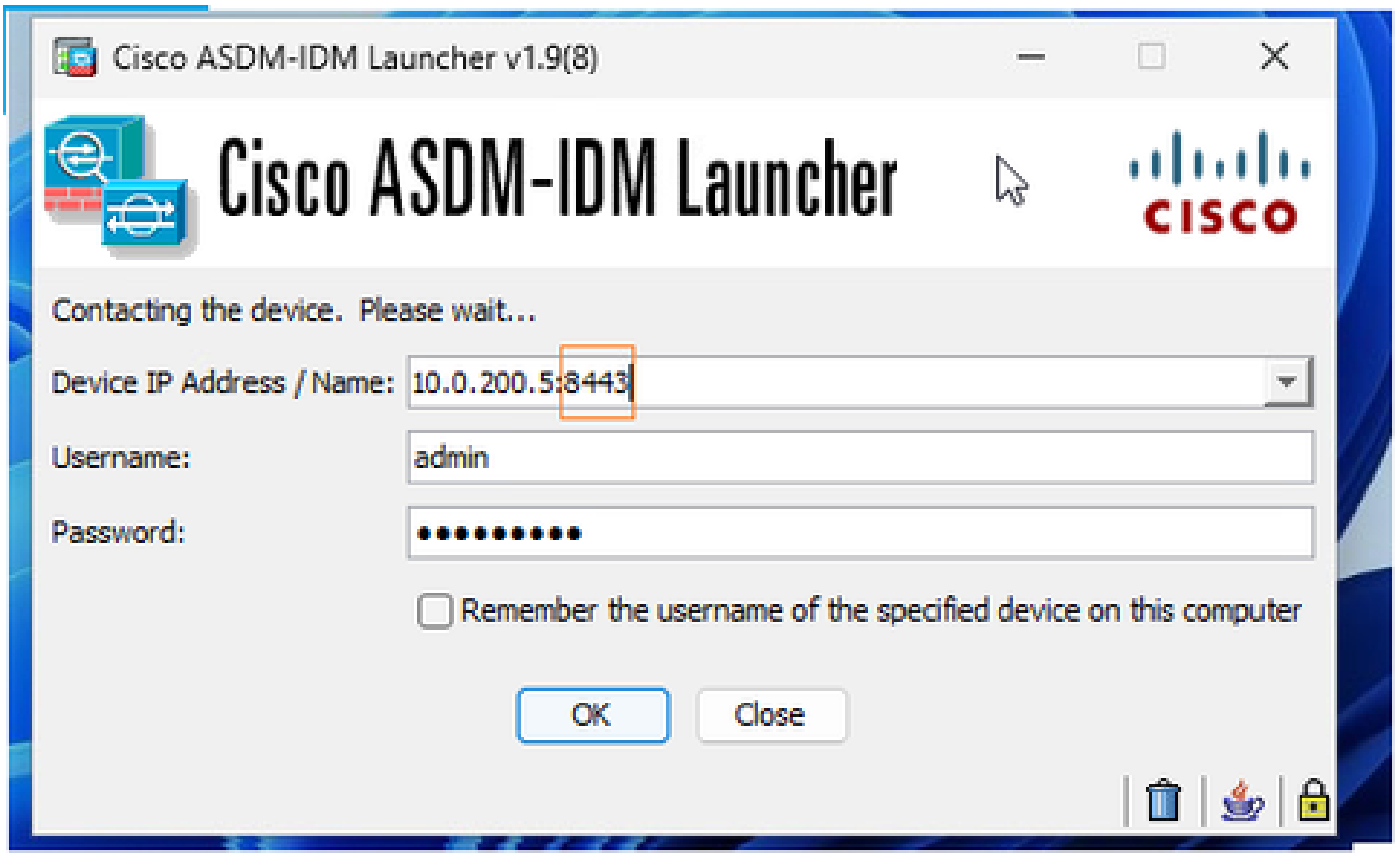
<#root>

ciscoasa#

configure terminal

ciscoasa(config)#

http server enable 8443



Solución alternativa 2

Cambie el puerto TCP para AnyConnect/Cisco Secure Client, por ejemplo:

<#root>

```
ciscoasa#
configure terminal

ciscoasa(config)#
webvpn

ciscoasa(config-webvpn)#
no enable outside
 <-- first you have disable WebVPN for all interfaces before changing the port
ciscoasa(config-webvpn)#
port 8443

ciscoasa(config-webvpn)#
enable outside
```

