Fehlerbehebung bei ASDM-Konfiguration, Authentifizierung und anderen Problemen

Inhalt

Einleitung

In diesem Dokument werden der Fehlerbehebungsprozess für die Konfiguration, die Authentifizierung und andere Probleme des Adaptive Security Appliance Device Managers (ASDM) beschrieben.

Hintergrund

Das Dokument ist zusammen mit den folgenden Dokumenten Teil der ASDM-Serie zur Fehlerbehebung:

Link1<>

Link2<>

Link3<>

Fehlerbehebung bei ASDM-Konfigurationsproblemen

Problem 1. ASDM zeigt keine Zugriffskontrolllisten (ACLs) an, die auf eine Schnittstelle angewendet werden.

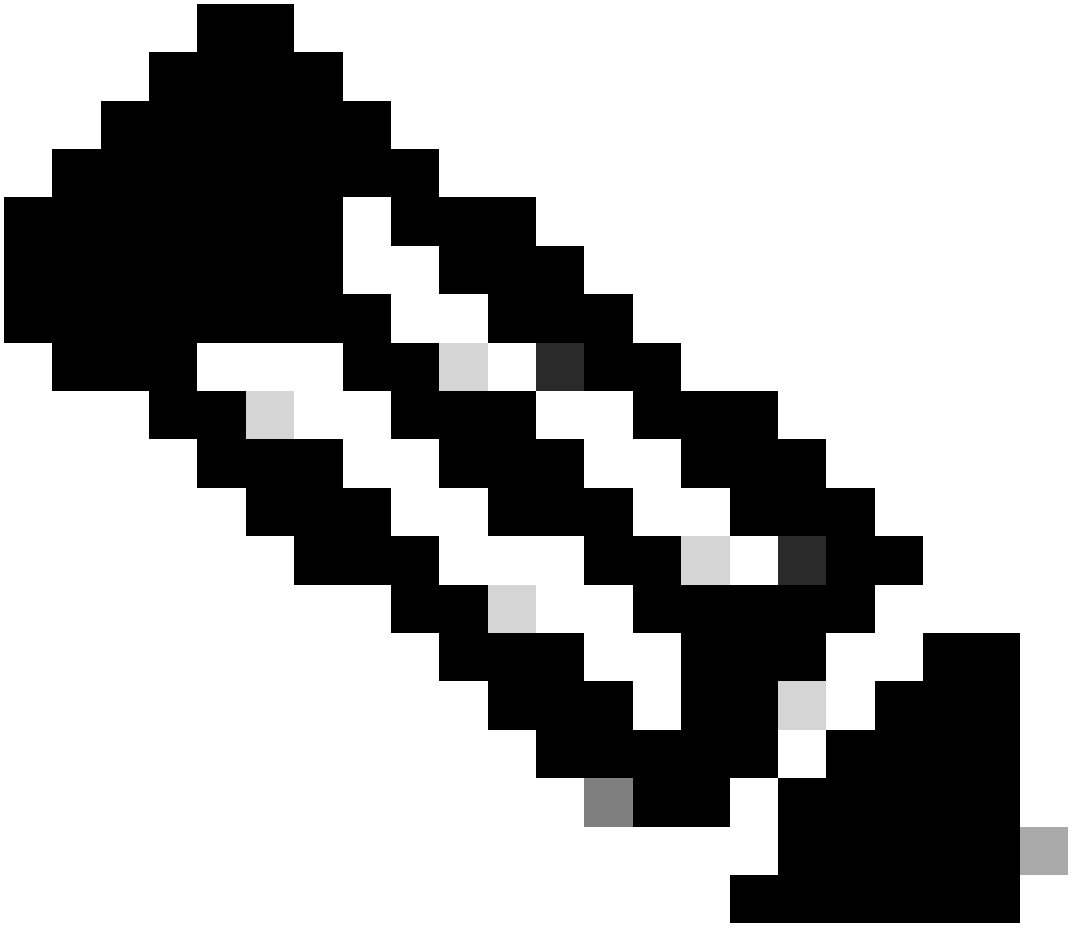
ASDM zeigt keine Zugriffskontrolllisten (ACLs) an, die auf eine Schnittstelle angewendet wurden, obwohl eine gültige Zugriffsgruppe auf die betreffende Schnittstelle angewendet wurde. Die Nachricht lautet stattdessen "0 incoming rules" (0 eingehende Regeln). Diese Symptome zeigen, dass die L3- und L2-ACLs in der Zugriffsgruppenkonfiguration für eine Schnittstelle konfiguriert wurden:

<#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
```

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCwj14147 "ASDM failed to load access-group config if L2 and L3 acl's are mixed" (ASDM lädt Zugriffsgruppenkonfiguration nicht, wenn L2- und L3-ACLs gemischt sind).



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 2. Inkonsistenz bei der Aufrufzählung zwischen ASA CLI und ASDM UI

Die Trefferzählereinträge im ASDM stimmen nicht mit den Trefferzählern in der Zugriffsliste überein, wie vom Befehl show access-list bei der Ausgabe der Firewall berichtet.

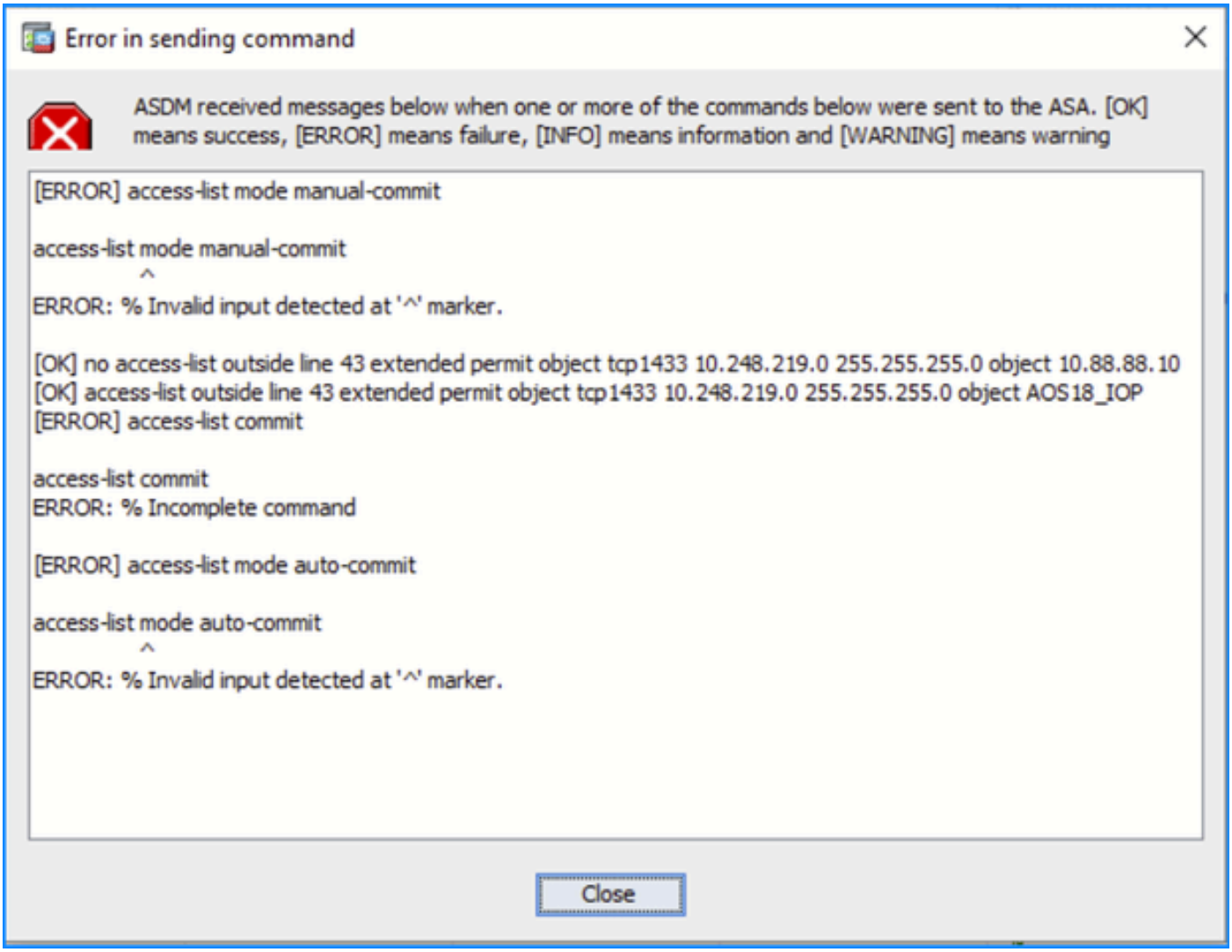
Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID von Cisco CSCtq38377 "DEU: ASDM sollte ACL-Hash-Calc'd auf der ASA und nicht lokal verwenden" und Cisco Bug-ID CSCtq38405"ENH: ASA benötigt einen Mechanismus zur Bereitstellung von ACL-Hash-Informationen an ASD"

Problem 3. "FEHLER: % Ungültige Eingabe bei Markierung '^' erkannt." Fehlermeldung beim Bearbeiten einer ACL in ASDM

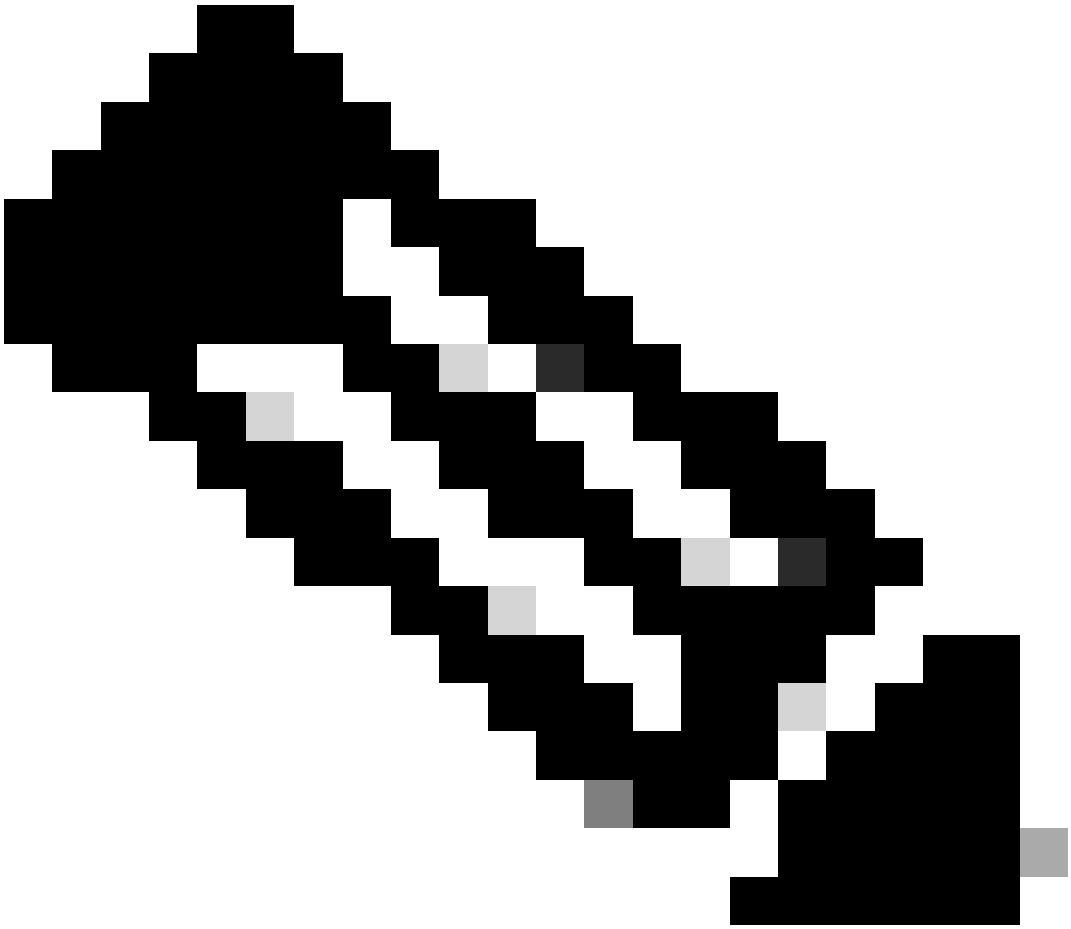
"FEHLER: % Ungültige Eingabe bei Markierung '^' erkannt." Beim Bearbeiten einer ACL in ASDM wird eine Fehlermeldung angezeigt:

```
[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.
```



Fehlerbehebung - empfohlene Maßnahmen

Unter der Software Cisco Bug-ID CSCvq05064 gibt die Meldung "Edit an entry (ACL) from ASDM has an error. Bei Verwendung von ASDM mit OpenJRE/Oracle - Version 7.12.2" und Cisco Bug-ID CSCvp88926 "Senden von zusätzlichen Befehlen beim Löschen der Zugriffsliste".



> Anmerkung: Diese Fehler wurden in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

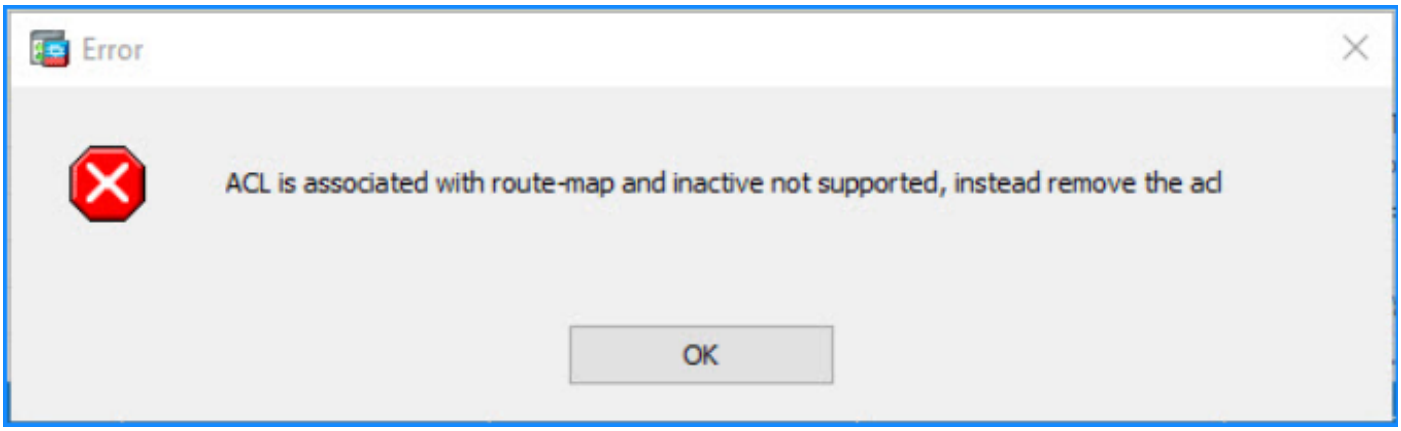
Problem 4. "FEHLER: ACL ist mit route-map verknüpft und inaktiv wird nicht unterstützt. Entfernen Sie stattdessen in bestimmten Fällen die acl-Fehlermeldung.

"FEHLER: ACL ist mit route-map verknüpft und inaktiv wird nicht unterstützt. Entfernen Sie stattdessen die acl"-Fehlermeldung, die in einem der folgenden Fälle angezeigt wird:

1. Bearbeiten einer ACL in ASDM, die in einer richtlinienbasierten Routing-Konfiguration verwendet wird:

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

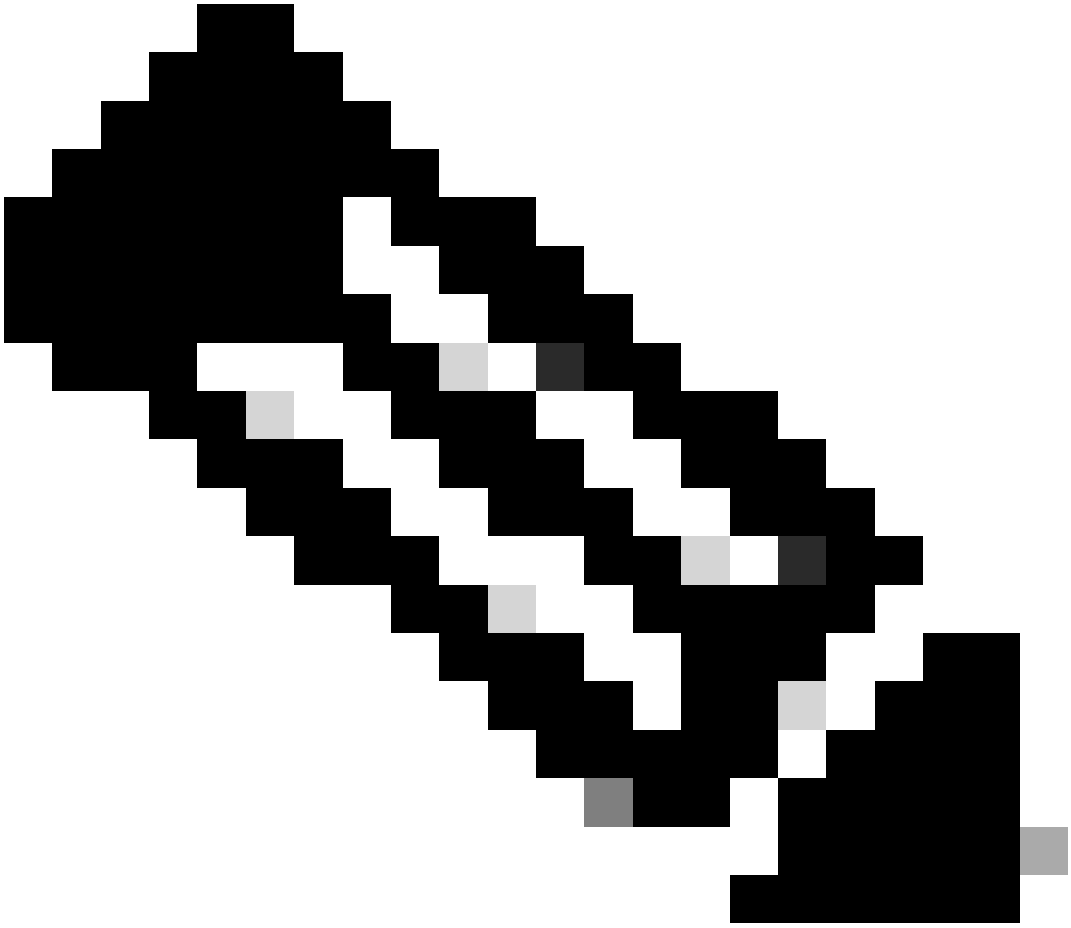
FEHLER: ACL ist mit route-map verknüpft und inaktiv nicht unterstützt; stattdessen wird der ACL entfernt



2. ACL-ASDM bearbeiten > Konfiguration -> Remotezugriff-VPN -> Netzwerkzugriff (Client) > dynamische Zugriffsrichtlinie

Fehlerbehebung - empfohlene Maßnahmen

1. Weitere Informationen finden Sie unter der Software-Bug-ID CSCwb57615 "Configuring pbr access-list with line number failed." (Konfiguration der pbr-Zugriffsliste mit der Zeilennummer fehlgeschlagen). Die Problemumgehung besteht darin, den Parameter "line" aus der Konfiguration auszuschließen.
2. Weitere Informationen finden Sie unter der Software-Bug-ID CSCwe34665 "Die ACL-Objekte können nicht bearbeitet werden, wenn sie bereits verwendet werden. Die Ausnahme wird abgerufen."



Anmerkung: Diese Fehler wurden in den letzten ASA-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 5. Keine Anmeldungen bei implizit abgelehnten Verbindungen im ASDM Real-Time Log Viewer

Der ASDM Real-Time Log Viewer zeigt keine Protokolle für implizit abgelehnte Verbindungen an.

Fehlerbehebung - empfohlene Maßnahmen

Die implizite deny-Anweisung am Ende der Zugriffsliste generiert kein Syslog. Wenn der gesamte abgelehnte Datenverkehr Syslog generieren soll, fügen Sie die Regel mit dem log-Schlüsselwort am Ende der ACL hinzu.

Problem 6. ASDM reagiert nicht mehr, wenn versucht wird, Netzwerkobjekte oder Objektgruppen zu ändern.

Der ASDM friert ein, wenn versucht wird, Netzwerkobjekte oder Objektgruppen auf der Seite Konfiguration > Firewall > Zugriffsregeln auf der Registerkarte Adressen zu ändern. Der Benutzer kann keinen der Parameter im Netzwerkobjektfenster bearbeiten, wenn dieses Problem auftritt.

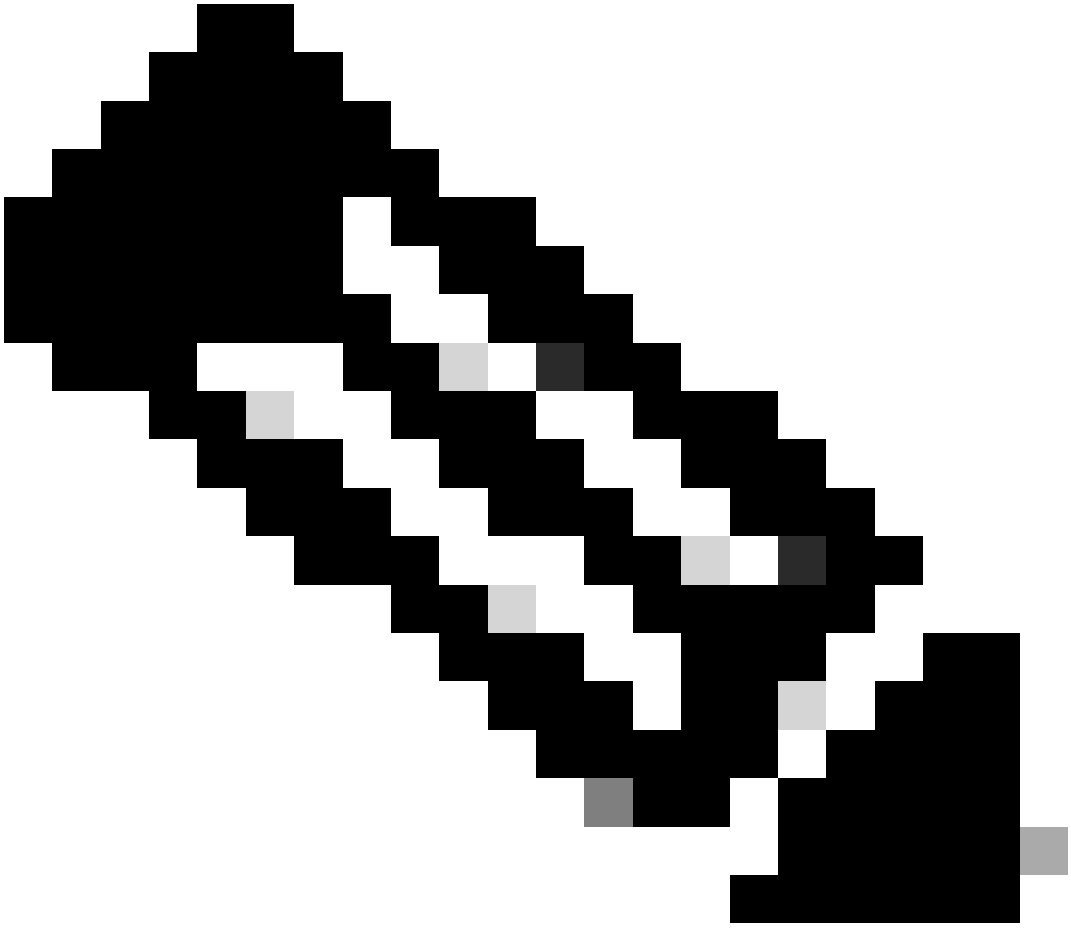
Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCwj12250 "ASDM friert beim Bearbeiten von Netzwerkobjekten oder Netzwerkobjektgruppen ein". Die Problemumgehung besteht darin, die Erfassung der TopN-Hoststatistiken zu deaktivieren:

<#root>