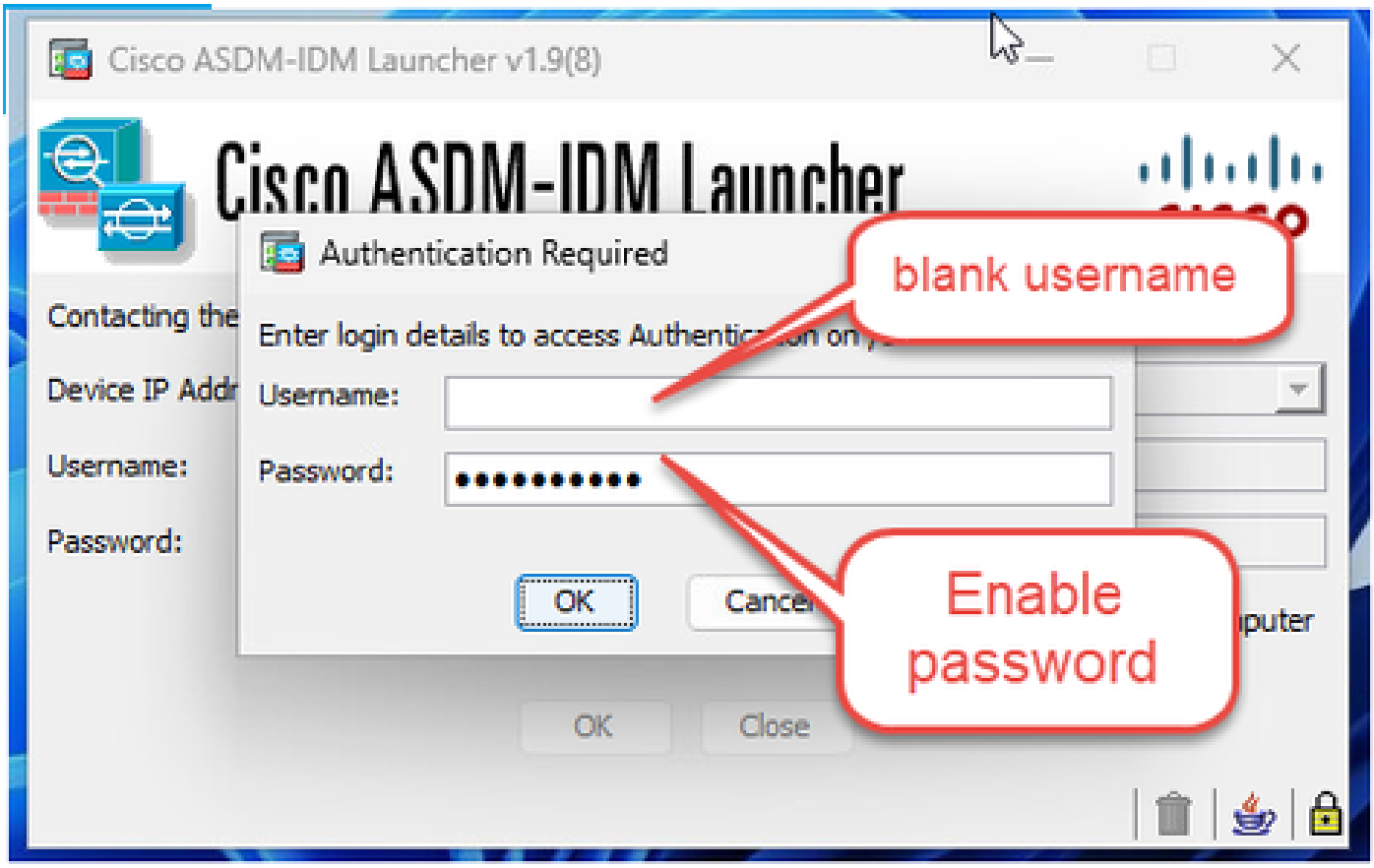
Solución alternativa 3

Una solución alternativa es eliminar la configuración "aaa authentication http console":

<#root>

```
ciscoasa(config)#
no aaa authentication http console LOCAL
```

En este caso, puede iniciar sesión en el ASDM usando la contraseña de habilitación:



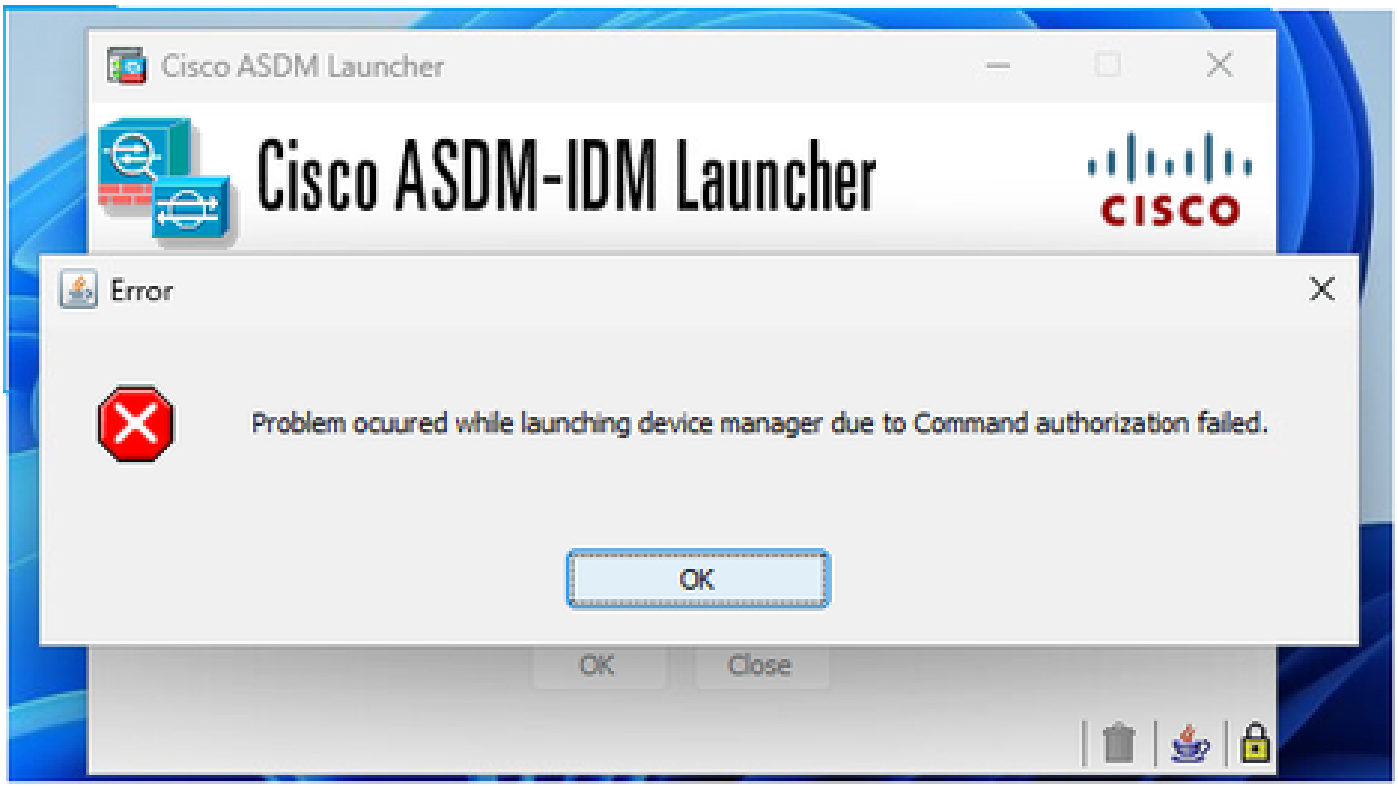
Defecto relacionado

ID de bug de Cisco CSCwb67583

Agregar advertencia cuando webvpn y ASDM están habilitados en la misma interfaz

Problema 2. Error en la autorización del comando ASDM

El error que se muestra en la IU de ASDM es:



Solución de problemas: pasos recomendados

Compruebe su configuración AAA en ASA y asegúrese de que:

- También tiene configurada la autenticación aaa.
- Si utiliza un servidor de autenticación remoto, es accesible y autoriza los comandos.

Referencia

https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-local.html

Problema 3. Configuración del acceso de solo lectura ASDM

A veces desea proporcionar acceso de sólo lectura a los usuarios de ASDM.

Solución de problemas: pasos recomendados

Cree un nuevo usuario con un nivel de privilegio personalizado (5), por ejemplo:

<#root>

```
asa(config)#
```

username [username] password [password] privilege 5

Este comando crea un usuario con un nivel de privilegio de 5, que es el nivel "solo supervisión". Sustituya `[username]` y `[password]` por el nombre de usuario y la contraseña deseados.

Detalles

La autorización de comandos local le permite asignar comandos a uno de los 16 niveles de privilegio (de 0 a 15). Por defecto, cada comando se asigna al nivel de privilegio 0 o 15. Puede definir cada usuario para que se encuentre en un nivel de privilegio específico, y cada usuario puede introducir cualquier comando en el nivel de privilegio asignado o menos. ASA admite niveles de privilegios de usuario definidos en la base de datos local, un servidor RADIUS o un servidor LDAP (si asigna atributos LDAP a atributos RADIUS).

Procedimiento

Paso 1	Elija Configuration > Device Management > Users/AAA > AAA Access > Authorization.
Paso 2	Marque la casilla de verificación Enable authorization for ASA command access > Enable.
Paso 3	Elija LOCAL en la lista desplegable Server Group.
Paso 4	Cuando habilita la autorización de comandos local, tiene la opción de asignar manualmente niveles de privilegio a comandos o grupos de comandos individuales o de habilitar los privilegios de cuenta de usuario predefinidos. · Haga clic en Set ASDM Defined User Roles para utilizar privilegios de cuenta de usuario predefinidos. Aparece el cuadro de diálogo Configuración de Roles de Usuario Definidos por ASDM. Haga clic en Sí para utilizar los privilegios de cuenta de usuario predefinidos: Admin (nivel de privilegio 15), con acceso completo a todos los comandos CLI; Sólo lectura (nivel de privilegio 5, con acceso de sólo lectura); y Sólo supervisión (nivel de privilegio 3, con acceso únicamente a la sección Supervisión). · Haga clic en Configure Command Privileges para configurar manualmente los niveles de comando. Aparece el cuadro de diálogo Configuración de Privilegios de Comando. Puede ver todos los comandos eligiendo All Modes de la lista desplegable Command Mode, o puede elegir un modo de configuración para ver los comandos disponibles en ese modo. Por ejemplo, si elige el contexto, puede ver todos los comandos disponibles en el modo de configuración de contexto. Si se puede ingresar un comando en el modo EXEC de usuario o en el modo EXEC privilegiado, así como en el modo de configuración, y el comando realiza diferentes acciones en cada modo, puede establecer el nivel de privilegio para estos modos por separado.

	La columna Variant muestra show, clear o cmd. Sólo puede establecer el privilegio para la forma show, clear o configure del comando. La forma de configuración del comando suele ser la forma que provoca un cambio de configuración, ya sea como el comando no modificado (sin el prefijo show o clear) o como el comando no form. Para cambiar el nivel de un comando, haga doble clic en él o haga clic en Editar. Puede establecer el nivel entre 0 y 15. Sólo puede configurar el nivel de privilegio del comando principal. Por ejemplo, puede configurar el nivel de todos los comandos aaa, pero no el nivel del comando aaa authentication y el comando aaa authorization por separado. Para cambiar el nivel de todos los comandos que aparecen, haga clic en Seleccionar todo y, a continuación, en Editar. Haga clic en Aceptar para aceptar los cambios.
Paso 5	Haga clic en Apply (Aplicar). Se asigna la configuración de autorización y los cambios se guardan en la configuración en ejecución.

Referencia

https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/asdm722/general/asdm-722-general-config/admin-management.html#ID-2111-00000650

Problema 4. Autenticación multifactor (MFA) de ASDM

Solución de problemas: pasos recomendados

En el momento de escribir este documento, ASDM no admite MFA (o 2FA). Esta limitación incluye MFA con soluciones como PingID, etc.

Referencia

ID de bug de Cisco CSCvs85995

ENH: Acceso ASDM con autenticación de dos factores o MFA

Problema 5. Configuración de autenticación externa de ASDM

Solución de problemas: pasos recomendados

Puede utilizar LDAP, RADIUS, RSA SecurID o TACACS+ para configurar la autenticación externa en ASDM.

Referencias

- https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-

firewalls/112967-acs-aaa-tacacs-00.html

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-radius.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-tacacs.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-ldap.html

Problema 6. La autenticación LOCAL de ASDM falla

Solución de problemas: pasos recomendados

En caso de que utilice la autenticación externa y la autenticación LOCAL como alternativa, la autenticación local sólo funciona si el servidor externo está inactivo o no funciona. Solo en este escenario la autenticación LOCAL toma el control y usted puede conectarse con los usuarios LOCALES.

Esto se debe a que la autenticación externa tiene prioridad sobre la autenticación LOCAL.

Ejemplo:

<#root>

```
asa(config)# aaa authentication ssh console RADIUS_AUTH LOCAL
```

Referencia

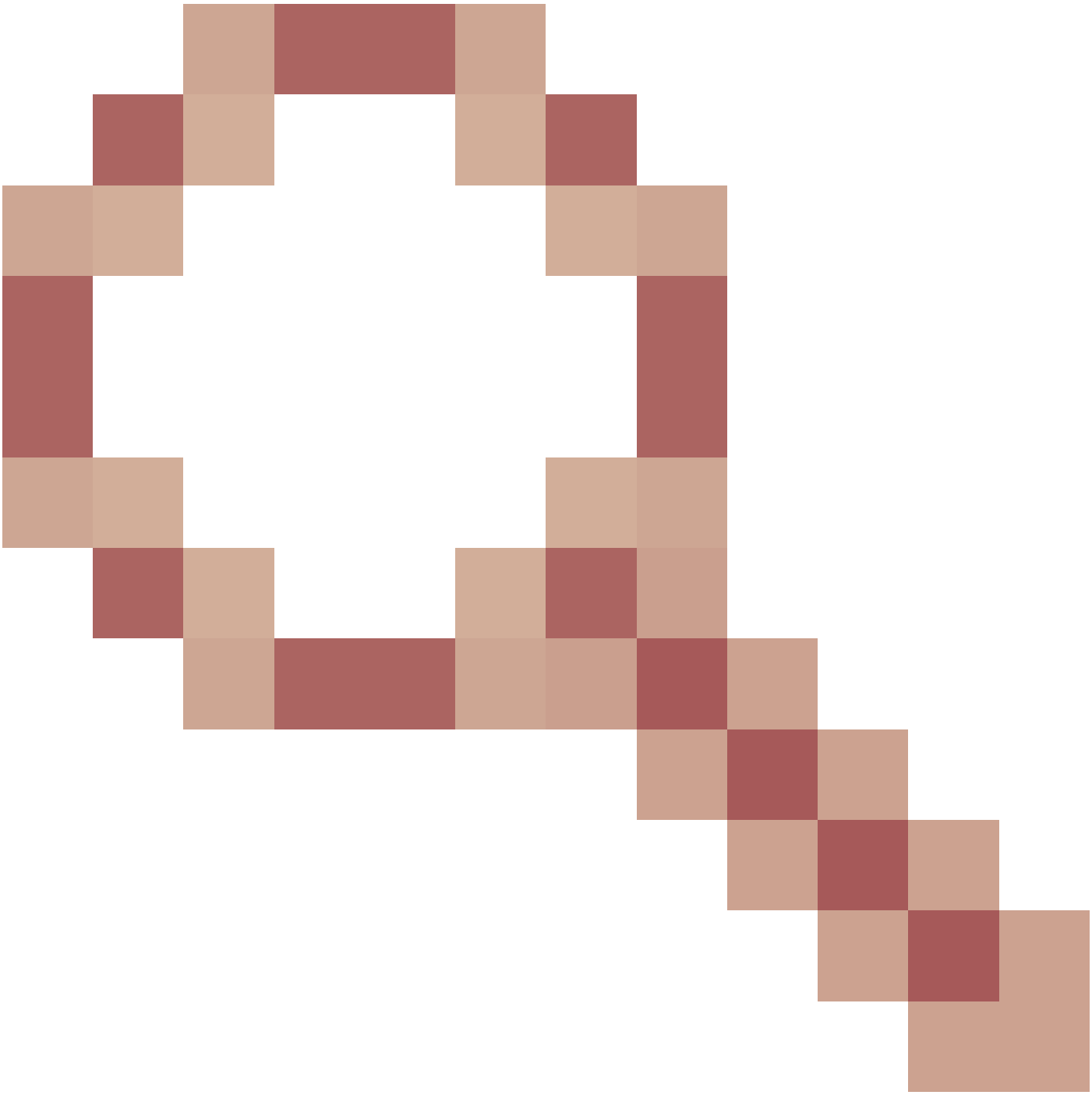
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