```
ASA(config)#
```

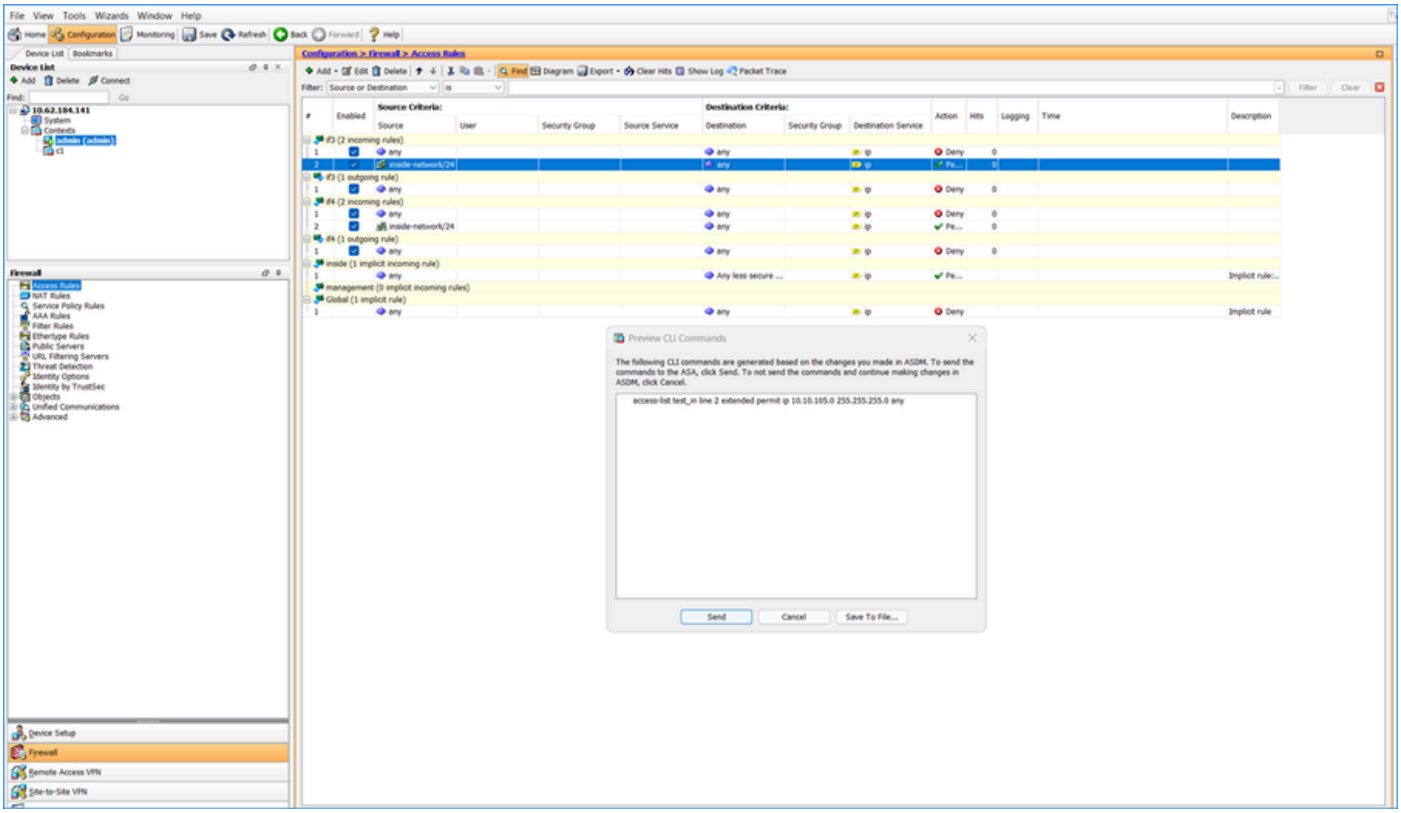
no hpm topN enable



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 7: ASDM kann zusätzliche Zugriffskontrolllistenregeln für verschiedene Schnittstellen anzeigen

ASDM kann zusätzliche Zugriffskontrolllisten-Regeln für verschiedene Schnittstellen anzeigen, wenn eine Zugriffskontrollliste auf Schnittstellenebene geändert wird. In diesem Beispiel wurde eine eingehende Regel 2 zur Schnittstelle if3 ACL hinzugefügt. ASDM zeigt auch #2 für die Schnittstelle if4 an, obwohl diese Regel nicht vom Benutzer konfiguriert wurde. In der Befehlsvorschau wird eine einzelne ausstehende Änderung richtig angezeigt. Dies ist ein Problem mit der Anzeige der Benutzeroberfläche.



Fehlerbehebung - empfohlene Maßnahmen

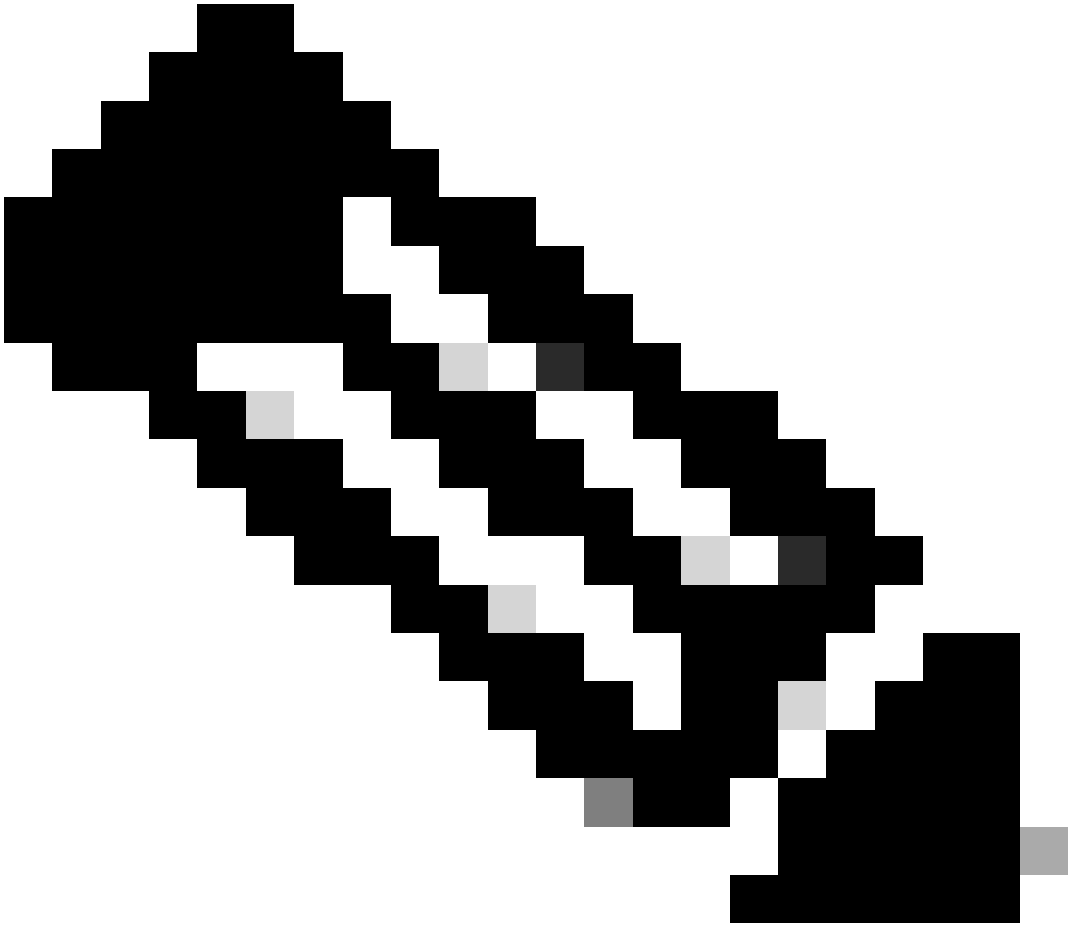
Weitere Informationen finden Sie unter der Software-Bug-ID CSCwm71434 "ASDM zeigt möglicherweise doppelte Einträge in der Zugriffsliste für die Schnittstelle an".

Problem 8. Echtzeitprotokolle sind im Real-Time Log Viewer nicht verfügbar

In der Echtzeit-Protokollanzeige werden keine Protokolle angezeigt

Fehlerbehebung - empfohlene Maßnahmen

1. Stellen Sie sicher, dass die Protokollierung konfiguriert ist. Siehe ASDM Book 1: Cisco ASA Series General Operations - ASDM-Konfigurationsleitfaden, 7.22, Kapitel: Protokollieren.
2. Weitere Informationen finden Sie unter der Software Cisco bug ID CSCvf82966 "ASDM - Logging: Die Echtzeitprotokolle können nicht angezeigt werden."

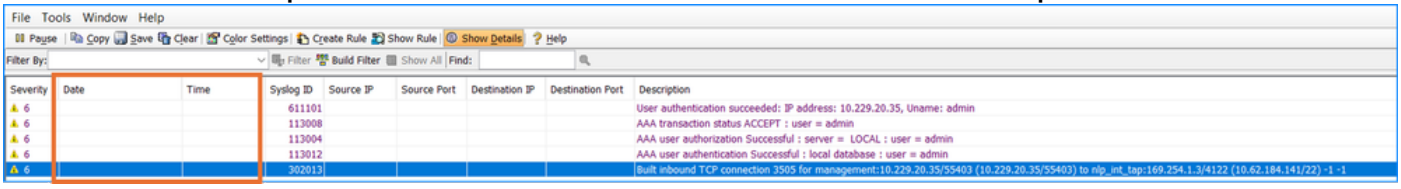


Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Referenzen

- ASDM-Buch 1: Cisco ASA Series General Operations - ASDM-Konfigurationsleitfaden, 7.22, Kapitel: Protokollieren.

Problem 9. Die Spalten für Datum und Uhrzeit sind im Echtzeitprotokoll-Viewer leer.



Fehlerbehebung - empfohlene Maßnahmen

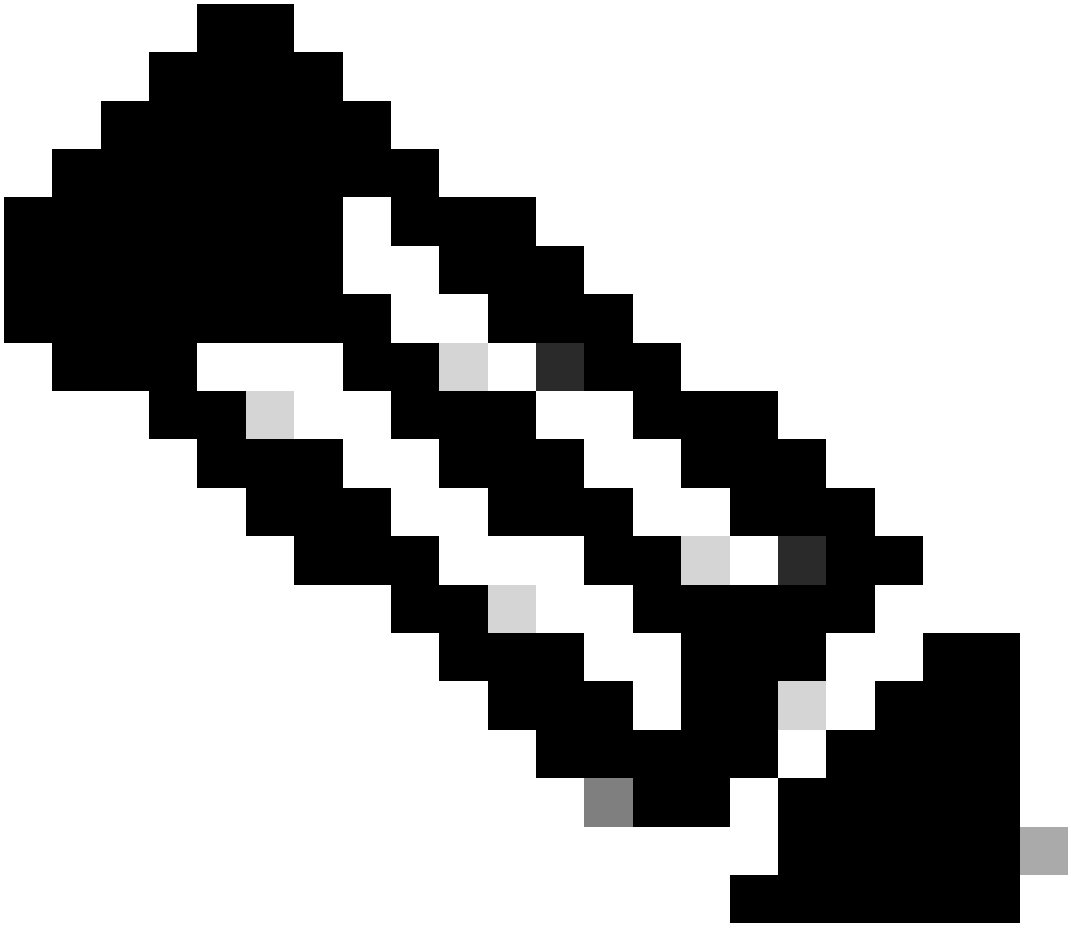
1. Überprüfen Sie, ob das Zeitstempelformat für die RFC5424-Protokollierung verwendet wird:

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. Wenn das Zeitstempelformat für die RFC5424-Protokollierung verwendet wird, finden Sie weitere Informationen in der Software Cisco bug ID CSCvs5212 "ASDM ENH: Möglichkeit für Event Log Viewers, ASA-Syslogs im rfc5424-Zeitstempelformat anzuzeigen". Die Problemumgehung besteht darin, das RFC 5424-Format zu vermeiden:

```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

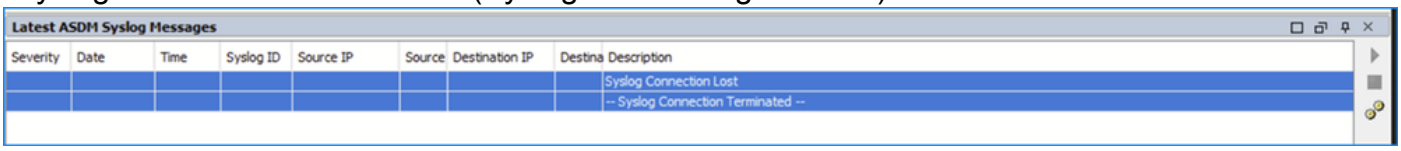
3. Weitere Informationen finden Sie unter dem Softwarefehler Cisco Bug-ID CSCwh70323 "Timestamp entry missing for some syslog messages sent to syslog server" (Zeitstempeleintrag fehlt für einige Syslog-Meldungen, die an den Syslog-Server gesendet wurden).



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

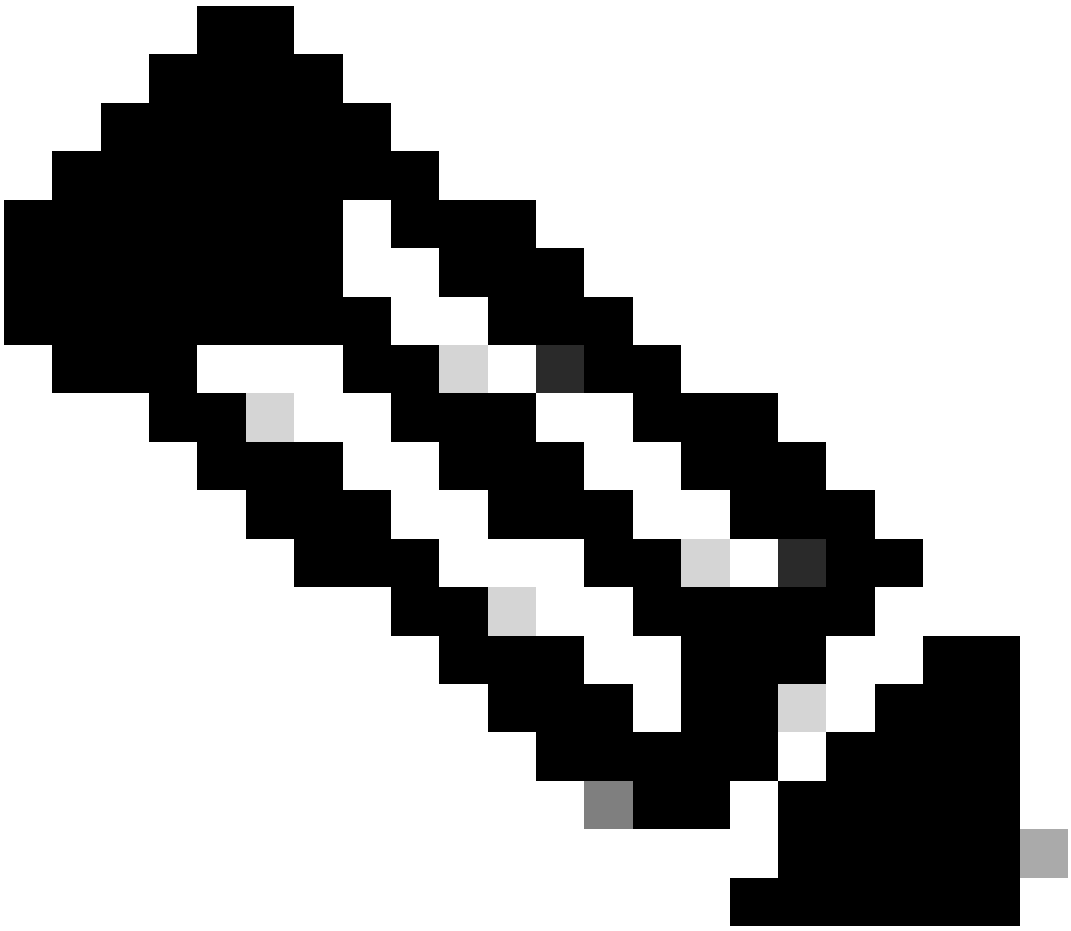
Problem 10: Die Anmeldung bei ASDM kann fehlschlagen, nachdem in einer ASA mit mehreren Kontexten zu einem anderen Kontext gewechselt wurde.

Die Registerkarte Latest ASDM Syslog Messages (Aktuelle ASDM-Syslog-Meldungen) auf der Startseite zeigt die Meldungen "Syslog Connection Lost" (Syslog-Verbindung unterbrochen) und "Syslog Connection Terminated" (Syslog-Verbindung beendet):



Fehlerbehebung - empfohlene Maßnahmen

Stellen Sie sicher, dass die Protokollierung konfiguriert ist. Weitere Informationen finden Sie unter der Software Cisco Bug ID CSCvz15404 "ASA: Multiple-Context-Modus: Die ASDM-Protokollierung wird beendet, wenn auf einen anderen Kontext umgeschaltet wird."



> Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 11: ASDM-Sitzung wird beim Wechsel zwischen verschiedenen Kontexten abrupt beendet

Die ASDM-Sitzung wurde abrupt beendet, wenn zwischen verschiedenen Kontexten gewechselt wurde. Die Fehlermeldung "Die maximale Anzahl an Verwaltungssitzungen für das Protokoll http oder den Benutzer ist bereits vorhanden. Versuchen Sie es später erneut." Diese Protokolle werden in den Syslog-Meldungen angezeigt:

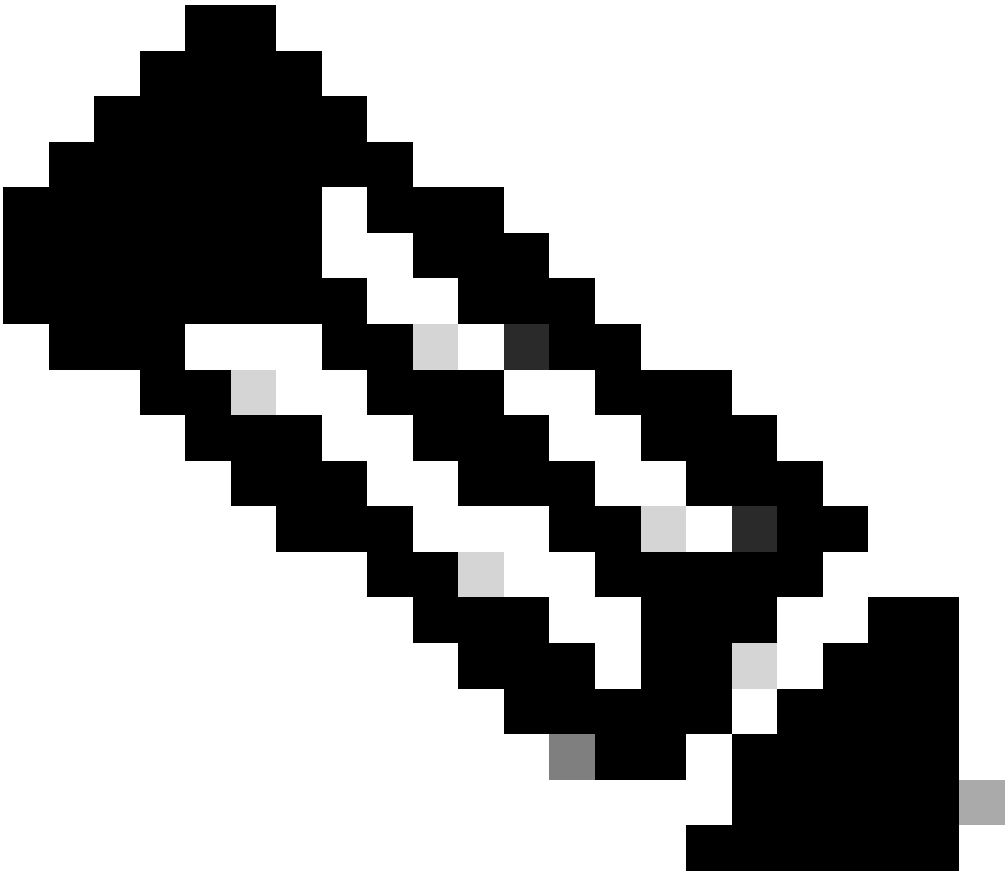
```
%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5

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

Fehlerbehebung - empfohlene Maßnahmen

1. Überprüfen Sie, ob die aktuelle ASDM-Ressourcennutzung den Grenzwert erreicht hat. In diesem Fall erhöht sich der Zähler Abgelehnt:

```
<#root>

firewall #

show resource usage resource ASDM


Resource                Current         Peak      Limit        Denied Context
ASDM

5

            5

5



10

 admin
```

2. Weitere Informationen finden Sie unter der Software Cisco bug ID CSCvs72378 "ASDM session being abrupt terminated when switching between different contexts" (ASDM-Sitzung wird beim Switching zwischen verschiedenen Kontexten abrupt beendet).



Anmerkung: Dieser Fehler wurde in den letzten ASA-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

3. Wenn die Softwareversion die Fehlerbehebung für die Cisco Bug-ID CSCvs72378 aufweist und die aktuelle Ressource den Grenzwert erreicht hat, trennen Sie einige der vorhandenen ASDM-Sitzungen. Sie können den ASDM schließen oder HTTPS-Verbindungen für die IP-Adresse des Hosts löschen, auf dem ASDM ausgeführt wird. In diesem Beispiel wird davon ausgegangen, dass der HTTP-Server auf ASDM auf dem Standard-HTTPS-Port 443 ausgeführt wird:

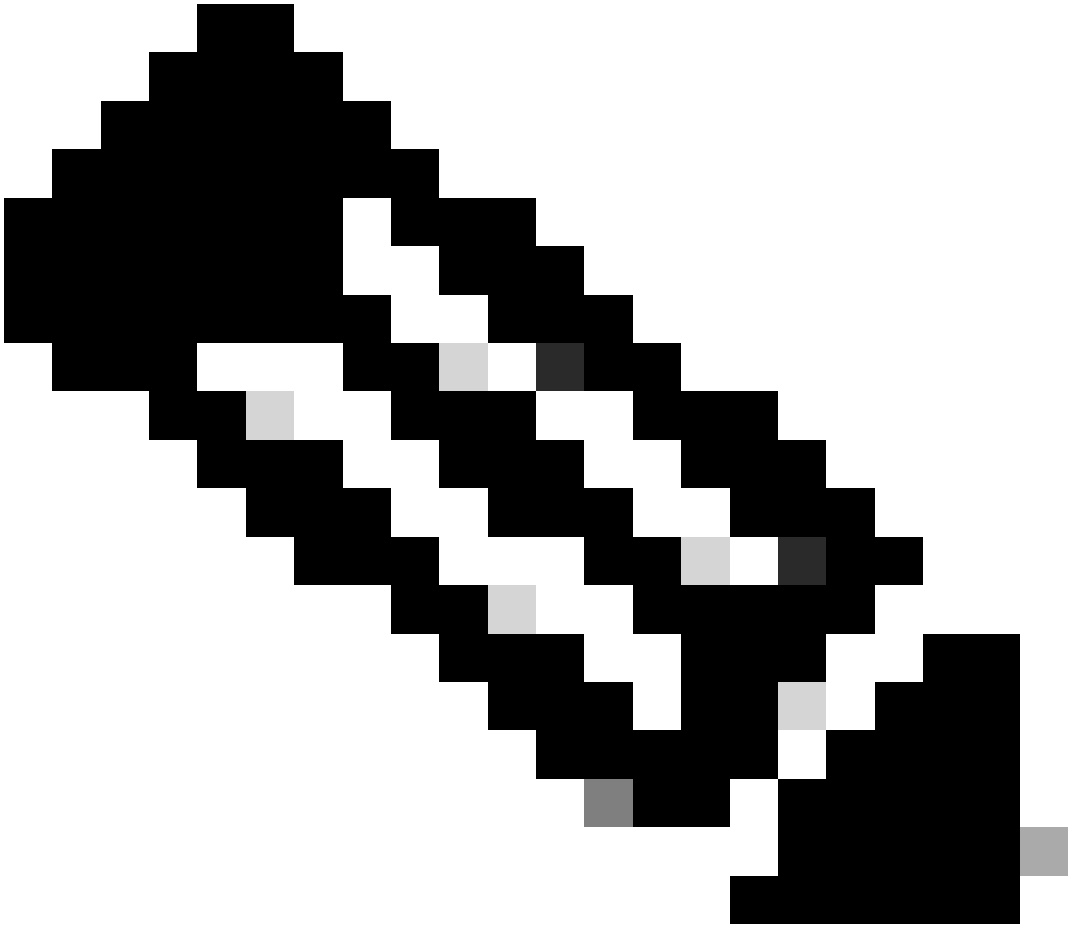
```
<#root>

#

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
```

Problem 12. ASDM wird zufällig mit der Meldung beendet/beendet, dass ASDM eine Nachricht vom ASA-Gerät erhalten hat, um die Verbindung zu trennen. ASDM wird jetzt beendet."

Auf Multi-Context-ASA wird ASDM zufällig mit der Meldung beendet/beendet, dass ASDM eine Nachricht vom ASA-Gerät erhalten hat, um die Verbindung zu trennen. ASDM wird beendet."

Fehlerbehebung - empfohlene Maßnahmen

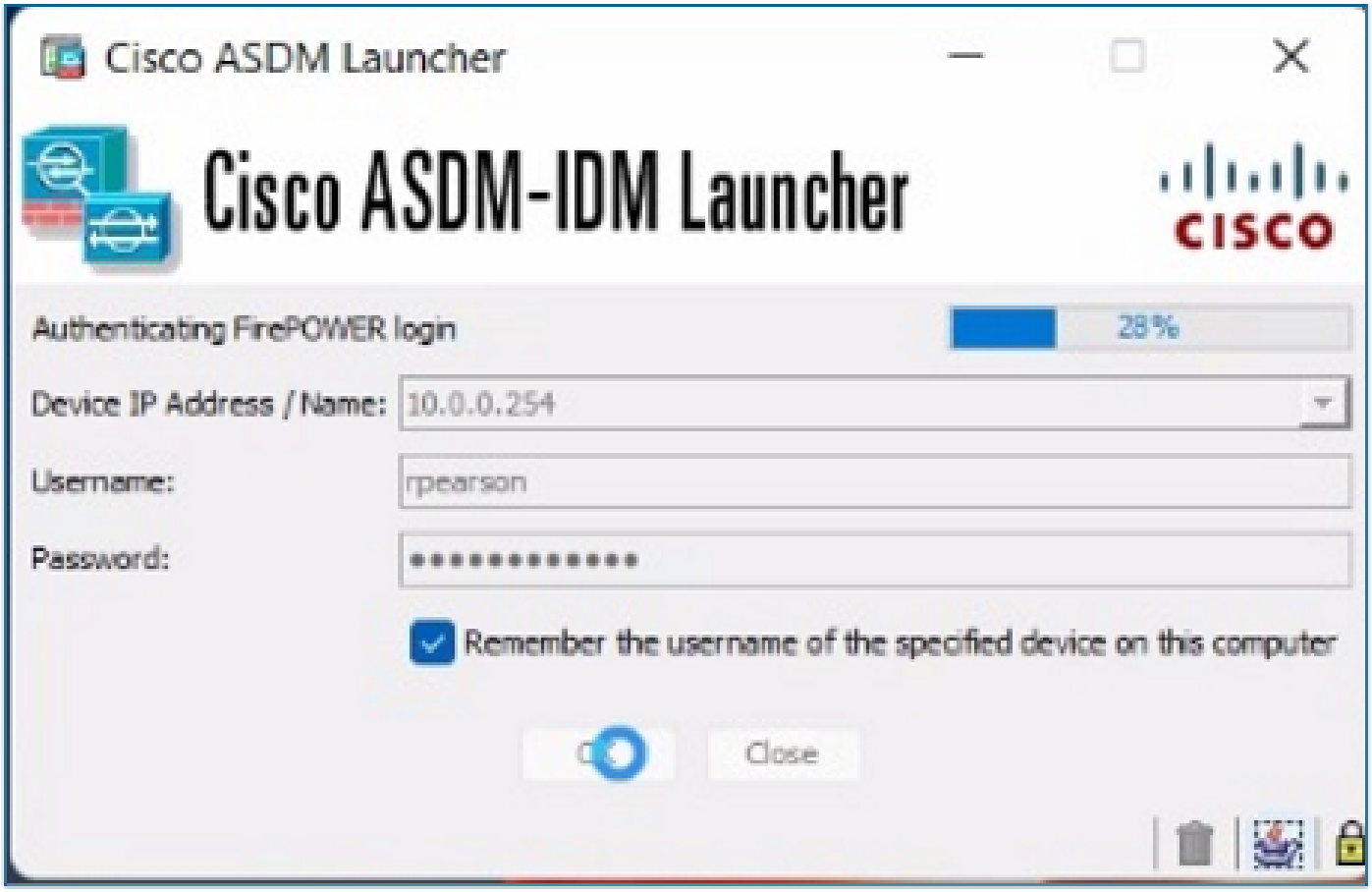
Weitere Informationen finden Sie unter dem Softwarefehler Cisco bug ID CSCwh04395 "ASDM application random exits/terminates with an alert message on multi-context setup" (ASDM-Anwendung wird bei Multi-Context-Einrichtung nach dem Zufallsprinzip beendet).



Anmerkung: Dieser Fehler wurde in den letzten ASA-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 13: Die ASDM-Last hängt mit der Meldung "Authentication FirePOWER login" (Authentifizierung, FirePOWER-Anmeldung).

Die ASDM-Last wird mit der Meldung "Authentication FirePOWER login" (Authentifizierung, FirePOWER-Anmeldung) geladen:



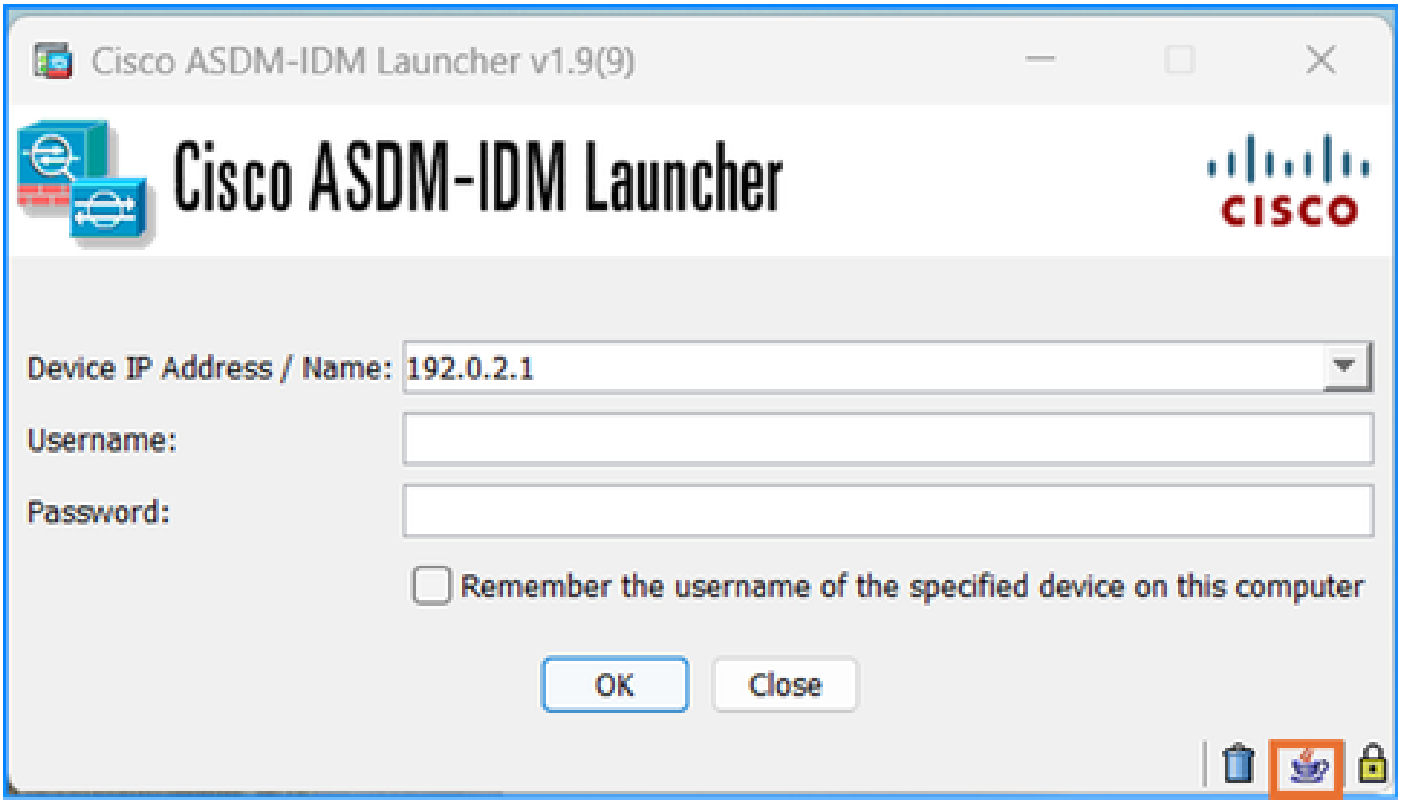
In den Java-Konsolenprotokollen wird die Meldung "Failed to connect to FirePower, continue without it" (Verbindung mit FirePower fehlgeschlagen, Fortsetzung ohne Verbindung) angezeigt:

<#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)
```

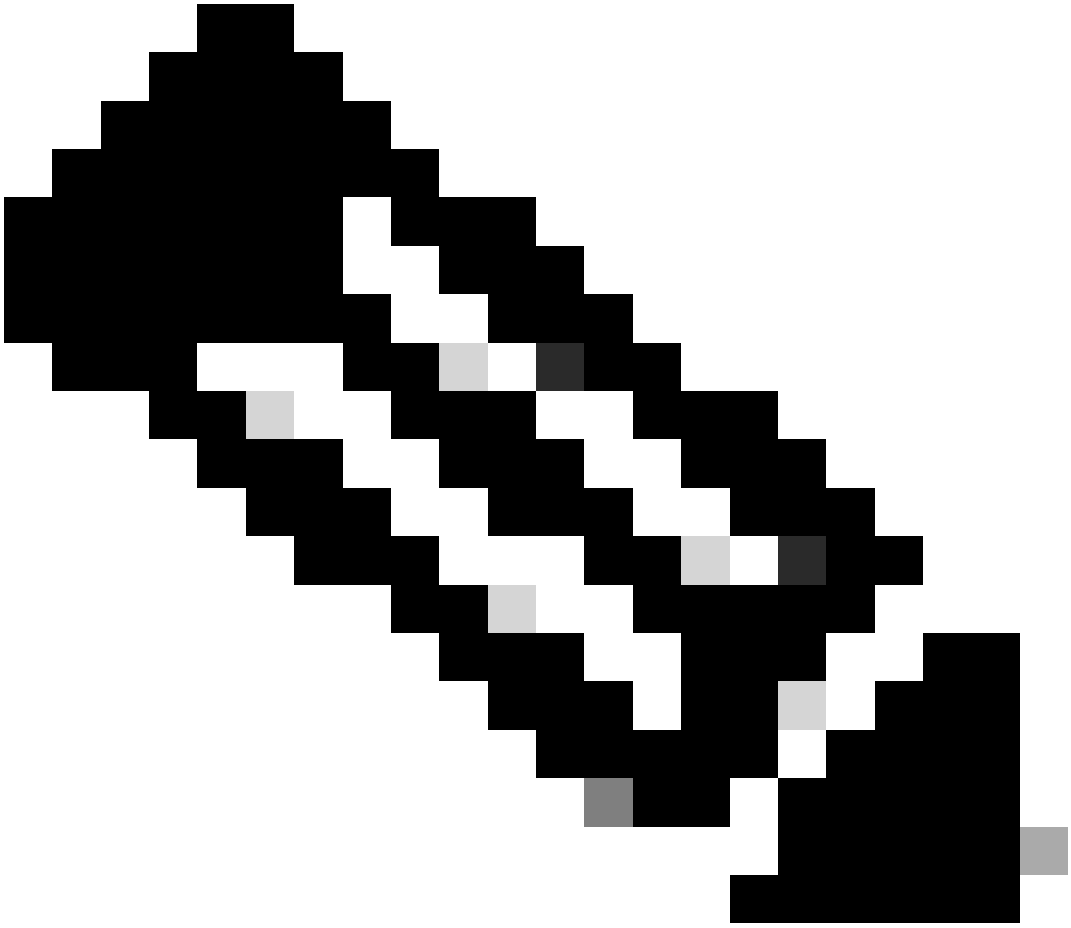
Um dieses Symptom zu überprüfen, aktivieren Sie die Java-Konsolenprotokolle:



Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco bug ID CSCwe15164 "ASA: ASDM kann SFR-Registerkarten erst anzeigen, wenn sie über die entsprechende CLI aktiviert wurden." Workaround-Schritte:

1. Schließen Sie den ASDM-Manager.
2. Sie erhalten SSH-Zugriff auf SFR und wechseln vom Benutzer zum Root (sudo su).
3. Starten Sie den ASDM erneut, nachdem Sie die obigen Schritte durchgeführt haben, und er kann die FirePOWER (SFR)-Registerkarten laden.



Anmerkung: Dieser Fehler wurde in den letzten Firepower-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 14. ASDM zeigt das Management/die Konfiguration des FirePOWER-Moduls nicht an.

Die Konfiguration des FirePOWER-Moduls ist für ASDM nicht verfügbar.

Fehlerbehebung - empfohlene Maßnahmen

1. Stellen Sie sicher, dass die ASA-, ASDM-, FirePOWER-Modul- und Betriebssystemversionen kompatibel sind. Weitere Informationen finden Sie in den Cisco Secure Firewall ASA Versionshinweisen, Cisco Secure Firewall ASDM Versionshinweisen, Cisco Secure Firewall ASA-Kompatibilität:

- ASA 9.14/ASDM 7.14/Firepower 6.6 ist die endgültige Version für das ASA FirePOWER-Modul auf den ASA 5525-X, 5545-X und 5555-X.
- ASA 9.12/ASDM 7.12/Firepower 6.4.0 ist die endgültige Version für das ASA FirePOWER-Modul auf der ASA 5515-X und 5585-X.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 ist die endgültige Version für das ASA FirePOWER-Modul der ASA 5506-X-Serie und 5512-X.
- Sofern nicht anders angegeben, sind ASDM-Versionen mit allen vorherigen ASA-Versionen abwärtskompatibel. Beispielsweise kann ASDM 7.13(1) eine ASA 5516-X auf ASA 9.10(1) verwalten.
- ASDM wird für das FirePOWER-Modulmanagement mit ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ und 9.16(3.19)+ nicht unterstützt. müssen Sie FMC verwenden, um das Modul mit diesen Versionen zu verwalten. Für diese ASA-Versionen ist ASDM 7.18(1.152) oder höher erforderlich, die ASDM-Unterstützung für das ASA FirePOWER-Modul endete jedoch mit 7.16.
- ASDM 7.13(1) und ASDM 7.14(1) unterstützen ASA 5512-X, 5515-X, 5585-X und ASASM nicht. Sie müssen ein Upgrade auf ASDM 7.13(1.101) oder 7.14(1.48) durchführen, um die ASDM-Unterstützung wiederherzustellen.

2. Wenn die Versionen kompatibel sind, überprüfen Sie, ob das Modul betriebsbereit ist:

<#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
```

Wenn das Modul heruntergefahren ist, kann der Befehl sw-module module reset verwendet werden, um das Modul zurückzusetzen und dann die Modulsoftware neu zu laden.

Referenzen

- Cisco Secure Firewall ASA - Versionshinweise
- Cisco Secure Firewall ASDM - Versionshinweise
- Cisco Secure Firewall ASA-Kompatibilität

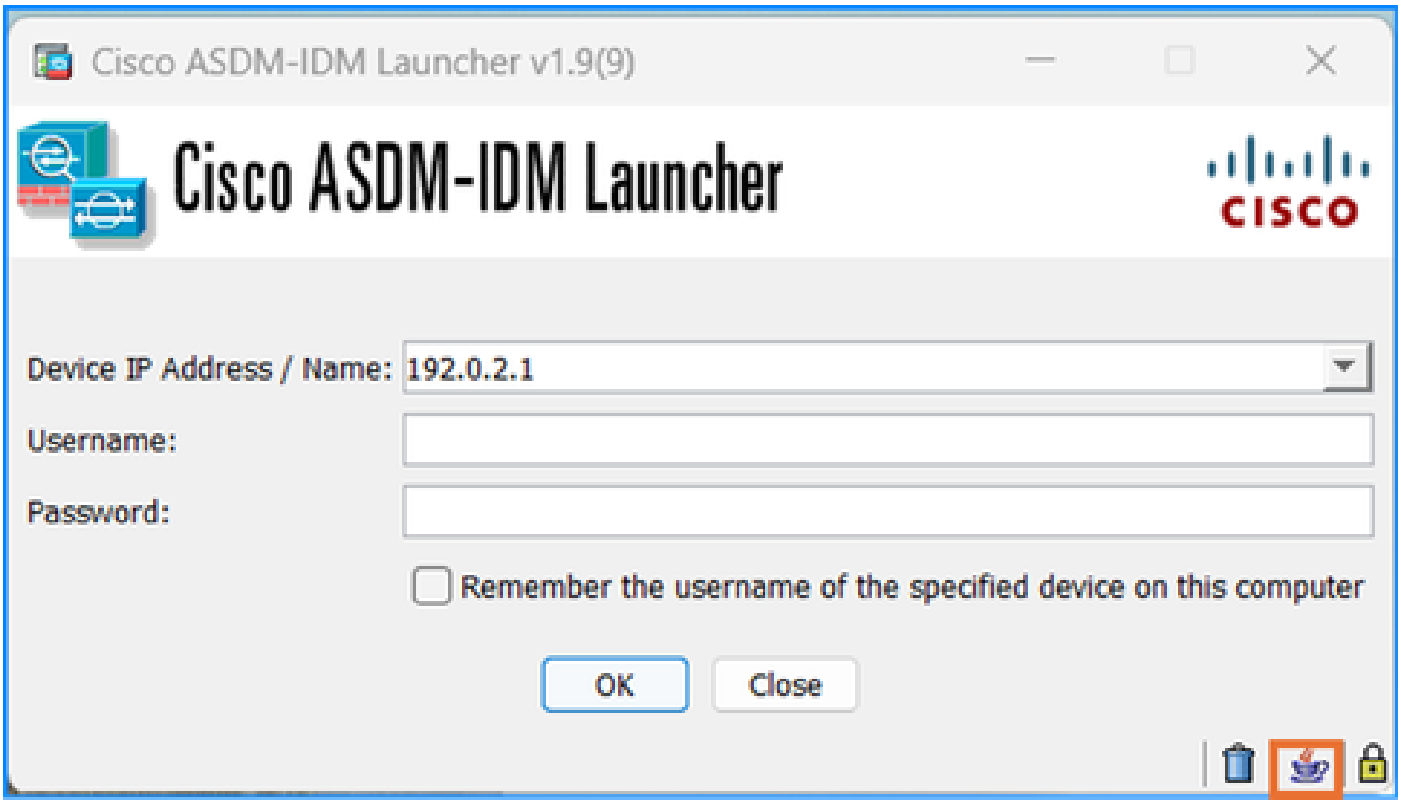
Problem 15. Auf die sicheren Clientprofile kann auf ASDM nicht zugegriffen werden.

Java-Konsolenprotokolle zeigen die "java.lang.ArrayIndexOutOfBoundsException: 3"-Fehlermeldung:

<#root>

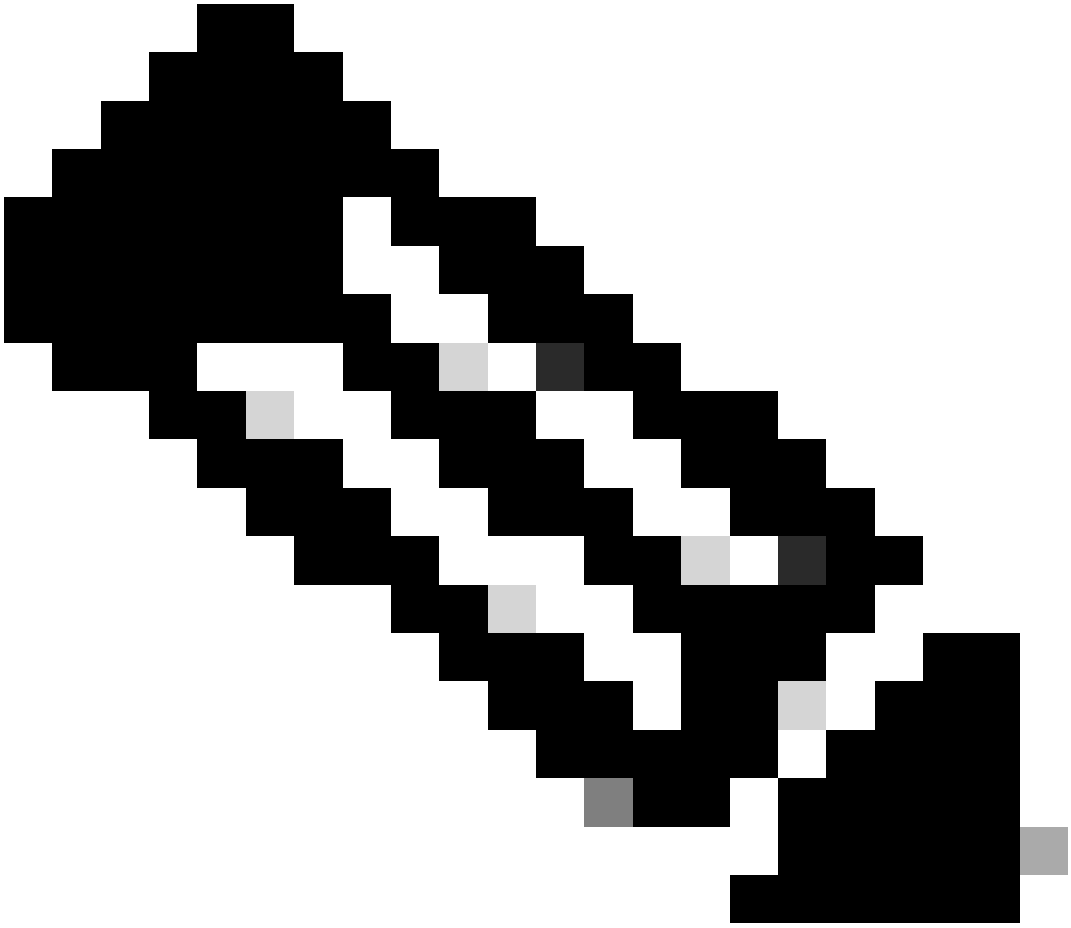
```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige

java.lang.ArrayIndexOutOfBoundsException: 3


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

Um dieses Symptom zu überprüfen, aktivieren Sie die Java-Konsolenprotokolle:



Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCwi56155 "Cannot access Secure Client Profile on ASDM" (Sicheres Client-Profil auf ASDM nicht möglich).