Problema 7. Contraseña de un solo uso de ASDM

Solución de problemas: pasos recomendados

- El soporte de autenticación OTP (contraseña de un solo uso) de ASDM fue agregado en ASA versión 8.x - 9.x y en modo de un solo enrutamiento.
- La autenticación OTP de ASDM para el modo transparente y/o el modo multicontexto del firewall ASA no entra en esta categoría.

Consulte el ID de bug de Cisco CSCtf23419



ENH: Compatibilidad con autenticación OTP de ASDM en modos transparente y multicontexto

Problema 8. El perfil de conexión no muestra todos los métodos

El problema en este caso es una discordancia entre la configuración de ASA CLI y la interfaz de usuario de ASDM.

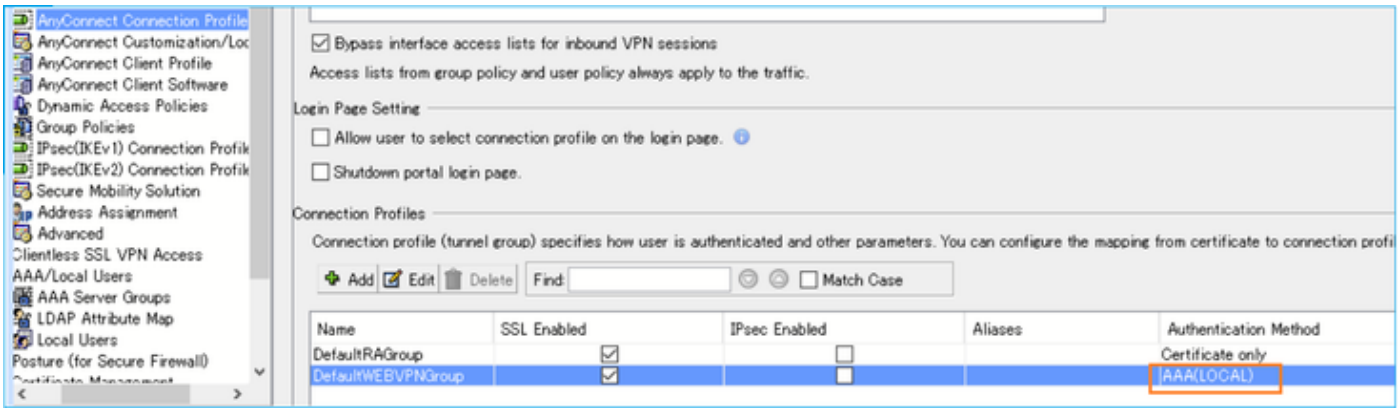
Específicamente, la CLI tiene:

<#root>

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
```

```
 authentication aaa certificate
```

Mientras que la interfaz de usuario de ASDM no menciona el método de certificado:



Solución de problemas: pasos recomendados

Este problema es cosmético. El método no aparece en ASDM, pero se utiliza la autenticación de certificado.

Problema 9. La sesión ASDM no agota el tiempo de espera

El síntoma es que el tiempo de espera de la sesión GUI de ASDM no se tiene en cuenta.

Solución de problemas: pasos recomendados

Esto ocurre cuando el comando "aaa authentication http console LOCAL" no se configura en el ASA administrado.

Consulte el ID de bug de Cisco CSCwj70826

ENH: agregar una advertencia: configurar el tiempo de espera de sesión, requiere "aaa authentication http console LOCAL"

Solución Aternativa

Configure el comando ""aaa authentication http console LOCAL" en el ASA administrado.

Problema 10. La autenticación LDAP de ASDM falla

Solución de problemas: pasos recomendados

Paso 1

Asegúrese de que la configuración esté en su lugar, por ejemplo:

<#root>

```
aaa-server ldap_server protocol ldap
aaa-server ldap_server (inside) host 192.0.2.1
 ldap-base-dn OU=ldap_ou,DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute cn
 ldap-login-password *****
 ldap-login-dn CN=example, DC=example,DC=com
 server-type microsoft
asa(config)#
```

aaa authentication http console ldap_server LOCAL

Paso 2

Verifique el estado del servidor LDAP:

<#root>

```
asa#
```

show aaa-server

Buen escenario:

<#root>

```
Server status:
```

ACTIVE

```
, Last transaction at 11:45:23 UTC Tue Nov 19 2024
```

Escenario incorrecto:

<#root>