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

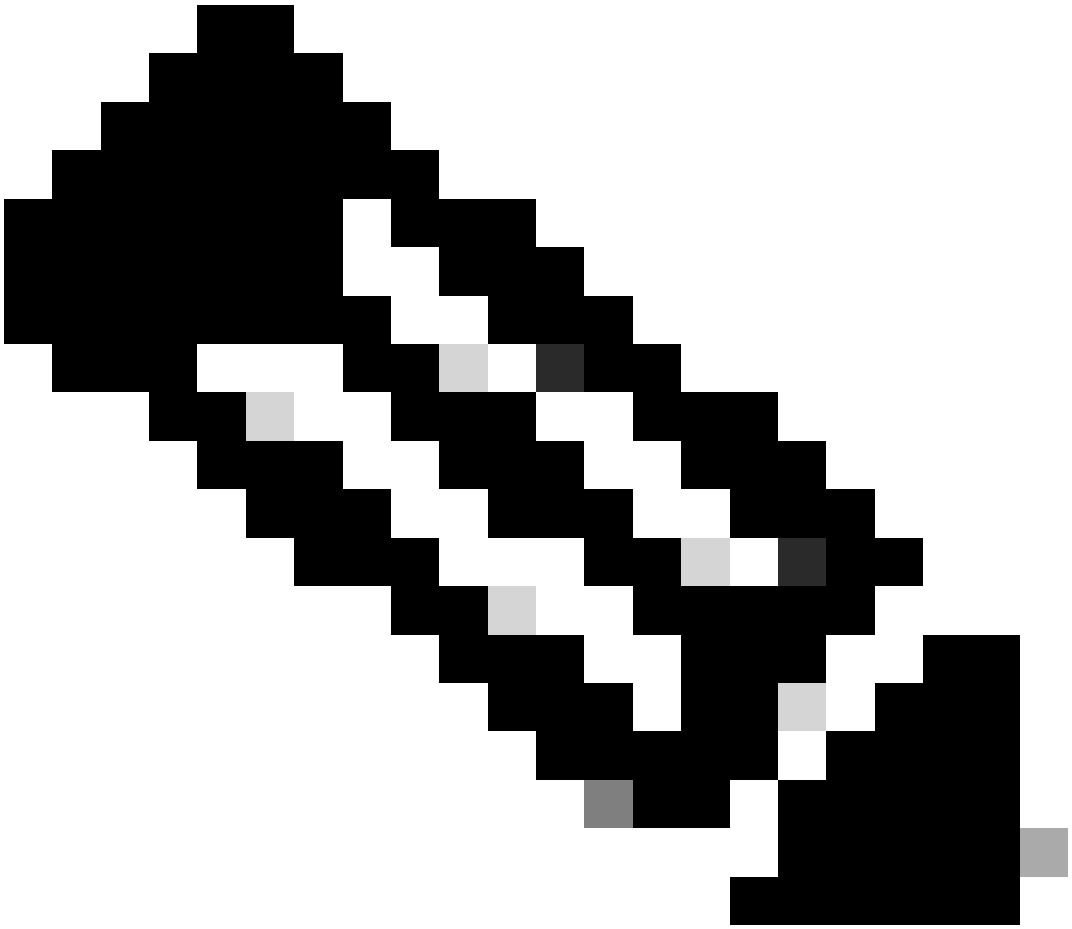
Problem 16. XML-Profile für das sichere Clientprofil auf ASDM können nicht bearbeitet werden

Die Secure Client Profile XML-Profile in ASDM Configuration > Remote Access VPN > Network (Client) Access können auf einem ASA-Gerät nicht bearbeitet werden, wenn auf der Festplatte ein AnyConnect-Image vorhanden ist, das älter als Version 4.8 ist.

Die Fehlermeldung "Es gibt kein Profil-Editor-Plugin in Ihrem Secure Client Image auf dem Gerät. Wechseln Sie zu Network (Client) Access > Secure Client Software, installieren Sie das Secure Client-Image Version 2.5 oder höher, und versuchen Sie es dann erneut" wird angezeigt.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID von Cisco CSCwk64399 "ASDM - Cannot edit Secure Client Profile" (ASDM - Sicheres Client-Profil konnte nicht bearbeitet werden). Die Problemumgehung besteht darin, ein anderes AnyConnect-Image mit einer niedrigeren Priorität festzulegen.



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 17. Sichere Client-Images fehlen nach Konfigurationsänderungen

Nachdem Sie die ASDM-Konfiguration > Netzwerkzugriff (Client) > sicheres Clientprofil geändert haben, sind die Abbilder in Konfiguration > Netzwerkzugriff (Client) > gesicherter Clientsoftware nicht mehr vorhanden.

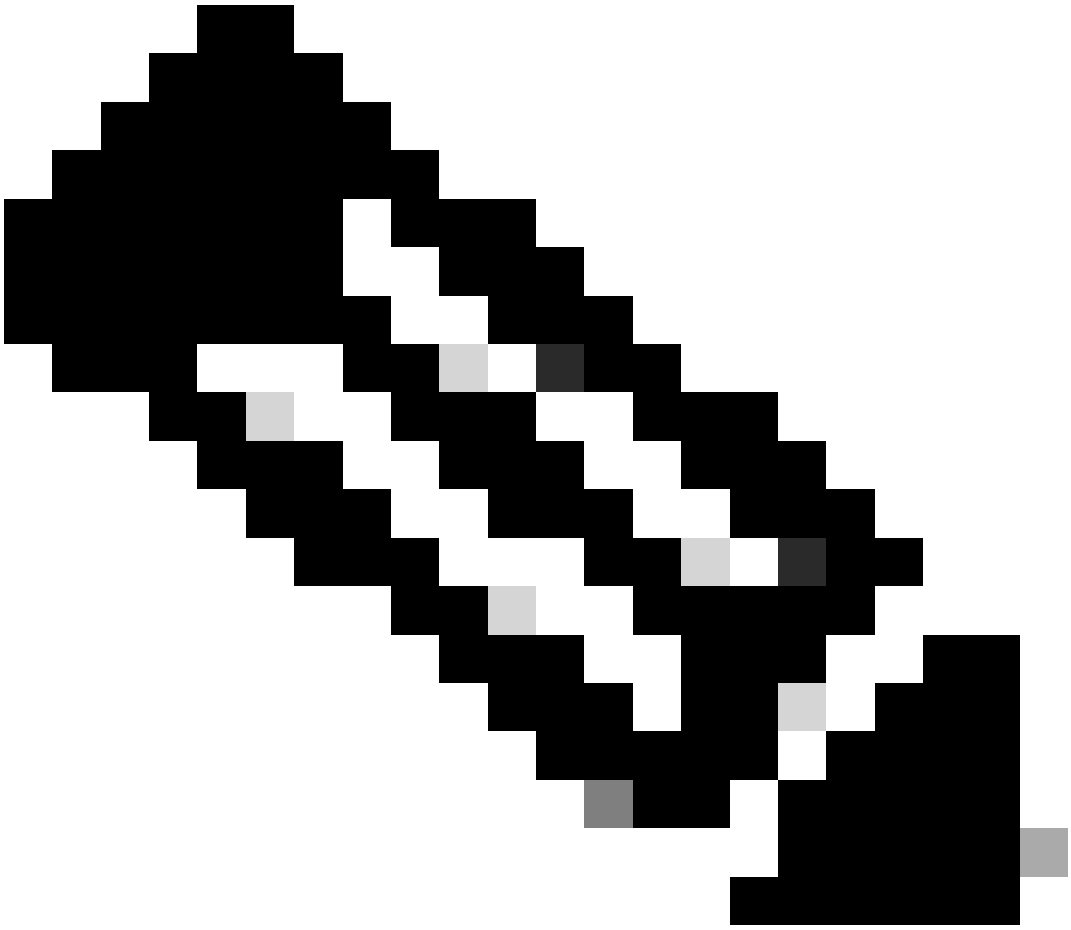
Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID von Cisco CSCwf23826 "Secure Client Software wird nach der Änderung des Secure Client Profile Editors im ASDM nicht angezeigt". Workaround-Optionen:

- Klicken Sie im ASDM auf das Symbol Aktualisieren.

ODER

- ASDM schließen und wieder öffnen



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 18: Ineffektive Befehle für HTTP-Serversitzungs-Timeout und HTTP-

Serveridle-Timeout

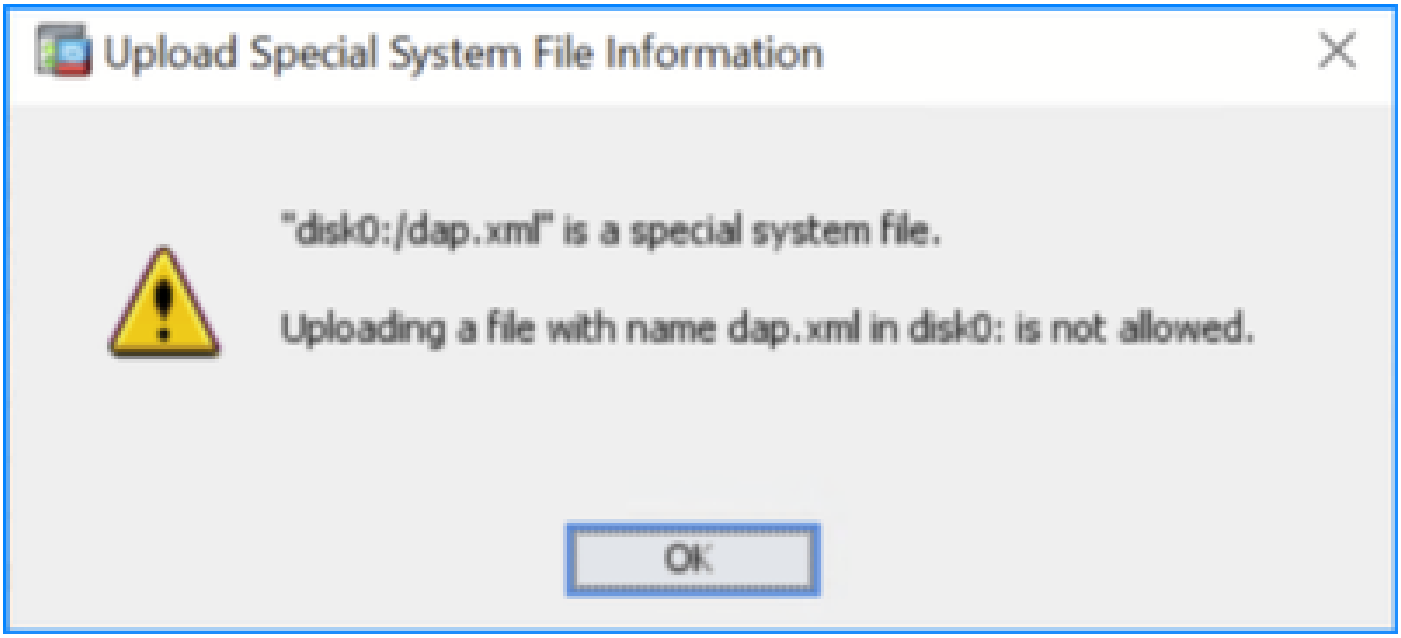
Die Befehle http server session-timeout und http server idle-timeout haben keine Auswirkungen auf ASA im Multi-Context-Modus.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCtx41707 "Support for http server timeout command in multi-context mode" (Unterstützung für HTTP-Server-Zeitüberschreitungsbefehl im Multi-Kontext-Modus). Die Befehle sind konfigurierbar, die Werte haben jedoch keine Auswirkungen.

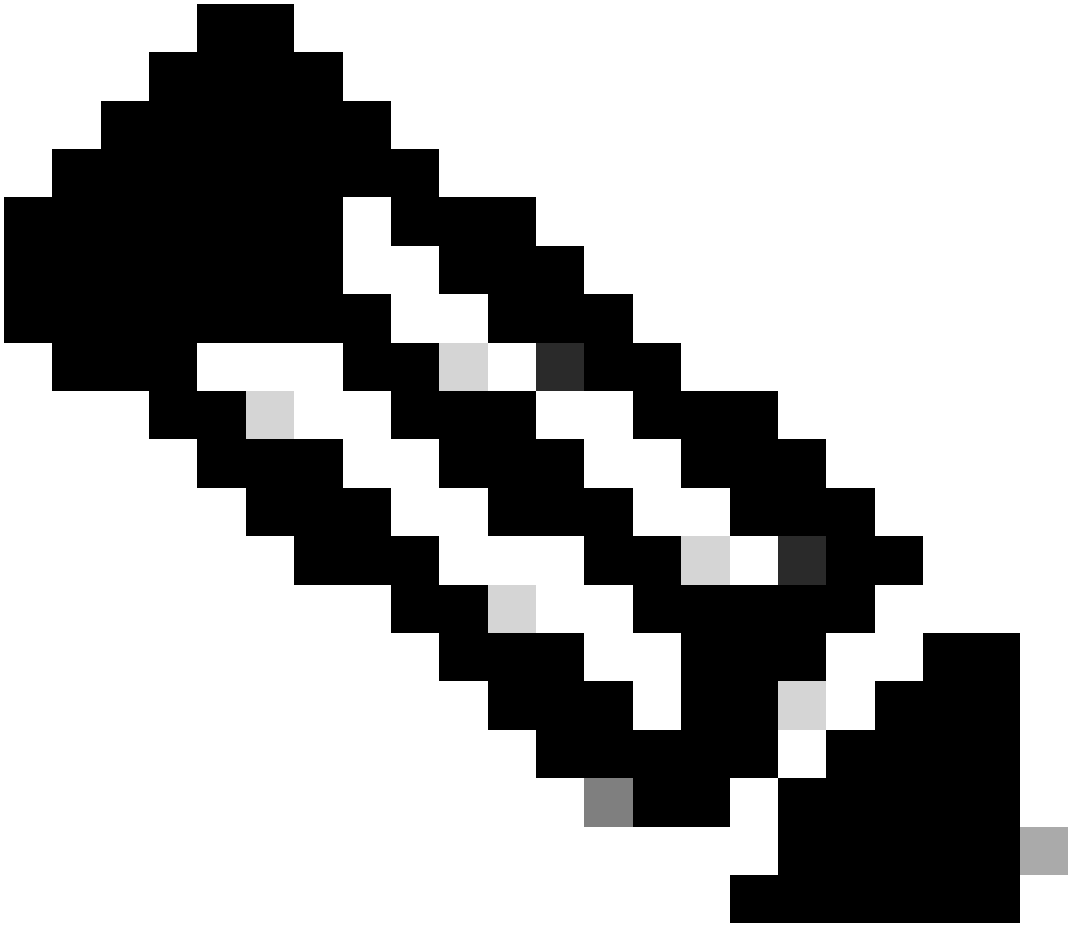
Problem 19: Dap.xml-Kopierfehler auf ASDM

Die Kopie von dap.xml auf ASA über das Dateiverwaltungsfenster in ASDM schlägt mit dem Fehler fehl: "disk0:/dap.xml ist eine spezielle Systemdatei. Hochladen einer Datei mit dem Namen dap.xml in disk0: ist nicht zulässig":



Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCvt62162 "dap.xml kann nicht mithilfe der Dateiverwaltung in ASDM 7.13.1 kopiert werden". Die Problemumgehung besteht darin, die Datei mithilfe von Protokollen wie FTP oder TFTP direkt auf die ASA zu kopieren.



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 20. Keine IKE-Richtlinien und IPSEC-Vorschläge auf ASDM sichtbar

Der ASDM zeigt keine IKE-Richtlinien und IPSEC-Vorschläge im Fenster Konfigurationen > Site-to-Site-VPN an.

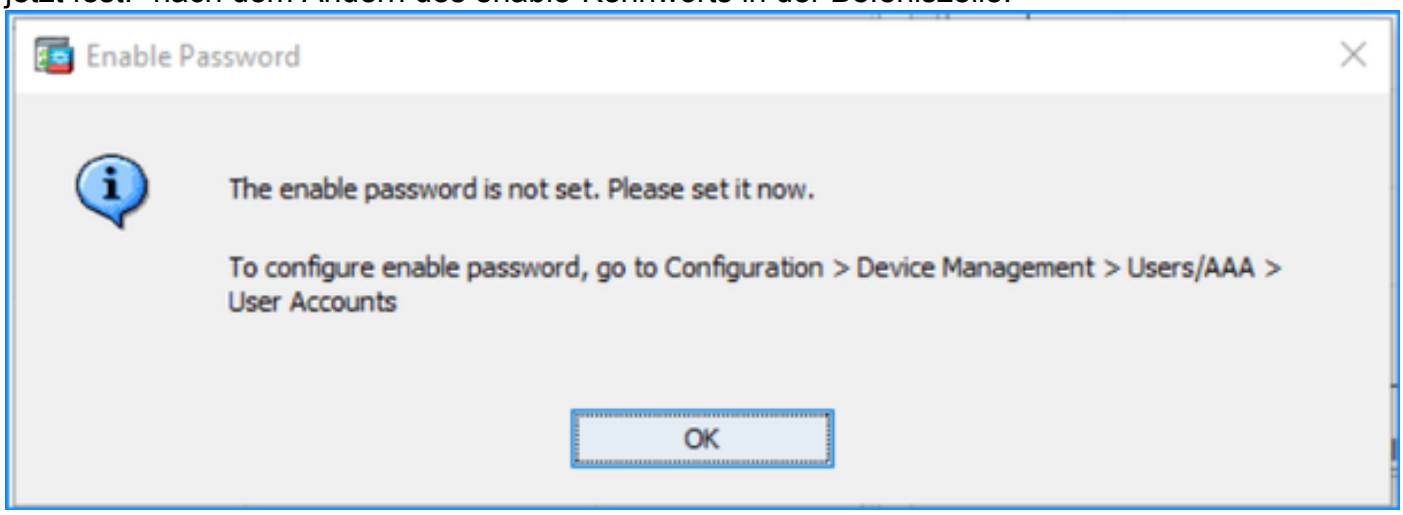
Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCwm42701 "ASDM display blank in IKE policies and IPSEC offer tab" (ASDM-Anzeige auf der Registerkarte "IKE-Richtlinien und IPSEC-Vorschläge").

Problem 21. ASDM zeigt die Meldung an, dass das Aktivierungskennwort nicht

festgelegt wurde. Bitte legen Sie es jetzt fest."

ASDM zeigt die Meldung an, dass das enable-Kennwort nicht festgelegt wurde. Bitte legen Sie es jetzt fest." nach dem Ändern des enable-Kennworts in der Befehlszeile:



Fehlerbehebung - empfohlene Maßnahmen

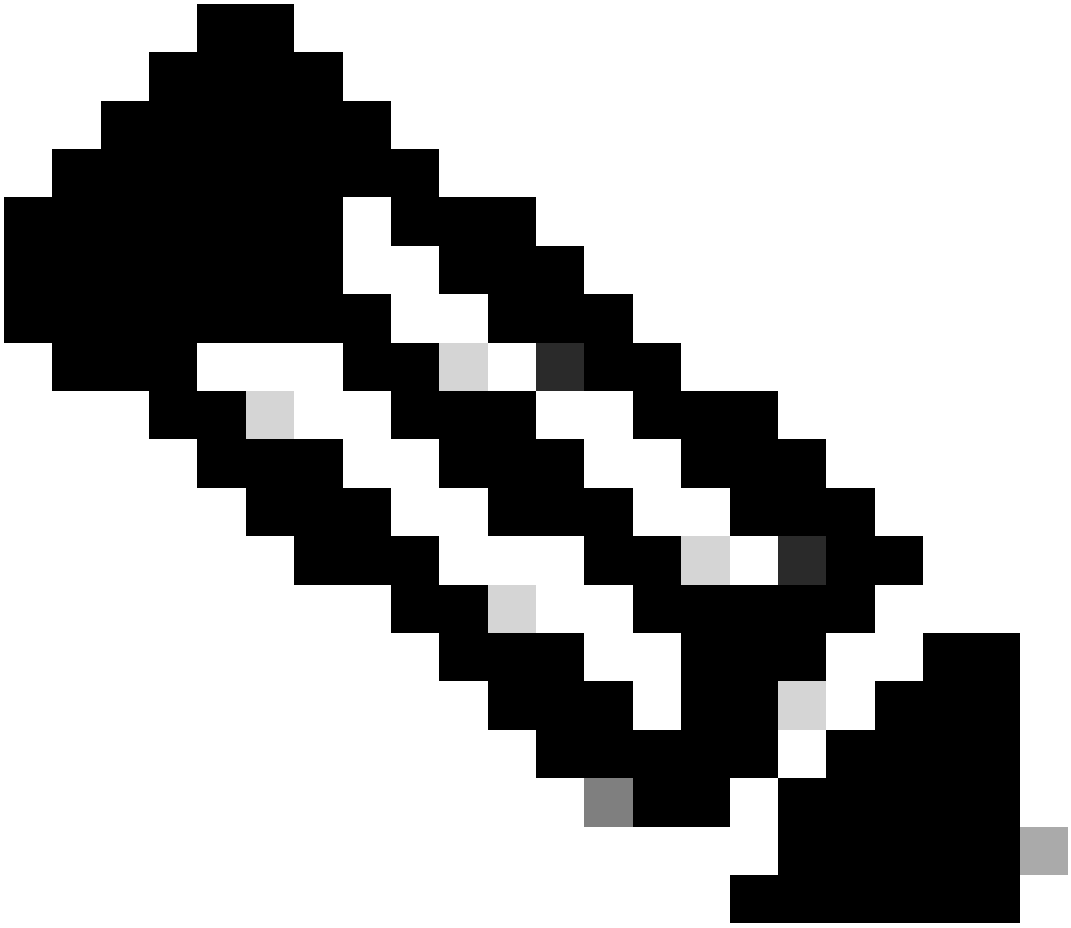
Weitere Informationen finden Sie unter der Software-Bug-ID CSCvq42317 "ASDM prompts to change enable password after it was set on CLI" (ASDM-Aufforderungen zum Ändern des Aktivierungskennworts, nachdem es für CLI festgelegt wurde).

Problem 22: ASDN-Objekt verschwindet nach Aktualisierung der ASDM-Benutzeroberfläche

Beim Hinzufügen einer Objektgruppe und eines Objekthosts zu einer vorhandenen Objektgruppe und nach der Aktualisierung des ASDM wird die Objektgruppe aus der ASDM-Liste entfernt. Die Objektnamen müssen mit Zahlen beginnen, damit dieser Defekt übereinstimmt.

Fehlerbehebung - empfohlene Maßnahmen

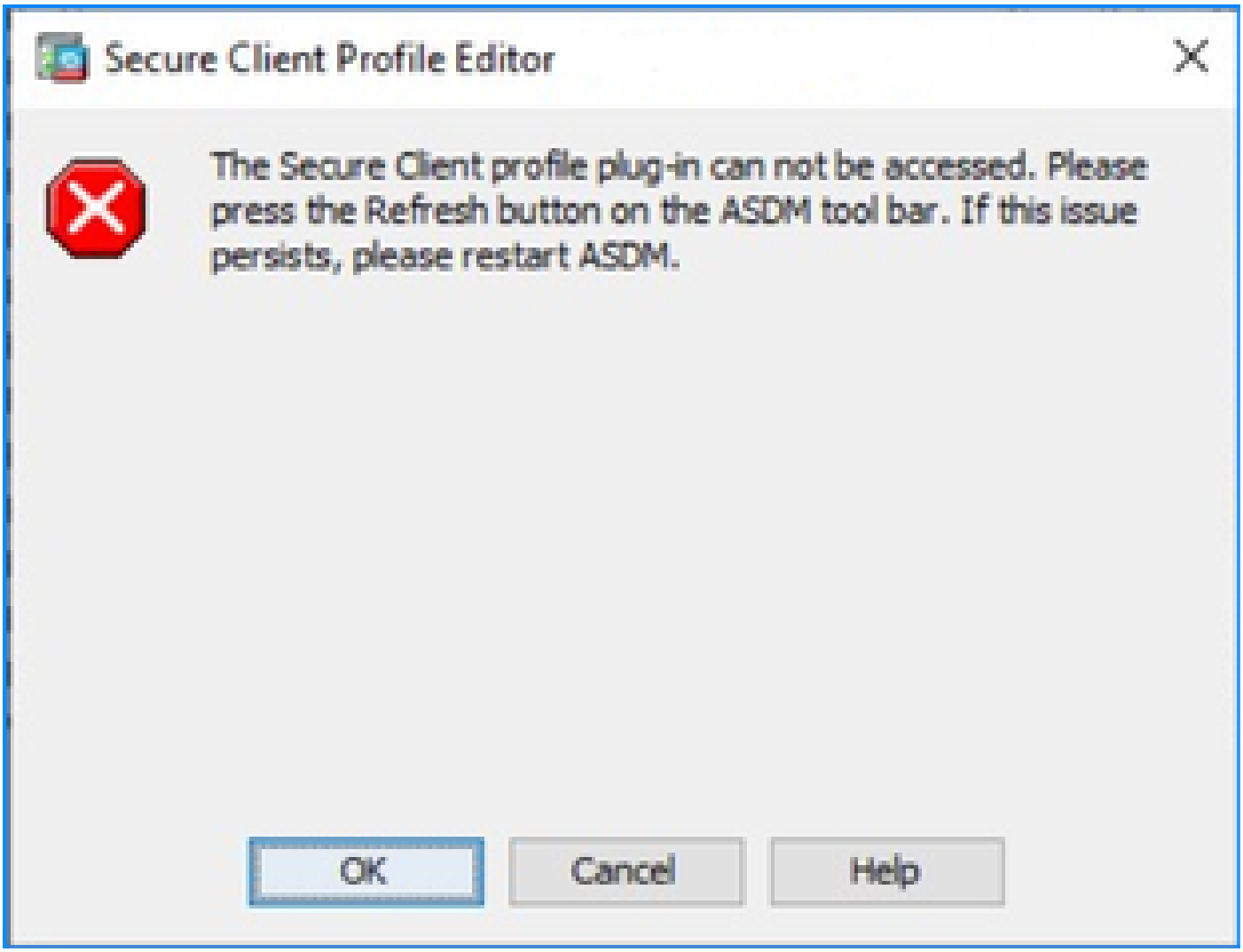
Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCwf71723 "ASDM lost configured objects/object groups" (ASDM verliert konfigurierte Objekte/Objektgruppen).



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

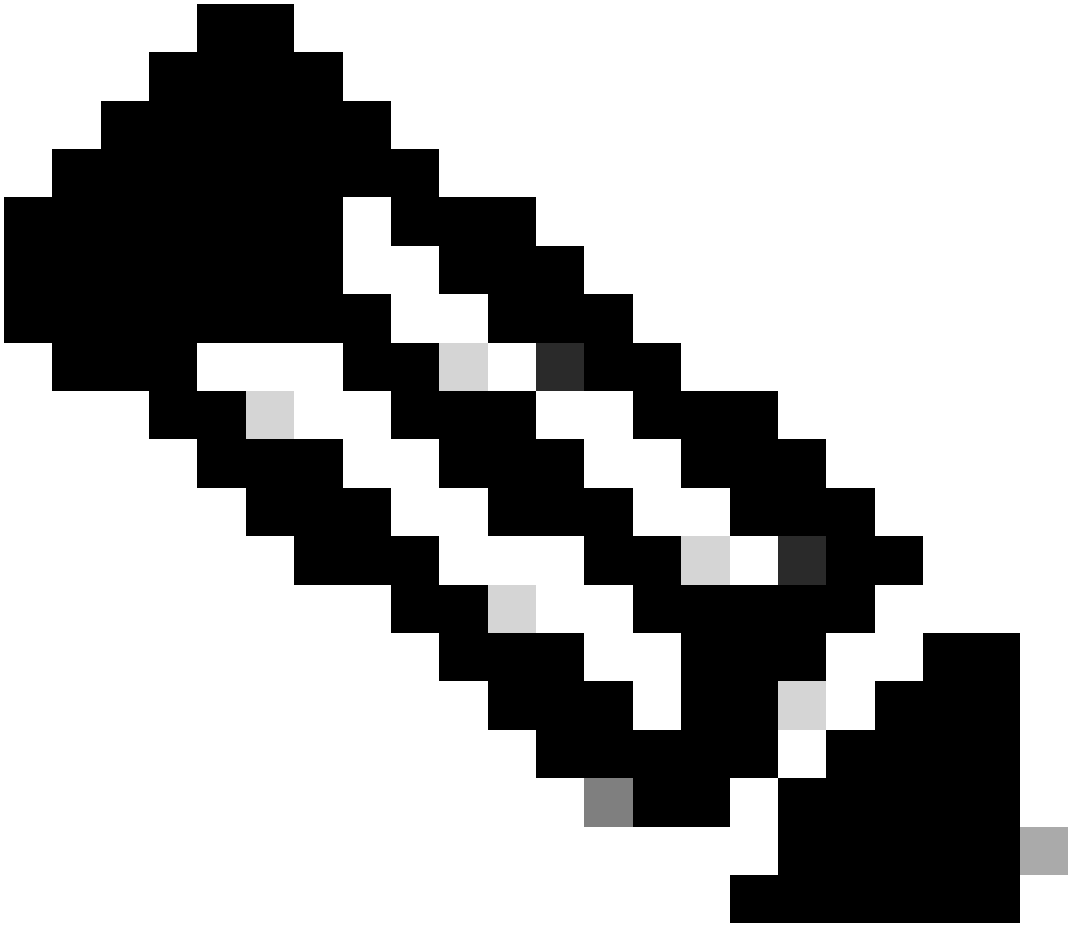
Problem 23. AnyConnect-Clientprofile für Versionen vor 4.5 können nicht bearbeitet werden.

Die AnyConnect-Clientprofile können nicht für AnyConnect-Profile vor Version 4.5 bearbeitet werden. Die Fehlermeldung lautet "Auf das Secure Client-Profil-Plug-in kann nicht zugegriffen werden. Klicken Sie in der ASDM-Symbolleiste auf die Schaltfläche "Aktualisieren". Wenn das Problem weiterhin besteht, starten Sie ASDM neu.":



Fehlerbehebung - empfohlene Maßnahmen

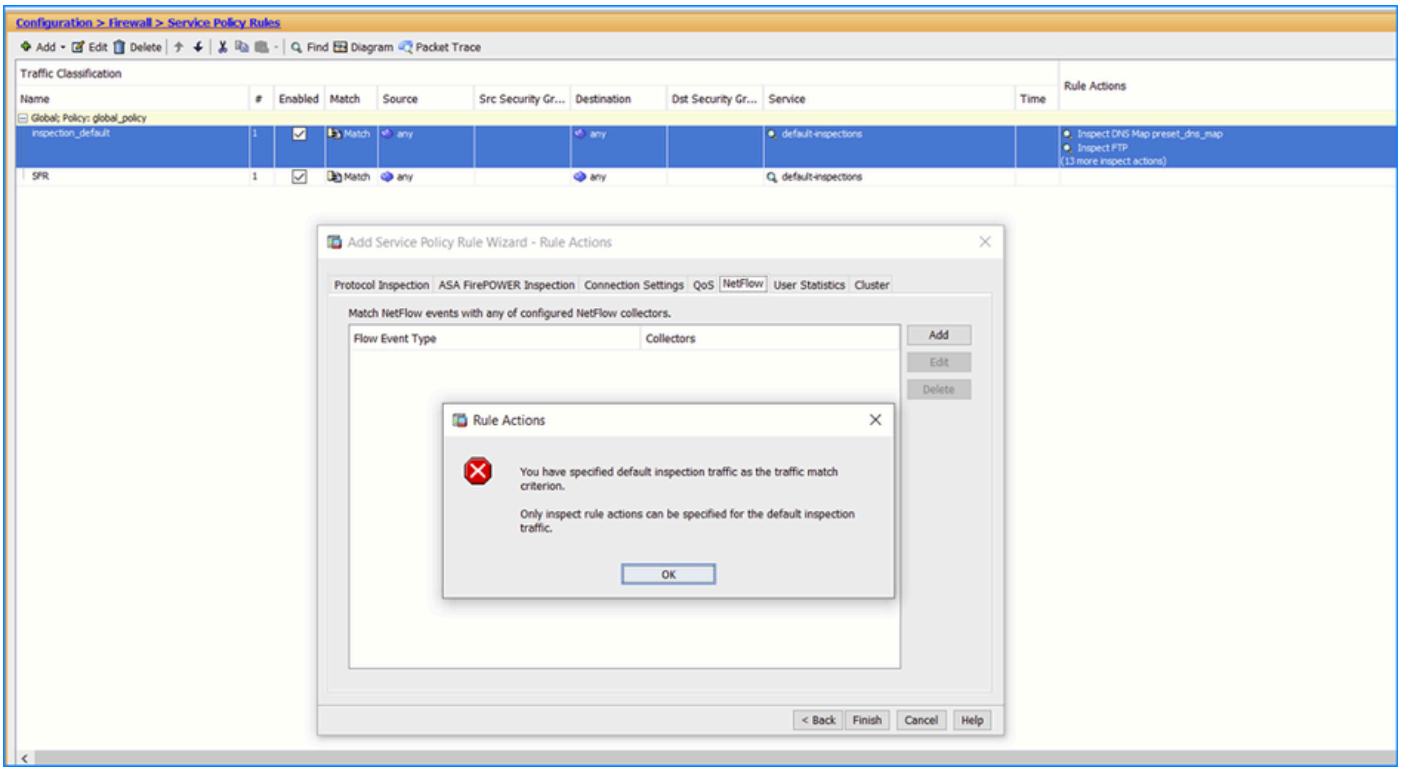
Weitere Informationen finden Sie unter der Software Cisco bug ID CSCwf16947 "ASDM - Cannot load AnyConnect Profile Editor" (ASDM - Anyconnect Profile Editor kann nicht geladen werden).



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

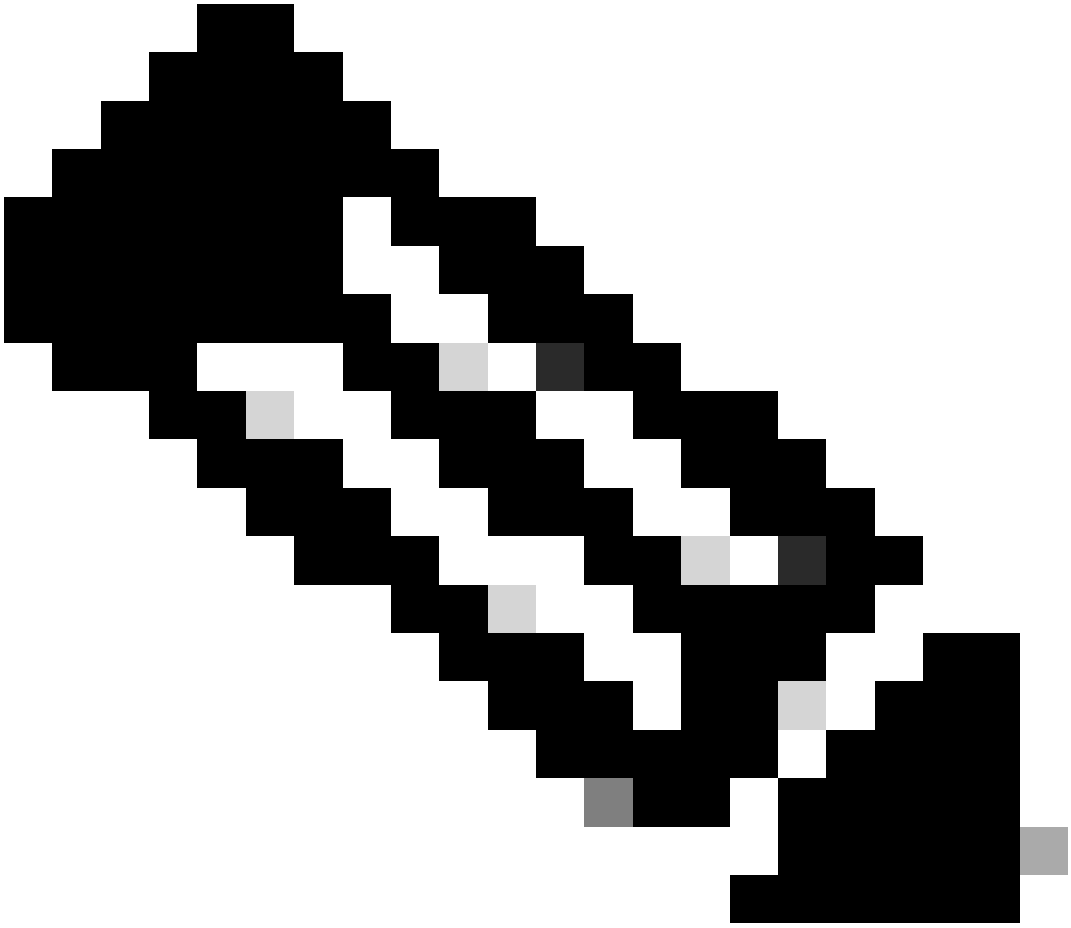
Problem 24. Es kann nicht zur Registerkarte "Servicerichtlinie bearbeiten" > "Regelaktionen" > "ASA FirePOWER-Inspektion" navigiert werden.

In ASDM Version 7.8.2 können Benutzer nicht zur Registerkarte "Edit Service Policy > Rule Actions > ASA FirePOWER Inspection" navigieren. Der Fehler wird angezeigt: "Sie haben als Kriterium für die Datenverkehrsübereinstimmung den standardmäßigen Überprüfungsdatenverkehr festgelegt. Für den Standardprüfungsverkehr können nur Prüfregelaktionen angegeben werden." Dies gilt auch dann, wenn eine ACL für die Umleitung ausgewählt wurde:



Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCvg15782 "ASDM - Cannot view modified SFR traffic redirection after upgrade to version 7.8(2)" (ASDM - Änderung der SFR-Datenverkehrsumleitung nach dem Upgrade auf Version 7.8(2) konnte nicht angezeigt werden). Die Problemumgehung besteht darin, die Konfiguration der Richtlinienzuordnung mithilfe der CLI zu bearbeiten.



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 25. AnyConnect Image Version 5.1 und AnyConnect-Profil-Editor auf ASDM

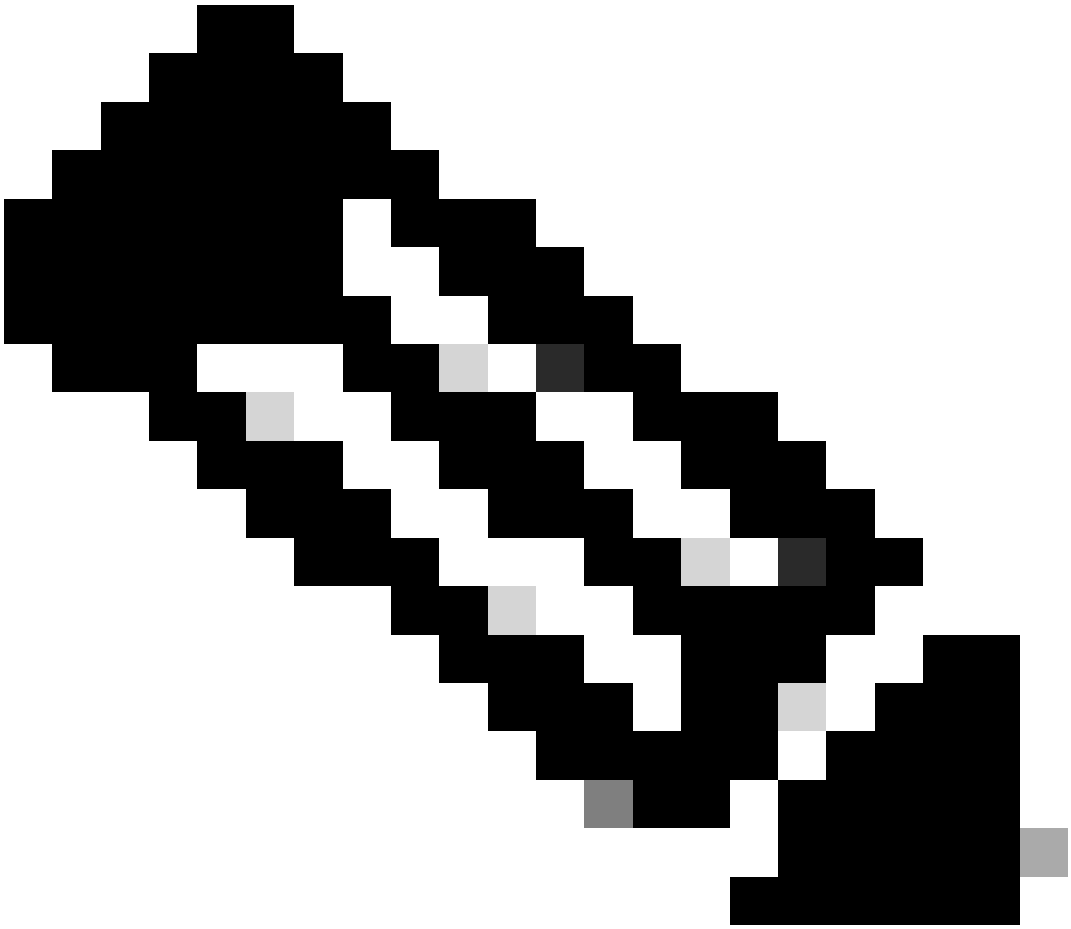
Diese Symptome treten bei Version 5.1 der Secure Client-Software auf:

1. Die Namen der Gruppenrichtlinienmodule werden beim Laden der Win/Mac/Linux-Pakete nicht aufgeführt.
2. ASDM kann AnyConnect Profile Editor nicht öffnen.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCwh74417 "ASDM :

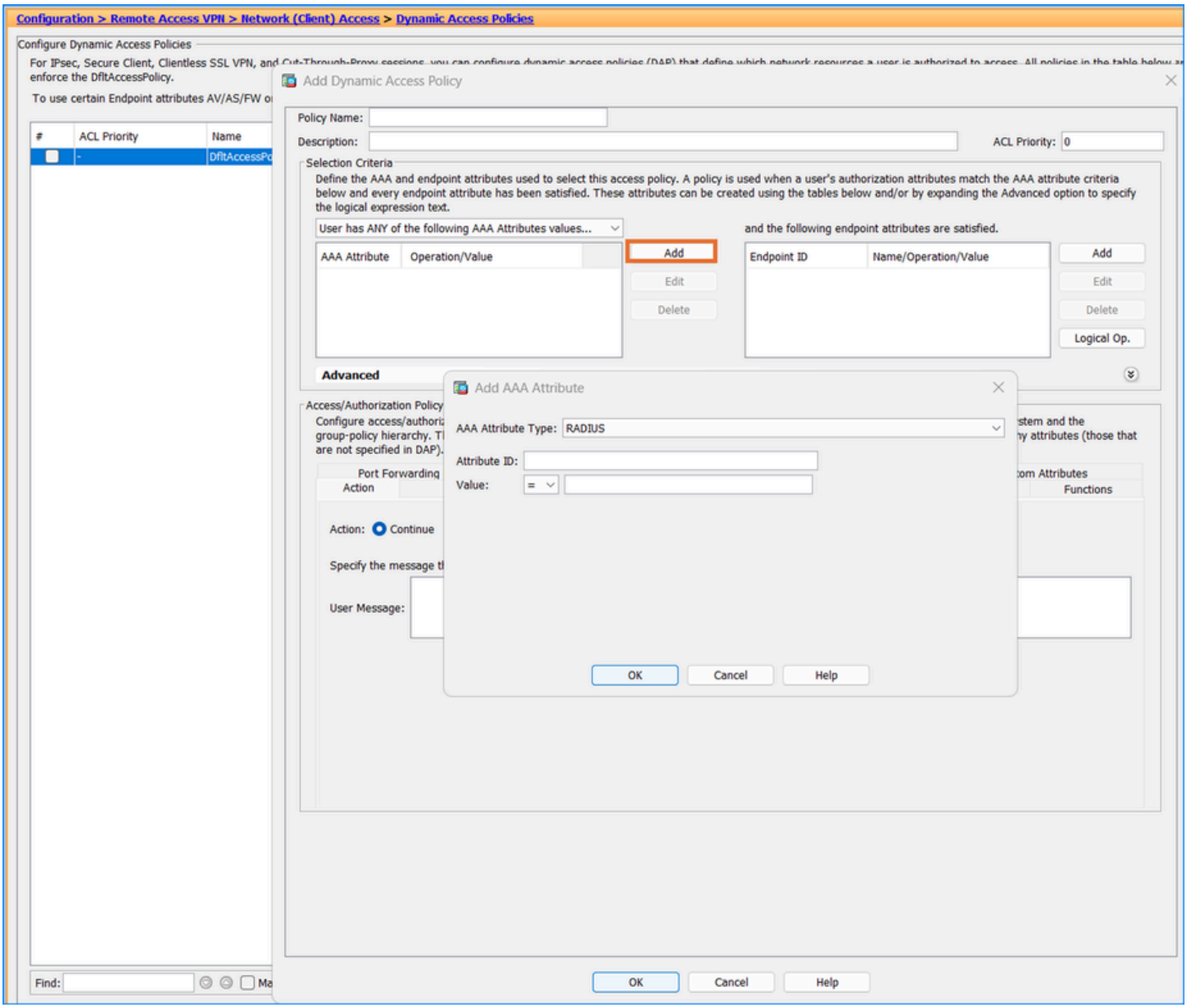
AnyConnect Profile Editor und Group Policy können bei Verwendung des CSC Image 5.1" nicht geladen werden. Die Problemumgehung besteht darin, niedrigere Versionen des sicheren Clients zu verwenden.



> Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

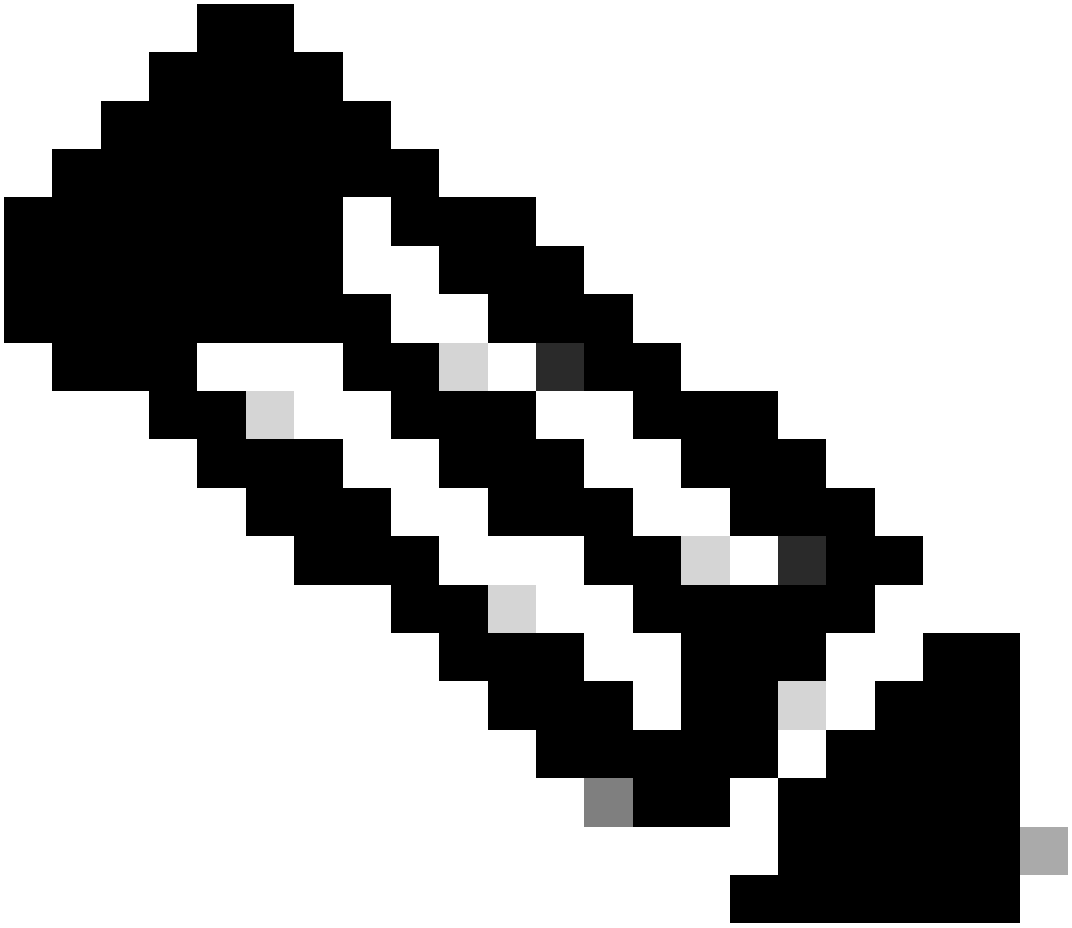
Problem 26: AAA-Attributtypen (Radius/LDAP) sind in ASDM nicht sichtbar

AAA-Attributtypen (Radius/LDAP) sind in ASDM > Konfiguration > Remote Access VPN > Netzwerkzugriff (Client) > dynamische Zugriffsrichtlinien nicht sichtbar > Hinzufügen > Bei AAA-Attributfeld > Hinzufügen > Radius oder LDAP auswählen:



Fehlerbehebung - empfohlene Maßnahmen

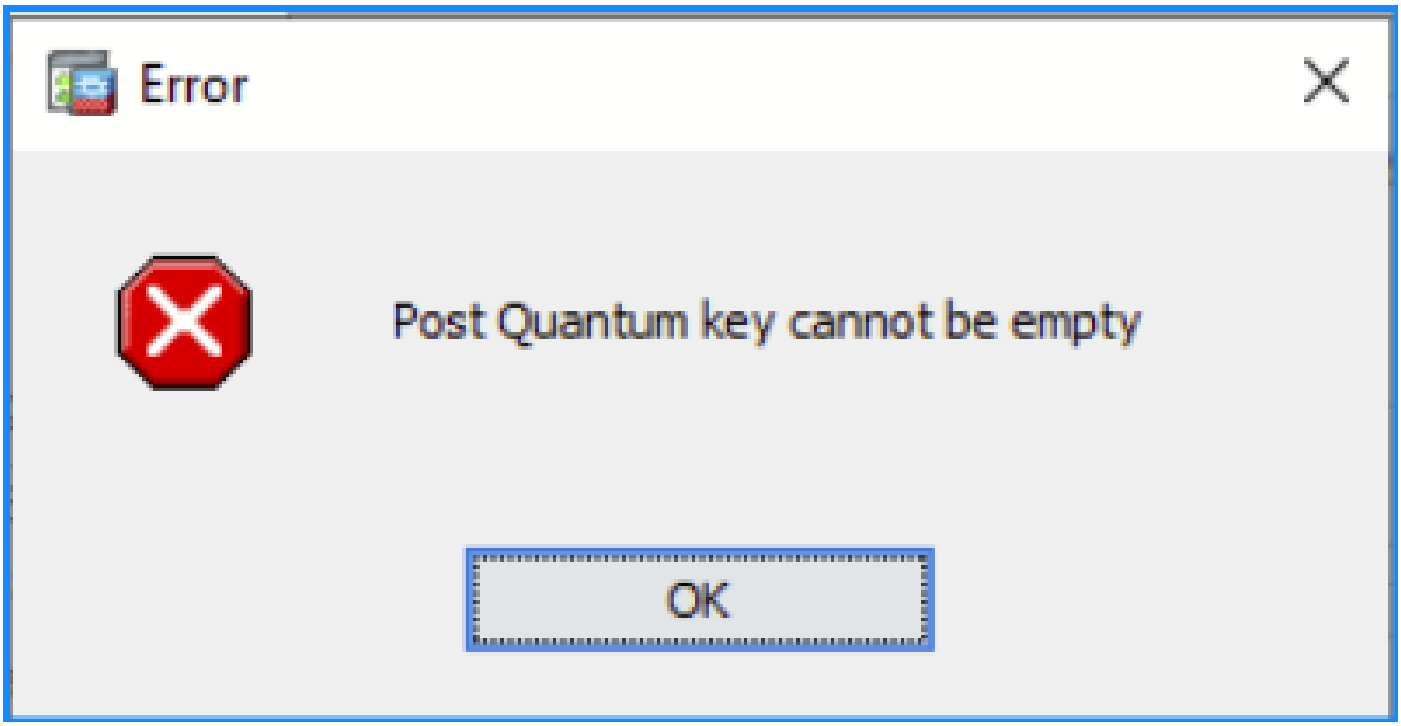
Weitere Informationen finden Sie unter der Software Cisco bug ID CSCwa99370 "ASDM : ASDM:DAP config missing AAA Attributes type (Radius/LDAP)" und Cisco Bug-ID CSCwd16386 "ASDM:DAP config missing AAA Attributes type (Radius/LDAP)".



Anmerkung: Diese Fehler wurden in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

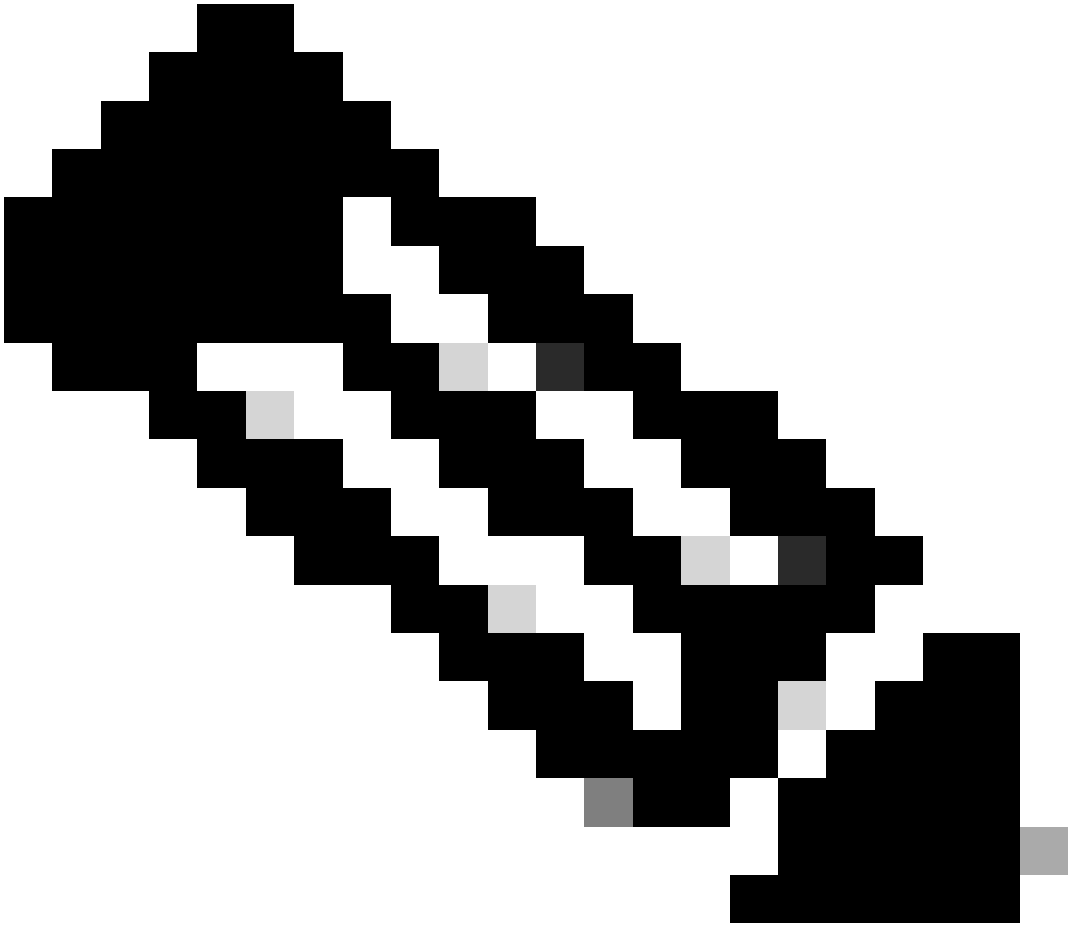
Problem 27: 'Der Post Quantum-Schlüssel darf nicht leer sein'-Fehler wird im ASDM angezeigt.

Die Fehlermeldung "Post Quantum key cannot be empty" wird angezeigt, wenn Sie den Abschnitt "Erweitert" unter "ASDM > Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client)> IPsec (IKEv2)-Verbindungsprofile" bearbeiten:



Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCwe58266 "ASDM IKev2 configuration - Post Quantum Key cannot be empty error message" (ASDM-IKev2-Konfiguration - Post Quantum Key darf nicht leer sein).



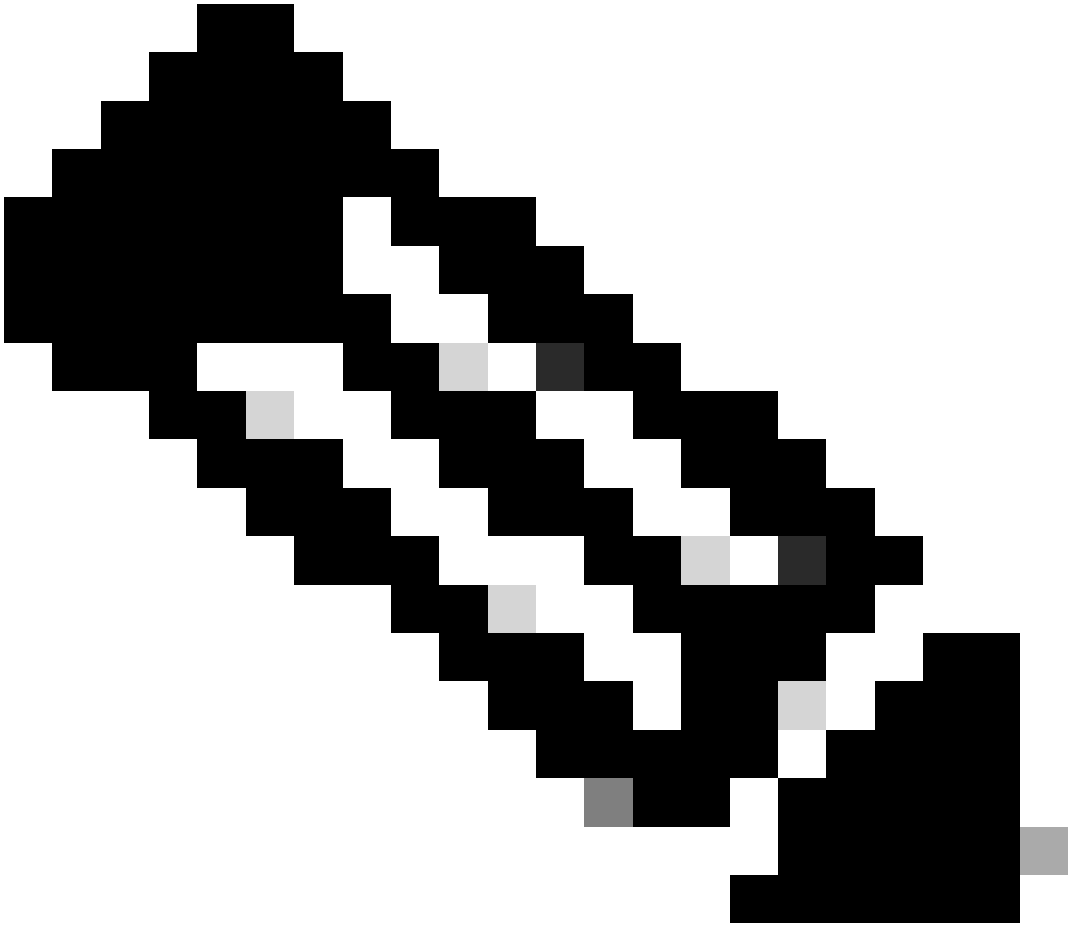
Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 28: ASDM zeigt bei Verwendung der Option "where used" (Wo verwendet) keine Ergebnisse an

ASDM zeigt keine Ergebnisse an, wenn die Option "where used" (Wo verwendet) verwendet wird, die Sie durch Navigieren zu Configuration > Firewall > Objects > Network Objects/Groups (Konfiguration > Objekte > Netzwerkobjekte/Gruppen) und Klicken mit der rechten Maustaste auf ein Objekt finden.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software-Bug-ID CSCwd98702 "Where used" (Wo verwendet) im ASDM Not Working (ASDM funktioniert nicht).



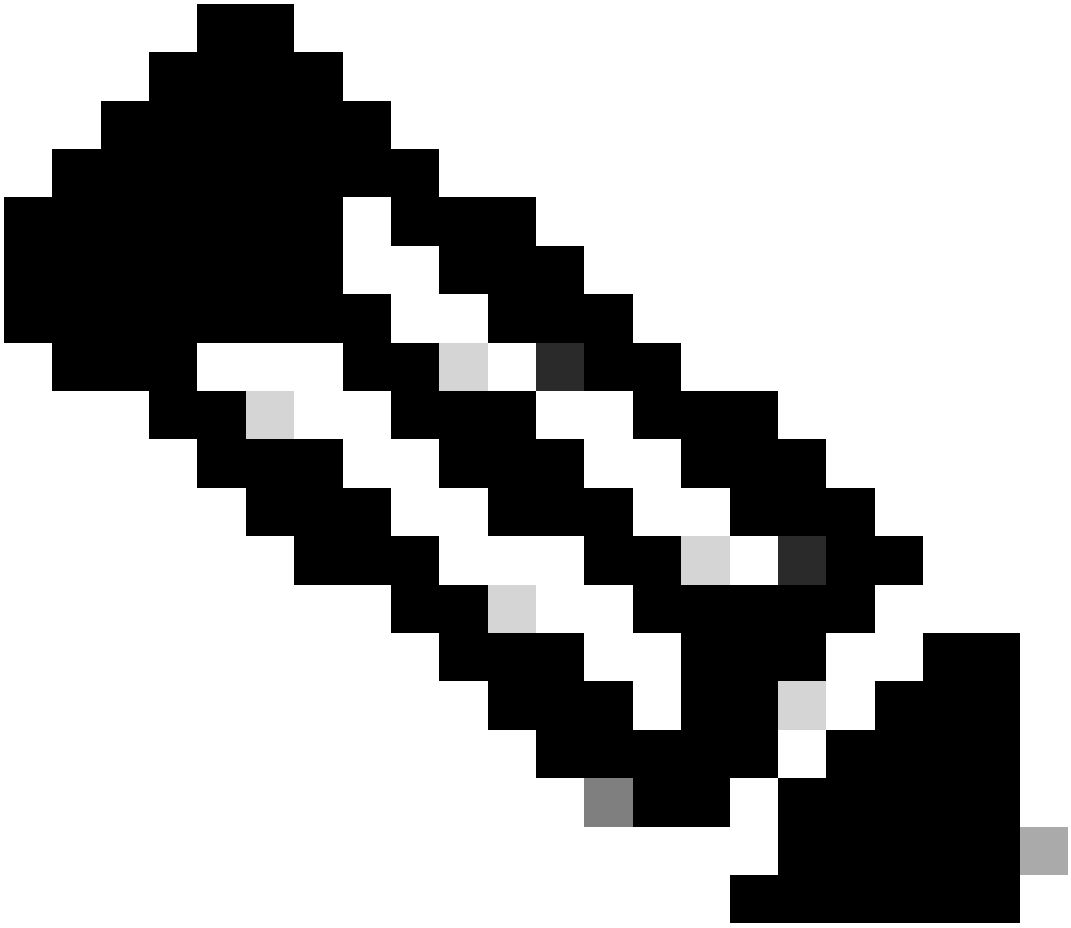
Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 29: Warnmeldung "[Network Object] cannot be delete, da es im Folgenden verwendet wird" beim Löschen eines Netzwerkobjekts

ASDM zeigt beim Löschen eines Netzwerkobjekts, auf das in einer Netzwerkgruppe in Configuration > Firewall > Objects > Network Objects/Groups verwiesen wird, nicht die folgende Warnmeldung an: "[Network Object] cannot be delete (Netzwerkobjekt] kann nicht gelöscht werden, da es nachfolgend verwendet wird).

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCwe67056 "[Network Object] cannot be delete, because it is used in the following" warning not appearing".