```
Server status:
```

FAILED

```
, Server disabled at 11:45:23 UTC Tue Nov 19 2024
```

Paso 3

Verifique que la autenticación LOCAL funcione correctamente inhabilitando temporalmente la autenticación LDAP.

Paso 4

En ASA ejecute los debugs LDAP e intente autenticar al usuario:

<#root>

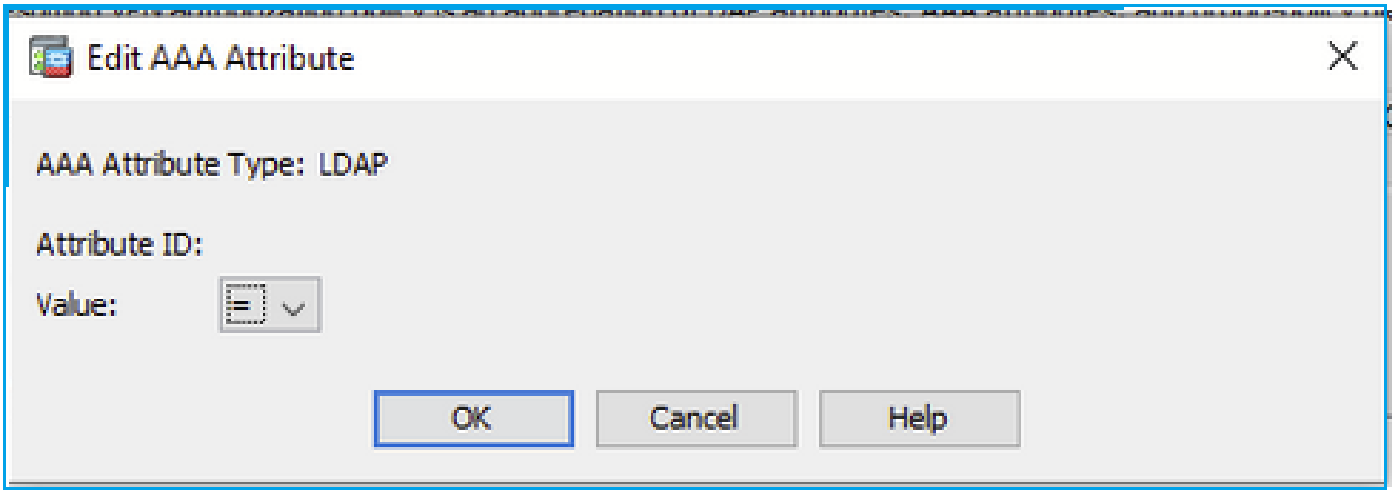
```
#
```

debug ldap 255

En las depuraciones, busque líneas que contengan sugerencias como "Failed".

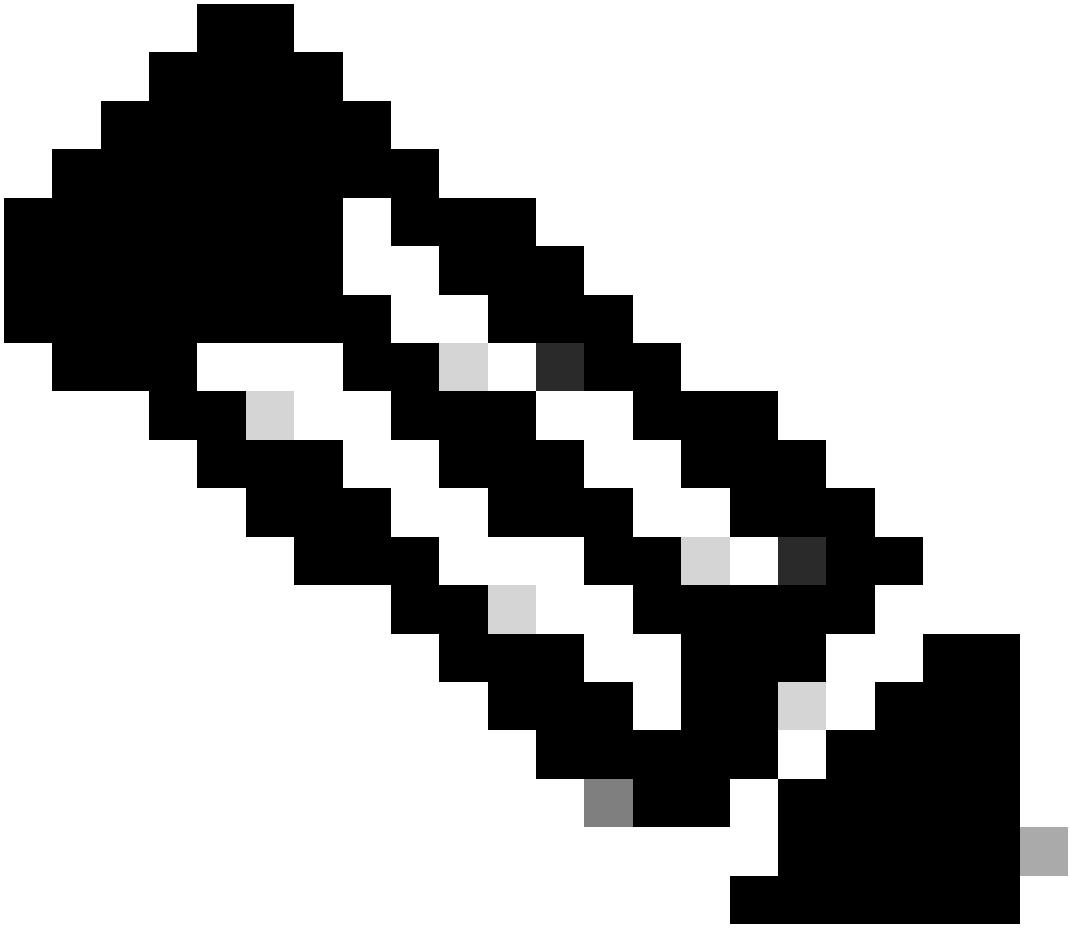
Problema 11. Falta la configuración de ASDM Webvpn DAP

En la configuración de DAP en el tipo de atributos AAA de ASDM (Radius/LDAP) no son visibles solo viendo = y != en el menú desplegable:



Solución de problemas: pasos recomendados

Este es un defecto de software rastreado por el ID de bug de Cisco CSCwa99370
ASDM:configuración DAP sin tipo de atributos AAA (Radius/LDAP)

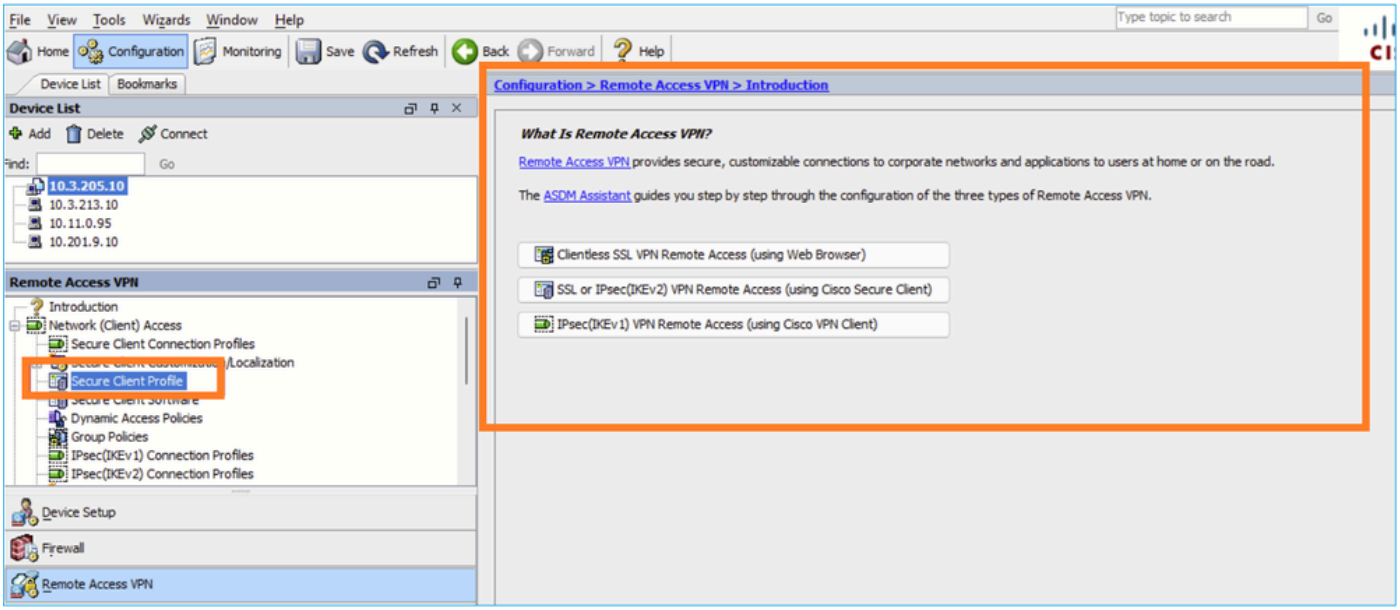


Nota: Este defecto se ha corregido en las últimas versiones del software ASDM. Consulte los detalles del defecto para obtener más información.

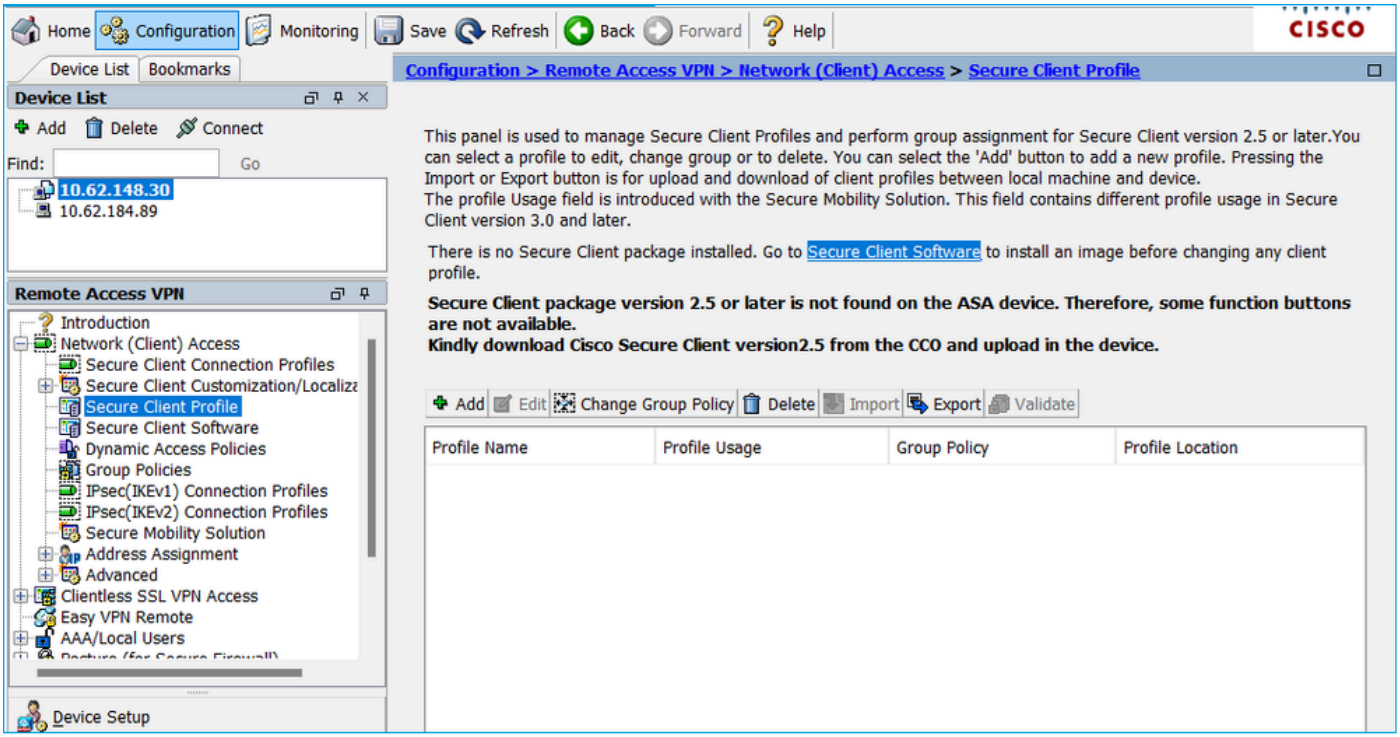
Solución de otros problemas de ASDM

Problema 1. No se puede acceder al perfil de cliente seguro en ASDM

La interfaz de usuario de ASDM muestra lo siguiente:



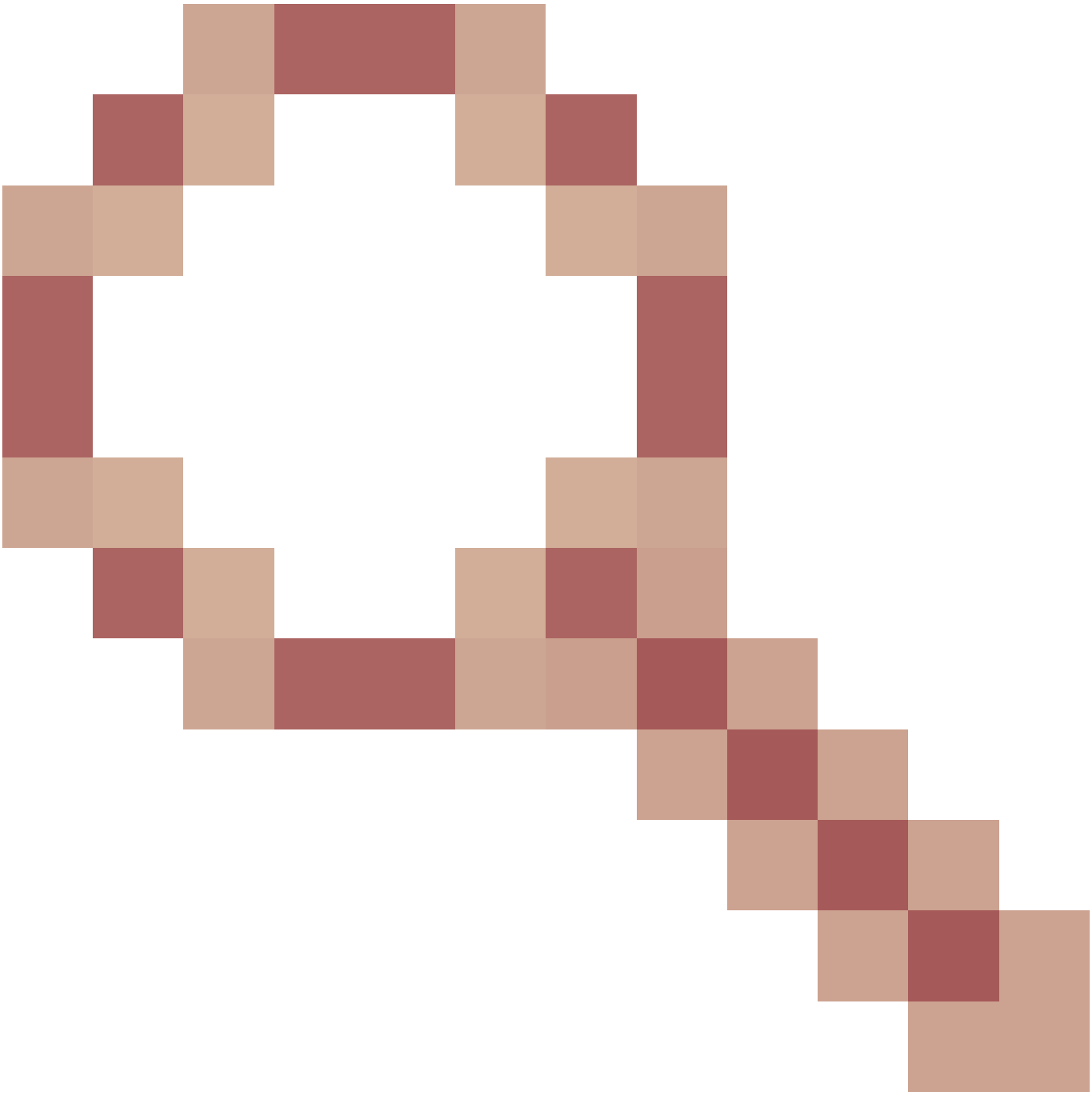
Mientras que el resultado esperado de la interfaz de usuario es:



Solución de problemas: pasos recomendados

Este es un defecto conocido:

ID de bug de Cisco CSCwi56155



No se puede acceder al perfil de cliente seguro en ASDM

Soluciones alternativas:

Reducir nivel de AnyConnect

or

Actualización de ASDM a la versión 7.20.2