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problem 30: Probleme mit der Verwendbarkeit der Registerkarte "Netzwerkobjekte/Gruppe" in ASDM

Eines oder mehrere dieser Symptome wurden beobachtet:

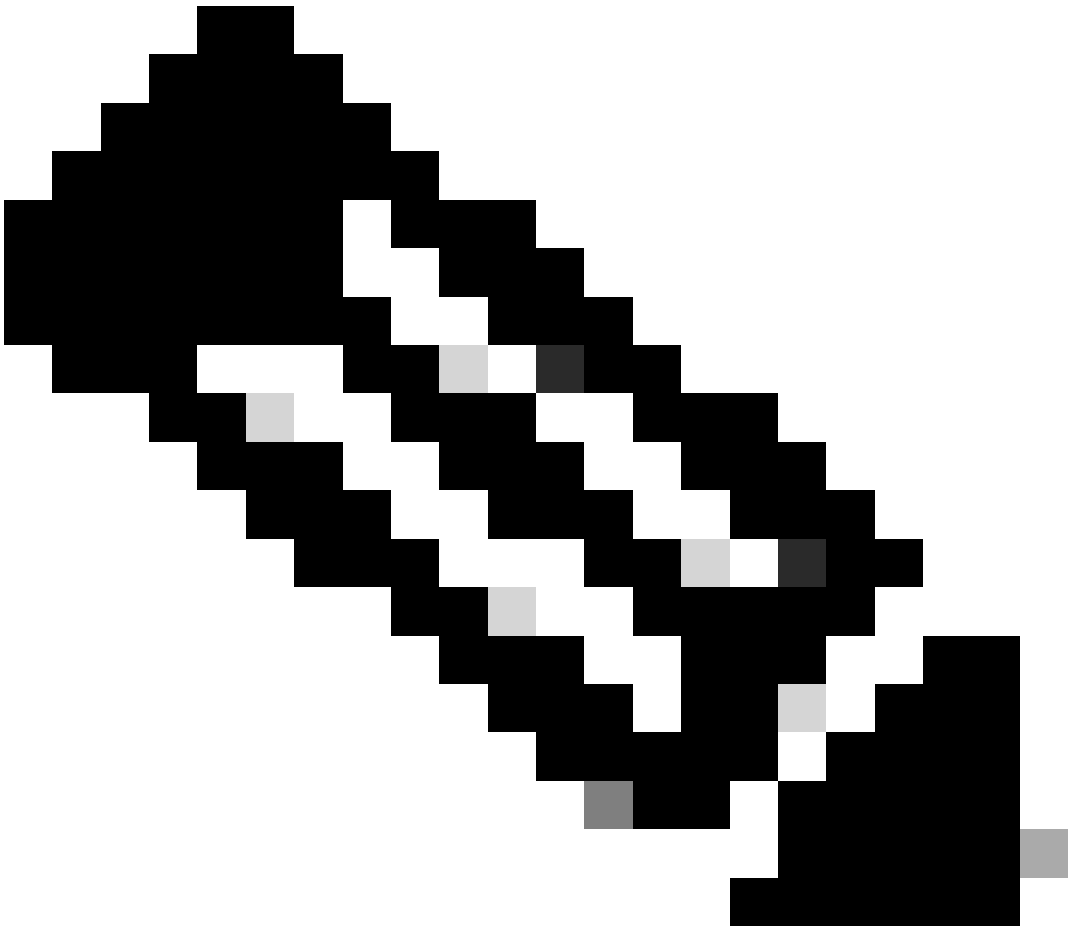
- Die Texteingabe "Name" im Bereich "Neues Objektmitglied erstellen" des Fensters "Objektgruppe hinzufügen/bearbeiten" ist als "optional" markiert. Die Schaltfläche "Hinzufügen>>" zum Erstellen und Hinzufügen des Objekts ist jedoch deaktiviert, es sei denn, es wurde ein Name eingegeben.
- Die Registerkarte "Usages" (Nutzung), die geöffnet wird, wenn ein Benutzer auf "Where Used..." (Wo verwendet) klickt. Im Kontextmenü werden nur Entitäten (ACLs, Routenzuordnungen, Objektgruppen) aufgelistet, die direkt auf das Objekt verweisen. Es muss auch rekursiv Liste zweite, dritte, und so weiter. Order-Referenzen (d. h. eine ACL, die

eine Objektgruppe verwendet, die ein Objekt enthält, muss auch als "Usage" des Object aufgeführt sein).
- Dieses Verhalten wird auch durch den im Kontextmenü verfügbaren Vorgang "Löschen" angezeigt. Sie löscht automatisch alle Entitäten, die direkt auf das Objekt verweisen (wenn die Entität leer würde, wenn das Objekt gelöscht wird). Es funktioniert nicht so, wenn ein zweiter, dritter, und so weiter. Der Ordnungsbezug würde leer, wenn das Objekt und der erste Ordnungsbezug gelöscht würden.

Der Benutzer kann zu der Annahme verleitet werden, dass ASDM Entitäten verhindert, die aufgrund des Löschens des Objekts aus der verbleibenden Konfiguration leer werden würden. Dies ist jedoch nicht notwendigerweise der Fall.

Fehlerbehebung - empfohlene Maßnahmen

Weitere Informationen finden Sie unter der Software Cisco Bug-ID CSCwe86257 "Usability of Network Objects/Group Tab in ASDM".

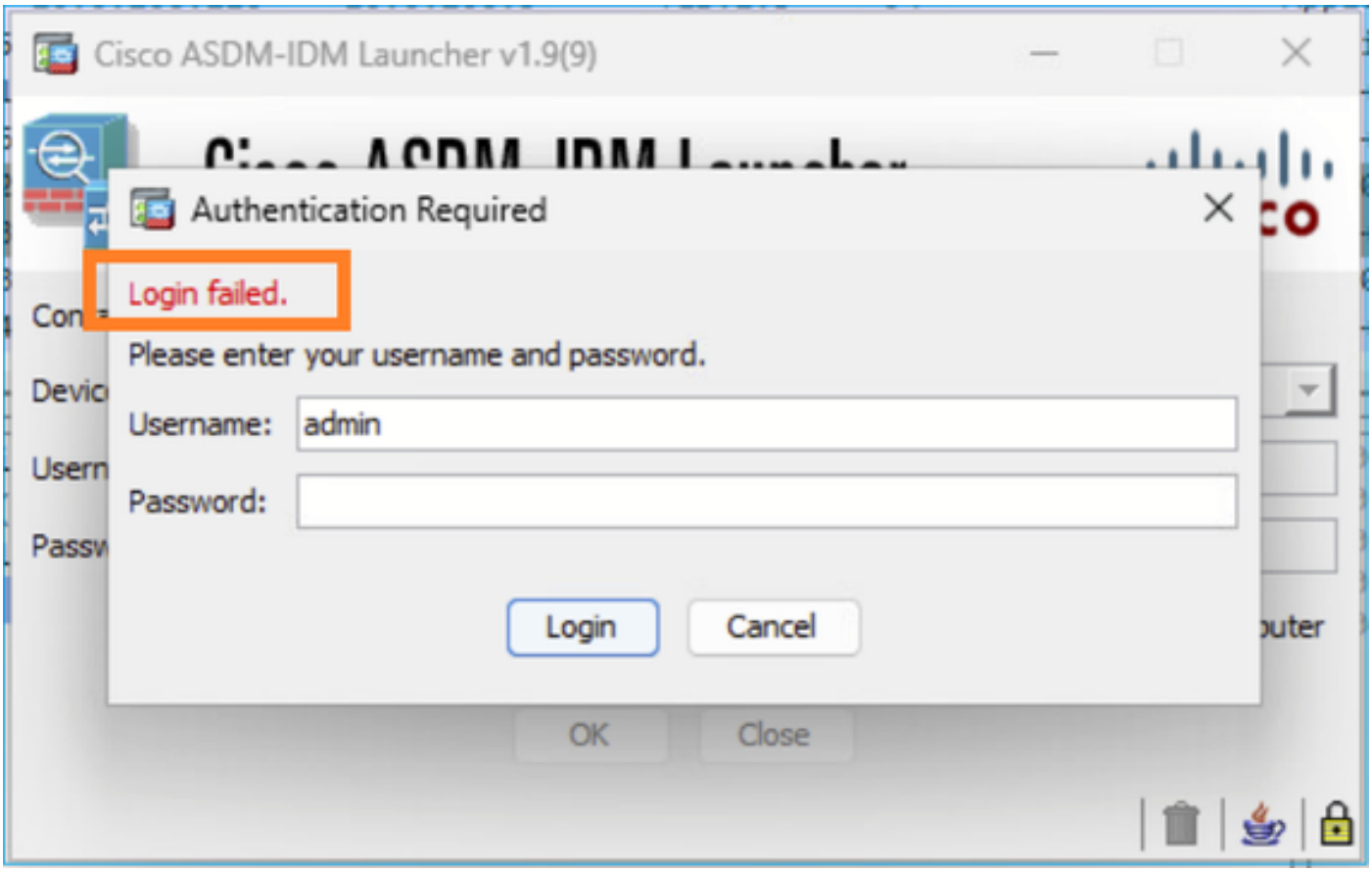


Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Fehlerbehebung bei ASDM-Authentifizierungsproblemen

Problem 1. ASDM-Anmeldung fehlgeschlagen

Der auf der ASDM-Benutzeroberfläche angezeigte Fehler ist:



Fehlerbehebung - empfohlene Maßnahmen

Dieser Fehler tritt auf, wenn sowohl HTTP als auch WebVPN Cisco Secure Client (AnyConnect) auf derselben Schnittstelle aktiviert sind. Daher müssen alle Voraussetzungen erfüllt sein:

1. AnyConnect/Cisco Secure Client ist auf einer Schnittstelle aktiviert.
2. Der HTTP-Server wird über dieselbe Schnittstelle und denselben Port wie AnyConnect/Cisco Secure Client aktiviert.

Beispiel:

<#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
```

Tipp zur Fehlerbehebung: Aktivieren Sie 'debug http 255', und Sie können den Konflikt zwischen ASDM und WebVPN sehen:

<#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
```

Nebenbei bemerkt zeigen die ASA-Syslogs trotz fehlgeschlagener Anmeldung, dass die Authentifizierung erfolgreich ist:

<#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

Problemumgehungen

Problemumgehung 1

Ändern Sie den TCP-Port für den ASA HTTP-Server. Beispiel:

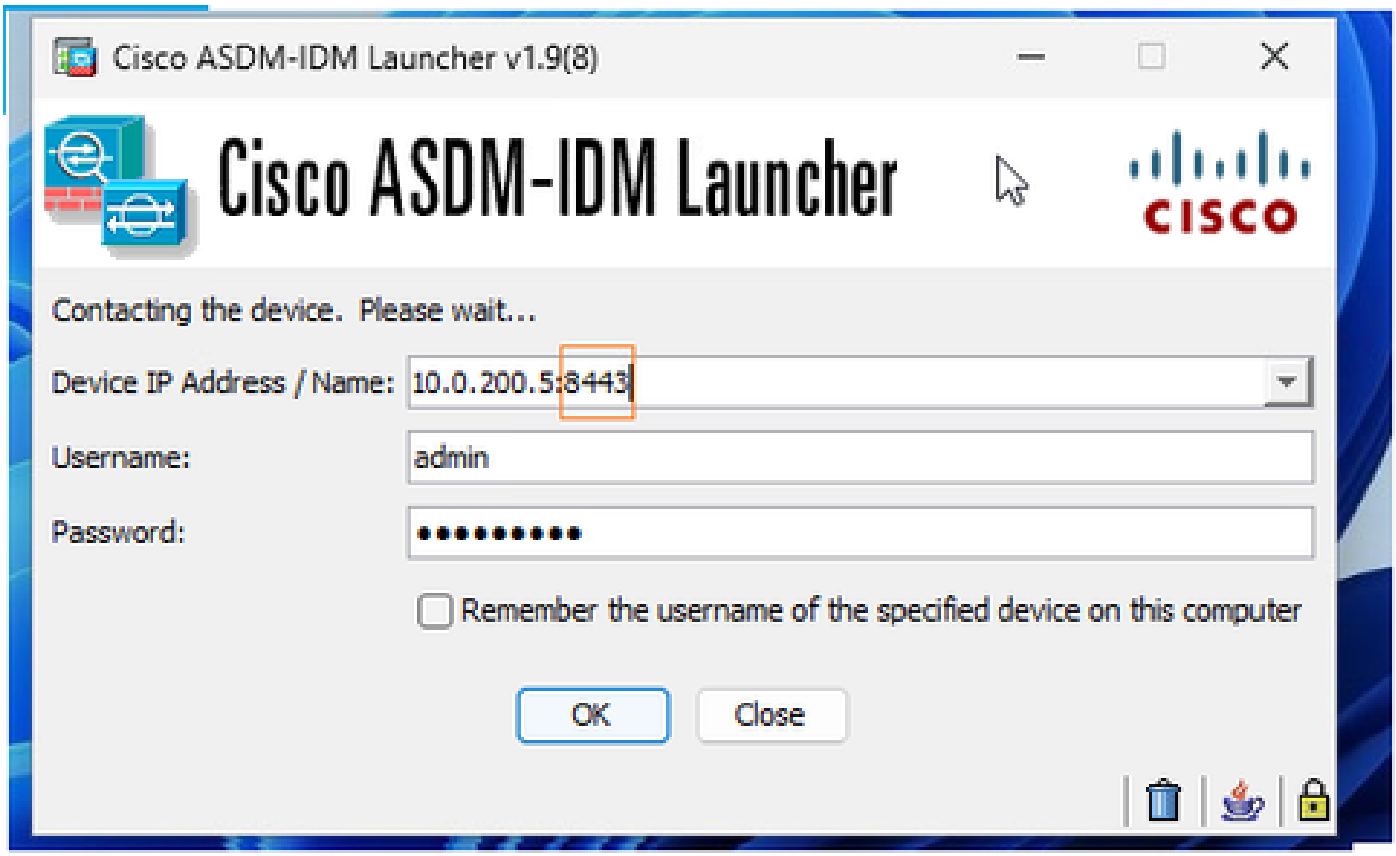
<#root>

ciscoasa#

configure terminal

ciscoasa(config)#

http server enable 8443



Problemumgehung 2

Ändern Sie den TCP-Port für AnyConnect/Cisco Secure Client, z. B.:

<#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
```

Problemumgehung 3

Eine alternative Problemumgehung besteht darin, die Konfiguration der "aaa authentication http

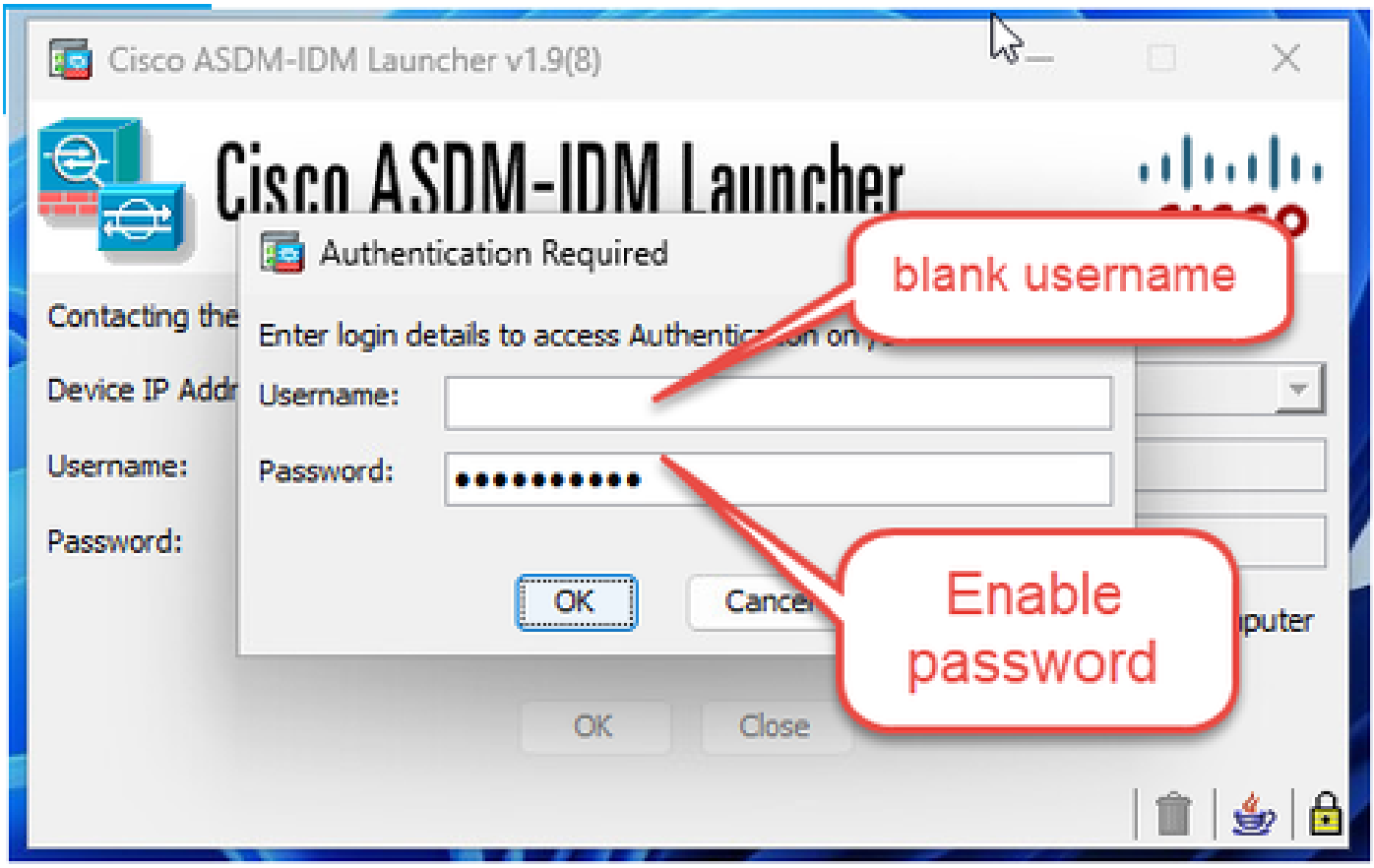
console" zu entfernen:

<#root>

```
ciscoasa(config)#
```

```
no aaa authentication http console LOCAL
```

In diesem Fall können Sie sich beim ASDM anmelden, indem Sie das folgende enable-Kennwort verwenden:



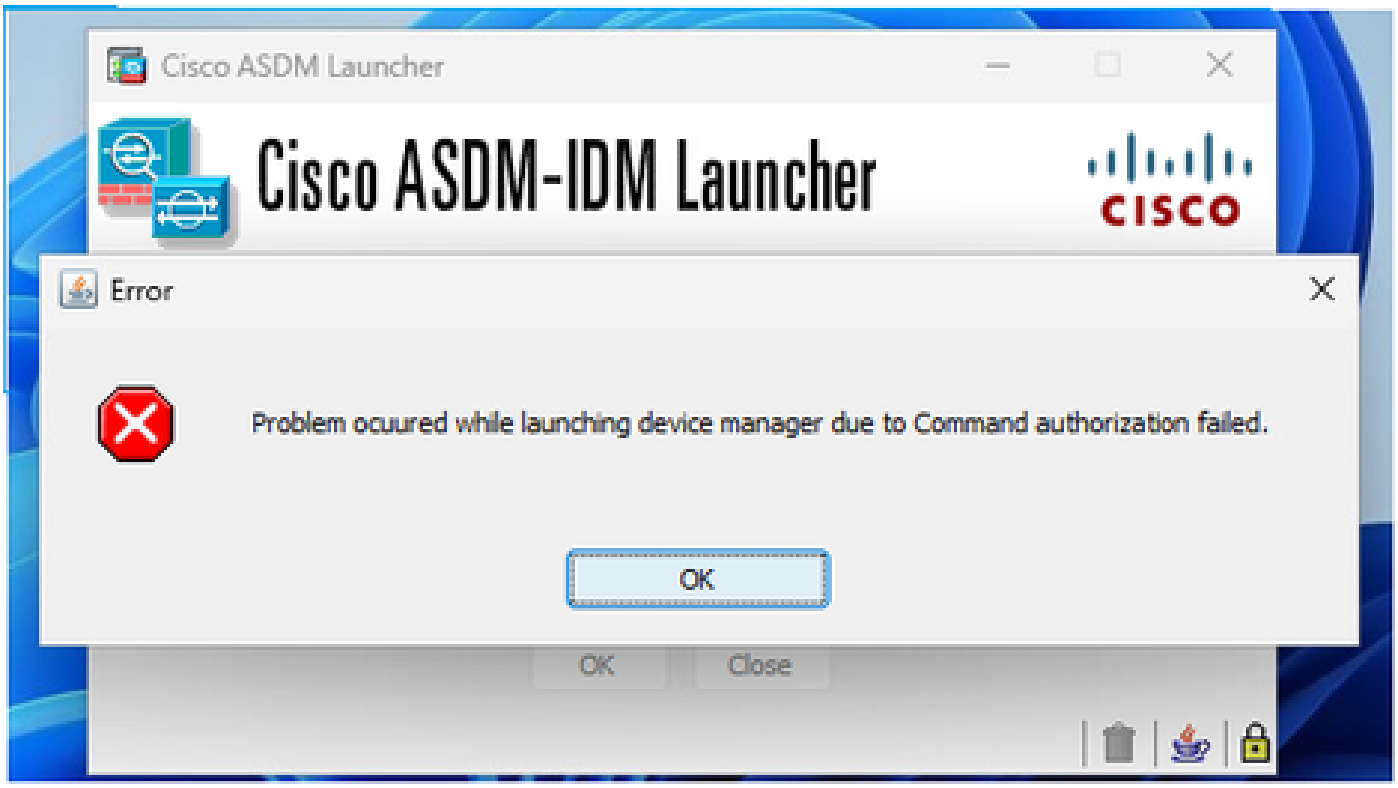
Zugehöriger Fehler

Cisco Bug-ID CSCwb67583

Hinzufügen einer Warnung, wenn Web-VPN und ASDM auf derselben Schnittstelle aktiviert sind

Problem 2: Fehler bei der ASDM-Befehlsautorisierung

Der auf der ASDM-Benutzeroberfläche angezeigte Fehler ist:



Fehlerbehebung - Empfohlene Schritte

Überprüfen Sie Ihre AAA-Konfiguration auf ASA-Geräten und stellen Sie sicher, dass:

- Sie haben auch eine Authentifizierung konfiguriert.
- Wenn Sie einen Remote-Authentifizierungsserver verwenden, ist dieser erreichbar und autorisiert die Befehle.

Referenz

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

Problem 3: Konfigurieren des schreibgeschützten ASDM-Zugriffs

Manchmal möchten Sie ASDM-Benutzern schreibgeschützten Zugriff gewähren.

Fehlerbehebung - Empfohlene Schritte

Erstellen Sie einen neuen Benutzer mit einer benutzerdefinierten Berechtigungsebene (5), z. B.:

<#root>