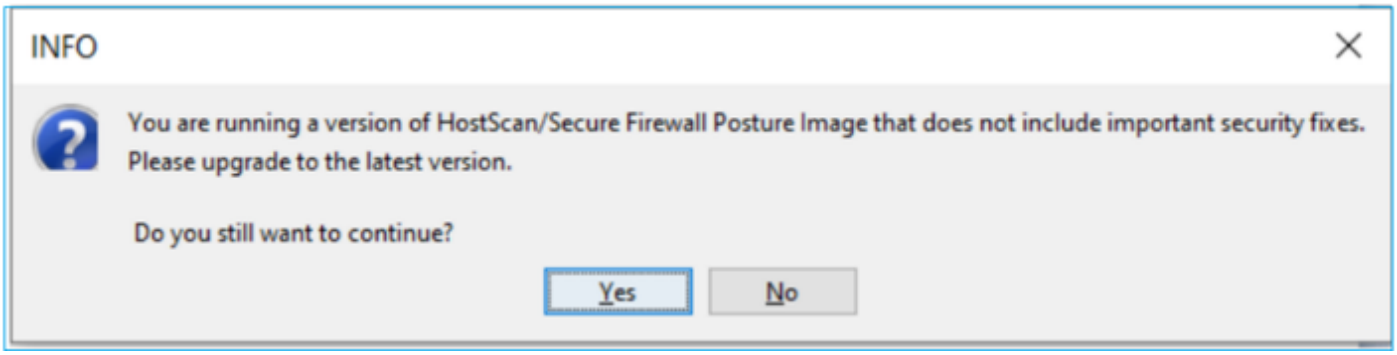
Consulte las notas de defectos para obtener más detalles. Además, puede suscribirse al defecto, de modo que recibirá una notificación sobre las actualizaciones de defectos.

Problema 2. ASDM muestra un elemento emergente para hostscan - la imagen no

incluye correcciones de seguridad importantes

La interfaz de usuario de ASDM muestra:

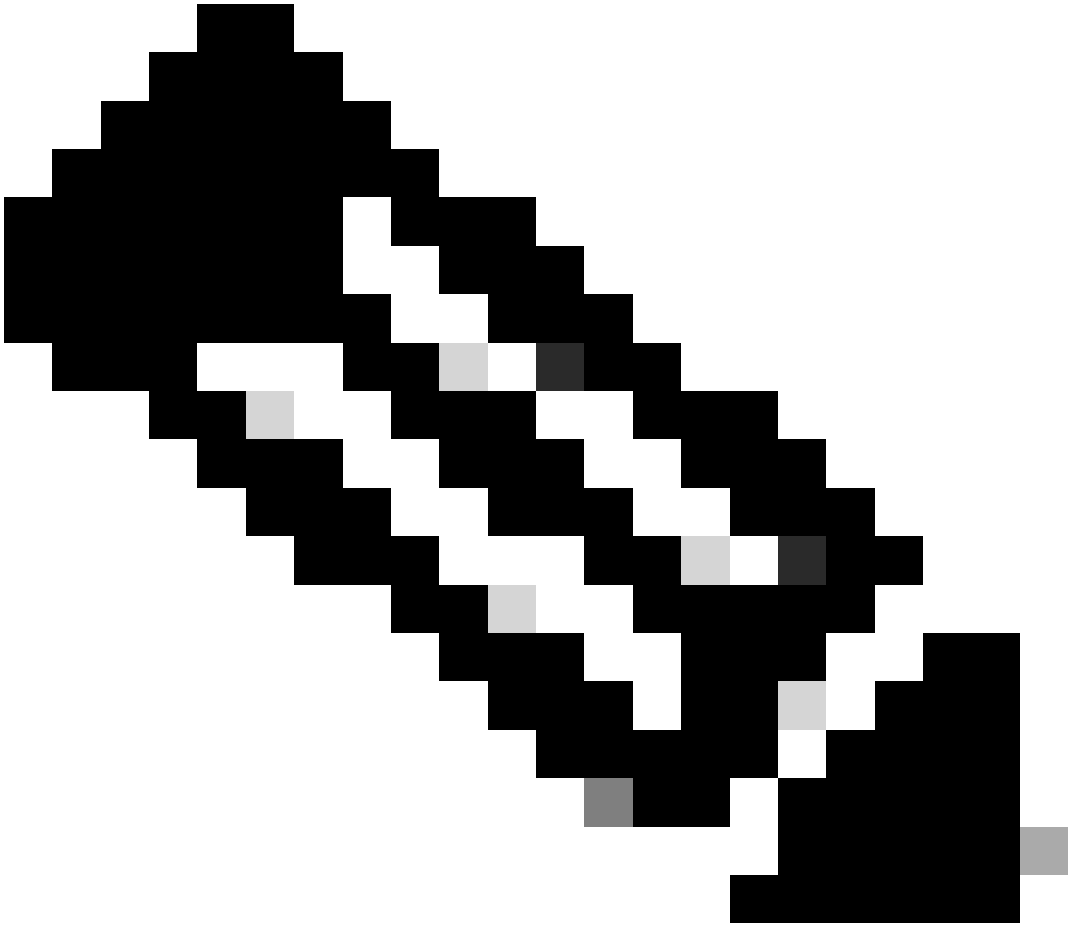
"Está ejecutando una versión de la imagen de estado de HostScan/SecureFirewall que no incluye correcciones de seguridad importantes. Actualice a la última versión. ¿Todavía desea continuar?"



Solución de problemas: pasos recomendados

Este es un defecto conocido:

ID de bug de Cisco CSCwc62461
Al iniciar sesión en el elemento emergente ASDM para hostscan, la imagen no incluye correcciones de seguridad importantes



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

Solución alternativa:

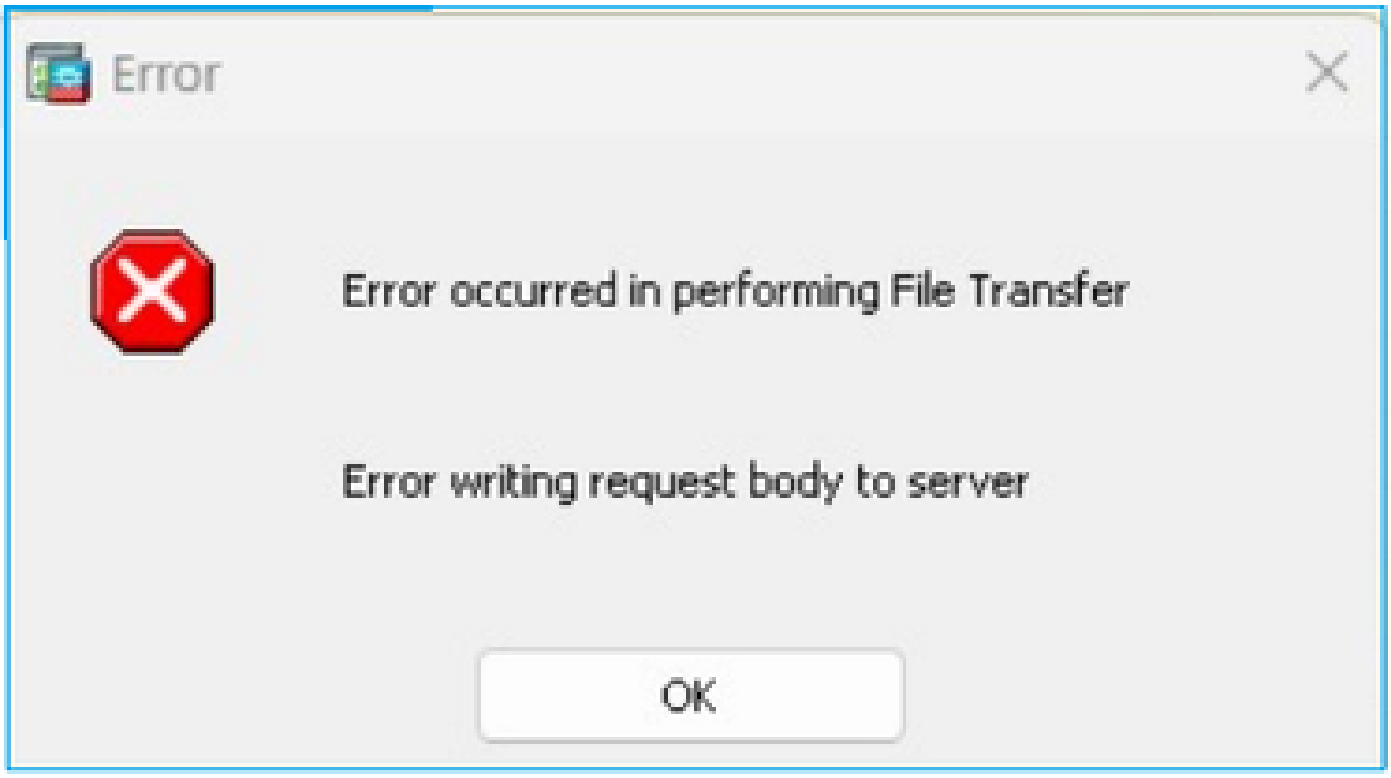
Haga clic en 'Sí' en el cuadro de mensaje emergente para continuar.

Problema 3. ASDM "Error al escribir el cuerpo de la solicitud en el servidor" al copiar una imagen sobre ASDM

La interfaz de usuario de ASDM muestra:

Error al realizar la transferencia de archivos

Error al escribir el cuerpo de la solicitud en el servidor



Solución de problemas: acciones recomendadas

Se trata de un defecto conocido del que se ha hecho un seguimiento:

ID de bug de Cisco CSCtf74236
ASDM "Error al escribir el cuerpo de la solicitud en el servidor" al copiar la imagen

Solución Aternativa

Utilice SCP/TFTP para transferir el archivo.

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).