```
asa(config)#
username [username] password [password] privilege 5
```

Mit diesem Befehl wird ein Benutzer mit der Berechtigungsebene 5 erstellt, die die Ebene "Monitoring-only" (Nur Überwachung) darstellt. Ersetzen Sie `[username]` und `[password]` durch den gewünschten Benutzernamen und das gewünschte Kennwort.

Details

Mit der lokalen Befehlsautorisierung können Sie Befehle einer von 16 Berechtigungsebenen (0 bis 15) zuweisen. Standardmäßig wird jeder Befehl entweder der Berechtigungsebene 0 oder 15 zugewiesen. Sie können für jeden Benutzer eine bestimmte Berechtigungsebene festlegen, und jeder Benutzer kann einen beliebigen Befehl auf der zugewiesenen Berechtigungsebene oder darunter eingeben. Die ASA unterstützt Benutzerberechtigungsstufen, die in der lokalen Datenbank, einem RADIUS-Server oder einem LDAP-Server definiert sind (wenn Sie RADIUS-Attributen LDAP-Attribute zuordnen).

Vorgehensweise

Schritt 1	Wählen Sie Configuration > Device Management > Users/AAA > AAA Access > Authorization aus.
Schritt 2	Aktivieren Sie das Kontrollkästchen Autorisierung für ASA-Befehlszugriff aktivieren > Aktivieren.
Schritt 3	Wählen Sie LOCAL aus der Dropdown-Liste Server Group (Servergruppe) aus.
Schritt 4	Wenn Sie die lokale Befehlsautorisierung aktivieren, haben Sie die Möglichkeit, einzelnen Befehlen oder Befehlsgruppen manuell Berechtigungsstufen zuzuweisen oder die vordefinierten Benutzerkontoberechtigungen zu aktivieren. • Klicken Sie auf ASDM-definierte Benutzerrollen festlegen, um vordefinierte Benutzerkontoberechtigungen zu verwenden. Das Dialogfeld Einrichtung von ASDM-definierten Benutzerrollen wird angezeigt. Klicken Sie auf Ja, um die vordefinierten Benutzerkontoberechtigungen zu verwenden: Admin (Berechtigungsebene 15, mit vollem Zugriff auf alle CLI-Befehle; Schreibgeschützt (Berechtigungsstufe 5 mit Schreibzugriff); und Monitor Only (Berechtigungsebene 3, mit Zugriff nur auf den Bereich Monitoring). • Klicken Sie auf Configure Command Privileges, um die Befehlsstufen manuell zu konfigurieren. Das Dialogfeld Command Privileges Setup wird angezeigt. Sie können alle Befehle anzeigen, indem Sie Alle Modi aus der Dropdown-Liste Befehlsmodus auswählen, oder Sie wählen einen Konfigurationsmodus aus, um die in diesem Modus verfügbaren Befehle anzuzeigen. Wenn Sie beispielsweise Kontext auswählen, können Sie alle

	Befehle anzeigen, die im Kontextkonfigurationsmodus verfügbar sind. Wenn ein Befehl im Benutzer-EXEC- oder privilegierten EXEC-Modus sowie im Konfigurationsmodus eingegeben werden kann und der Befehl in jedem Modus unterschiedliche Aktionen ausführt, können Sie die Berechtigungsstufe für diese Modi separat festlegen. In der Spalte Variant wird show, clear oder cmd angezeigt. Sie können die Berechtigung nur für die Form des Befehls show, clear oder configure festlegen. Die configure-Form des Befehls ist normalerweise die Form, die eine Konfigurationsänderung verursacht, entweder als unveränderter Befehl (ohne Präfix anzeigen oder löschen) oder als no-Form. Um die Ebene eines Befehls zu ändern, doppelklicken Sie darauf oder klicken Sie auf Bearbeiten. Sie können die Ebene zwischen 0 und 15 einstellen. Sie können nur die Privilegstufe des Hauptbefehls konfigurieren. Sie können z. B. die Ebene aller aaa-Befehle konfigurieren, nicht jedoch die Ebene des aaa-Authentifizierungs-Befehls und des aaa-Autorisierungs-Befehls. Um die Ebene aller angezeigten Befehle zu ändern, klicken Sie auf Alle auswählen und dann auf Bearbeiten. Klicken Sie auf OK, um Ihre Änderungen zu übernehmen.
Schritt 5	Klicken Sie auf Apply (Anwenden). Die Autorisierungseinstellungen werden zugewiesen und die Änderungen in der aktuellen Konfiguration gespeichert.

Referenz

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

Problem 4: ASDM Multi-Factor Authentication (MFA)

Fehlerbehebung - Empfohlene Schritte

Zum Zeitpunkt dieser Veröffentlichung bietet ASDM keine Unterstützung für MFA (oder 2FA). Diese Einschränkung umfasst MFA mit Lösungen wie PingID usw.

Referenz

Cisco Bug-ID CSCvs85995

ENH: ASDM-Zugang mit Zwei-Faktor-Authentifizierung oder MFA

Problem 5: Konfiguration der externen ASDM-Authentifizierung

Fehlerbehebung - Empfohlene Schritte

Sie können LDAP, RADIUS, RSA SecurID oder TACACS+ verwenden, um die externe Authentifizierung für ASDM zu konfigurieren.

Referenzen

- 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

Problem 6. Die lokale ASDM-Authentifizierung schlägt fehl.

Fehlerbehebung - Empfohlene Schritte

Wenn Sie die externe und die LOKALE Authentifizierung als Ausweichmöglichkeit verwenden, funktioniert die lokale Authentifizierung nur, wenn der externe Server ausgefallen ist oder nicht funktioniert. Nur in diesem Szenario übernimmt die LOKALE Authentifizierung und Sie können sich mit den LOKALEN Benutzern verbinden.

Dies liegt daran, dass die externe Authentifizierung Vorrang vor der LOKALEN Authentifizierung hat.

Beispiel:

<#root>

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

Referenz

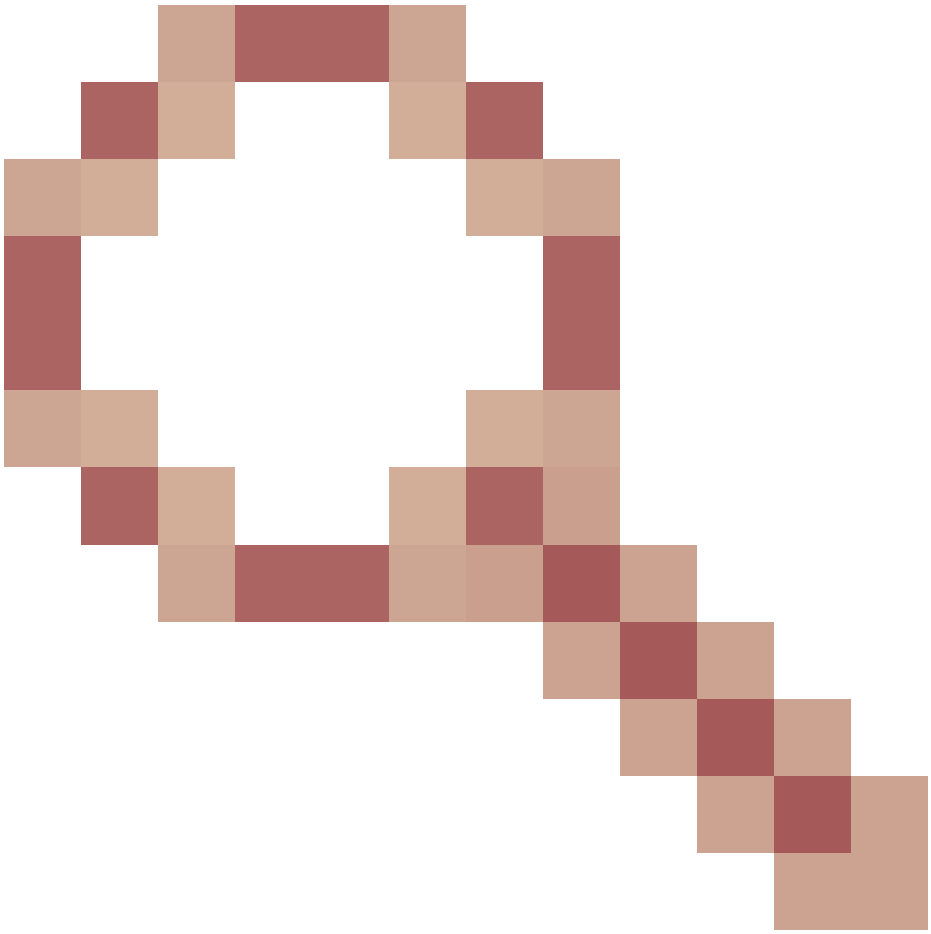
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

Problem 7. Einmaliges ASDM-Kennwort

Fehlerbehebung - Empfohlene Schritte

- Die Unterstützung für ASDM OTP-Authentifizierung (einmaliges Kennwort) wurde in der ASA-Version 8.x - 9.x und nur im Single-Routing-Modus hinzugefügt.
- Die ASDM-OTP-Authentifizierung für den transparenten Modus der ASA-Firewall und/oder

den Multi-Context-Modus fällt nicht in diese Kategorie.



Siehe Cisco Bug-ID CSCtf23419
ENH: Unterstützung der ASDM OTP-Authentifizierung im Multi-Kontext- und transparenten Modus

Problem 8. Im Verbindungsprofil werden nicht alle Methoden angezeigt.

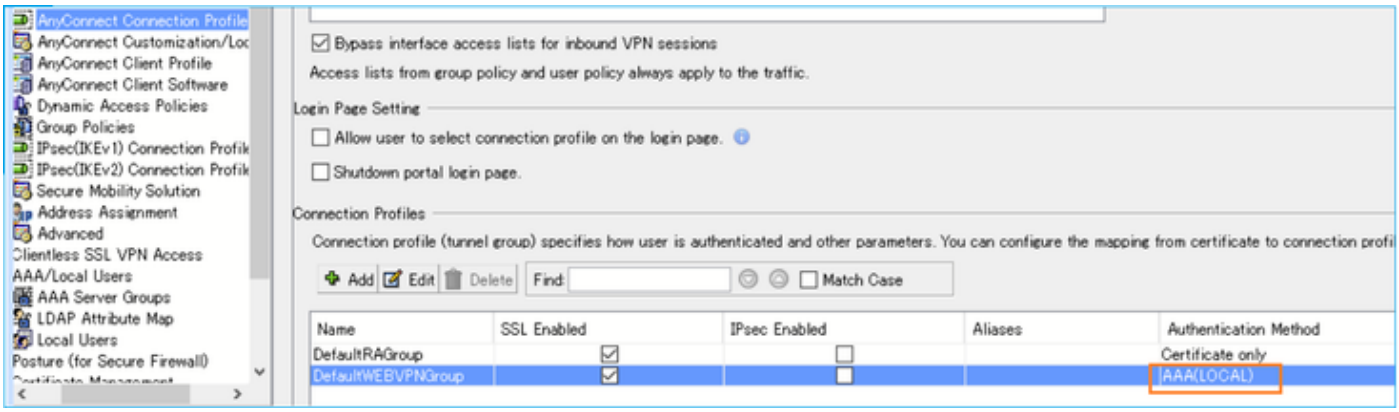
Das Problem besteht in diesem Fall in einer Diskrepanz zwischen der ASA CLI-Konfiguration und der ASDM-Benutzeroberfläche.

Die Kommandozeile bietet folgende Funktionen:

<#root>

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication aaa certificate
```

Während die ASDM-Benutzeroberfläche die Zertifikatmethode nicht erwähnt:



Fehlerbehebung - Empfohlene Schritte

Das ist ein kosmetisches Problem. Die Methode wird nicht im ASDM angezeigt, es wird jedoch die Zertifikatsauthentifizierung verwendet.

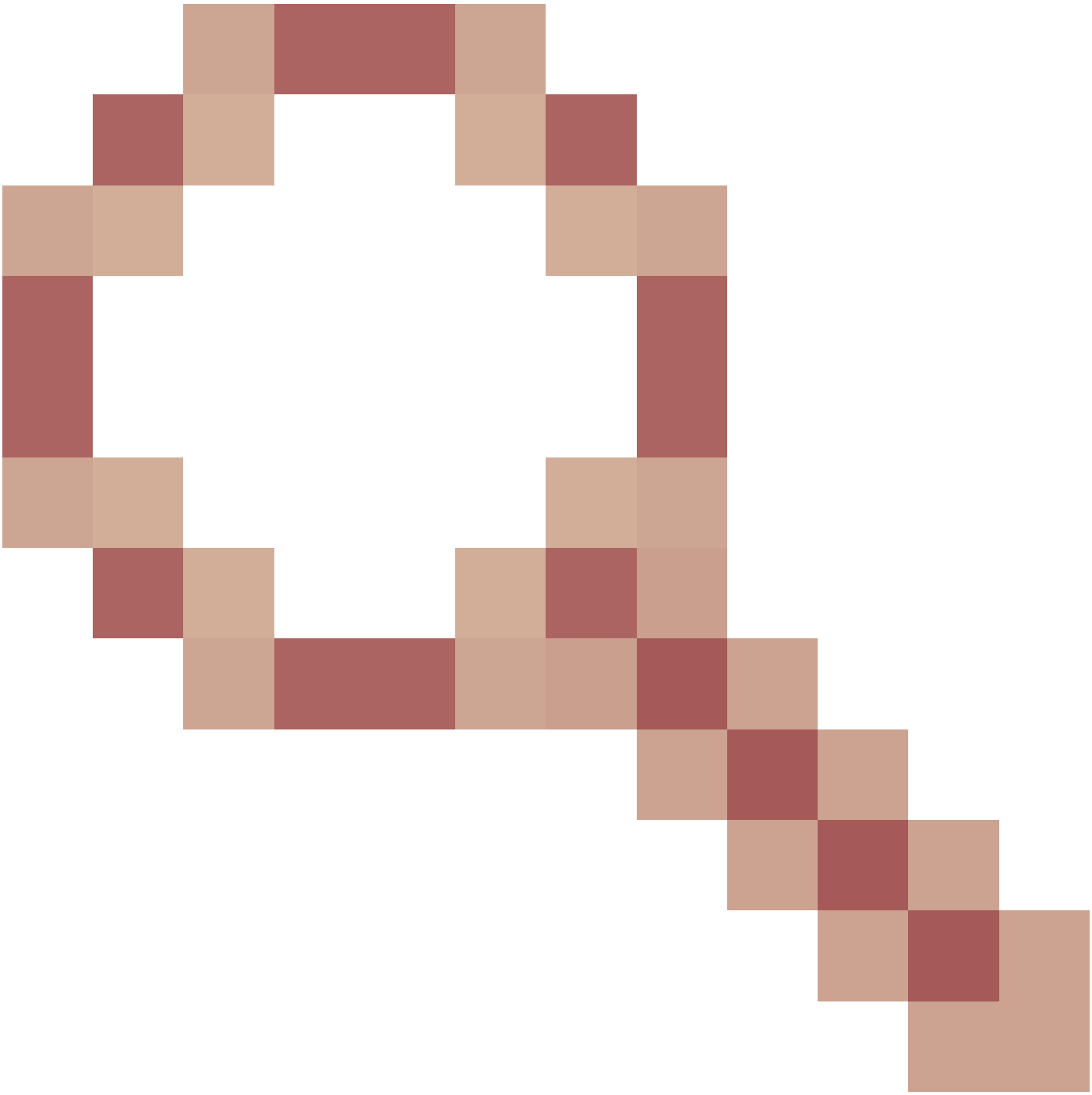
Problem 9: ASDM-Sitzung wird nicht unterbrochen

Das Symptom ist, dass das Timeout für ASDM-GUI-Sitzungen nicht berücksichtigt wird.

Fehlerbehebung - Empfohlene Schritte

Dies ist der Fall, wenn der Befehl "aaa authentication http console LOCAL" auf der verwalteten ASA nicht festgelegt ist.

Siehe Cisco Bug-ID CSCwj70826



ENH: Warnung hinzufügen: Einstellung Sitzungs-Timeout, erfordert "aaa authentication http console LOCAL"

Problemumgehung

Konfigurieren Sie den Befehl "aaa authentication http console LOCAL" auf der verwalteten ASA.

Problem 10. Die ASDM LDAP-Authentifizierung ist fehlgeschlagen

Fehlerbehebung - Empfohlene Schritte

Schritt 1

Stellen Sie sicher, dass die Konfiguration vorhanden ist. Beispiel:

<#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

Schritt 2

Überprüfen Sie den LDAP-Serverstatus:

<#root>

```
asa#
```

show aaa-server

Gutes Szenario:

<#root>

```
Server status:
```

ACTIVE

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

Schlechtes Szenario:

<#root>

```
Server status:
```

FAILED

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

Schritt 3

Überprüfen Sie, ob die LOKALE Authentifizierung ordnungsgemäß funktioniert, indem Sie die

LDAP-Authentifizierung vorübergehend deaktivieren.

Schritt 4

Führen Sie auf der ASA LDAP-Debugging-Programme aus, und versuchen Sie, den Benutzer zu authentifizieren:

<#root>

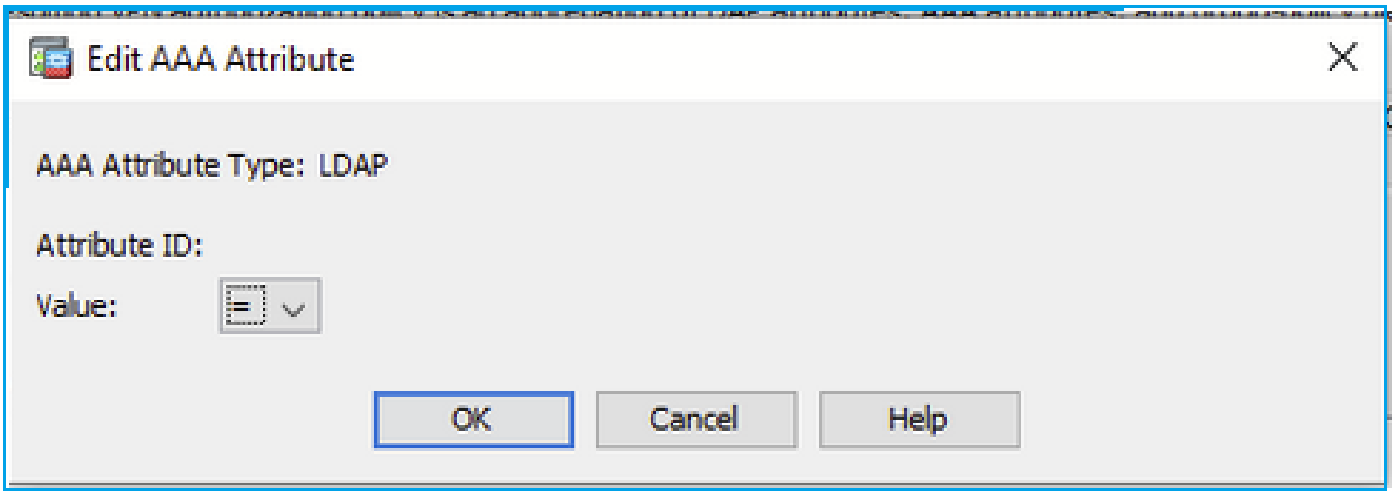
#

debug ldap 255

Suchen Sie in den Debugs nach Zeilen, die Hinweise wie "Failed" (Fehlgeschlagen) enthalten.

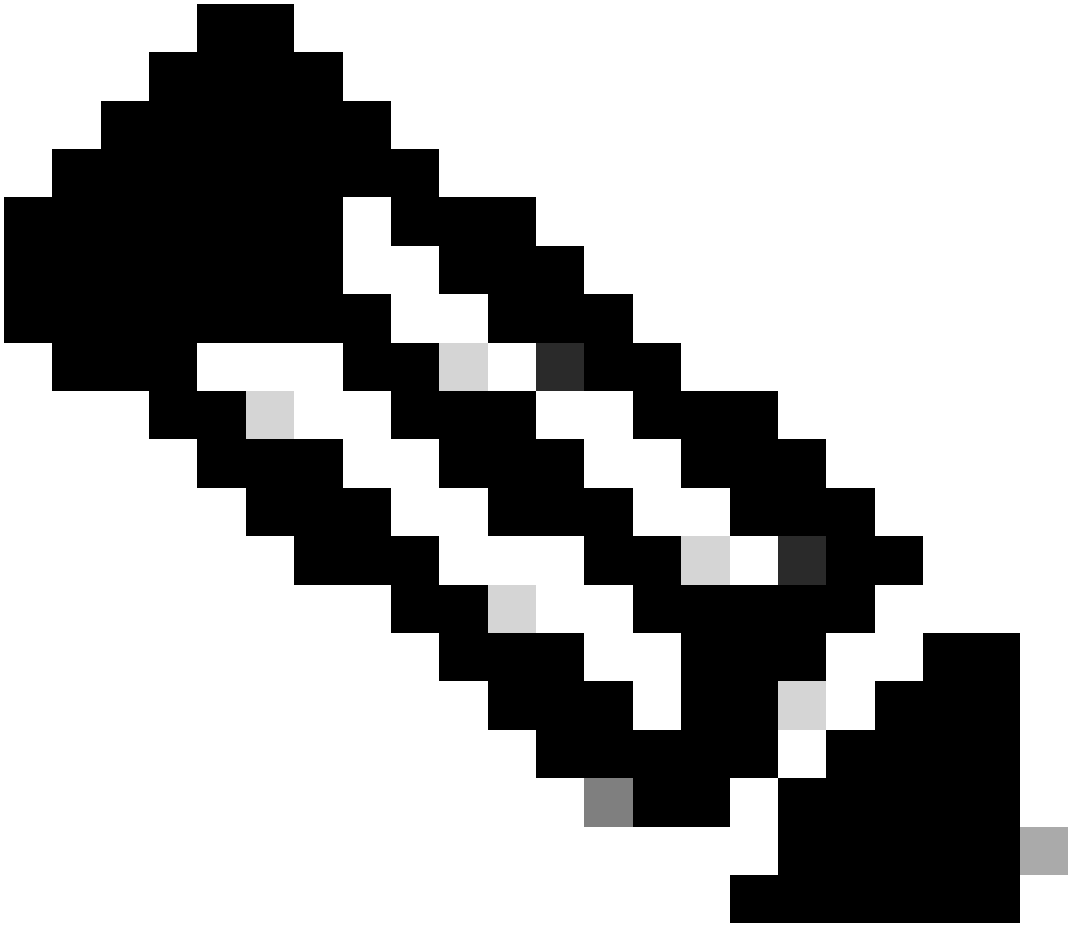
Problem 11. Konfiguration des ASDM WebVPN DAP fehlt

Unter der DAP-Konfiguration für ASDM sind AAA-Attributtypen (Radius/LDAP) nicht sichtbar. Es werden nur = und != bei Dropdown-Liste angezeigt:



Fehlerbehebung - Empfohlene Schritte

Dies ist ein Softwarefehler, der von der Cisco Bug-ID CSCwa99370 verfolgt wird. ASDM:DAP-Konfiguration ohne AAA-Attributtyp (Radius/LDAP)

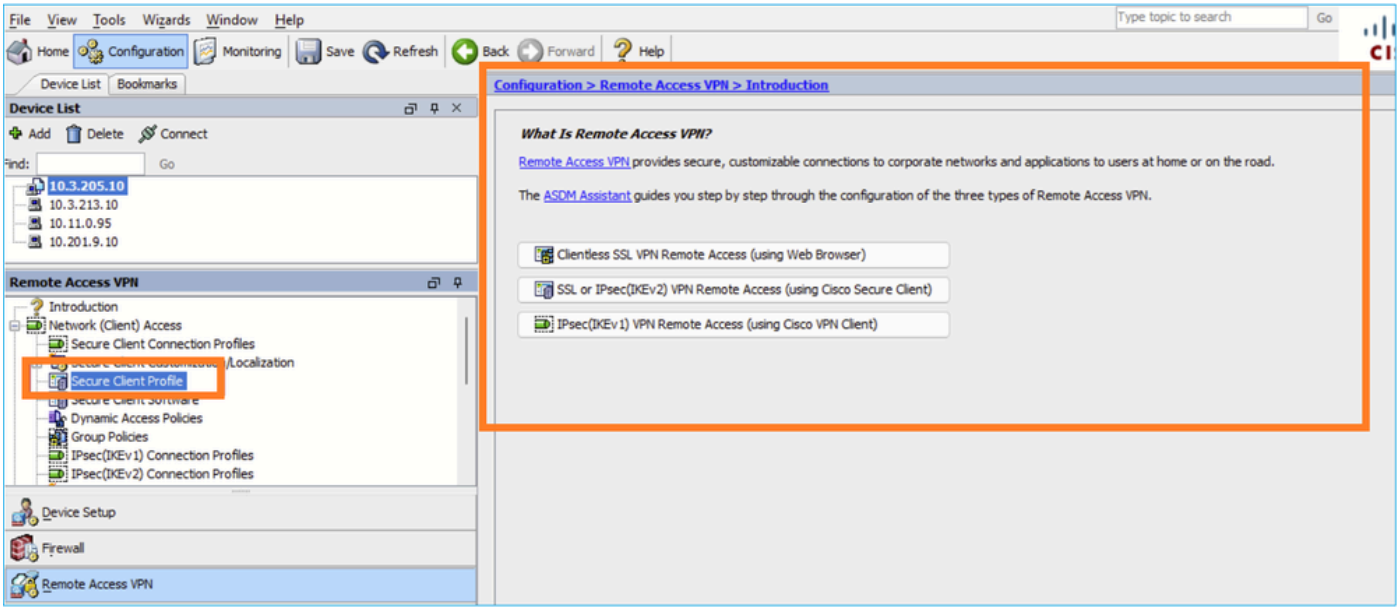


Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

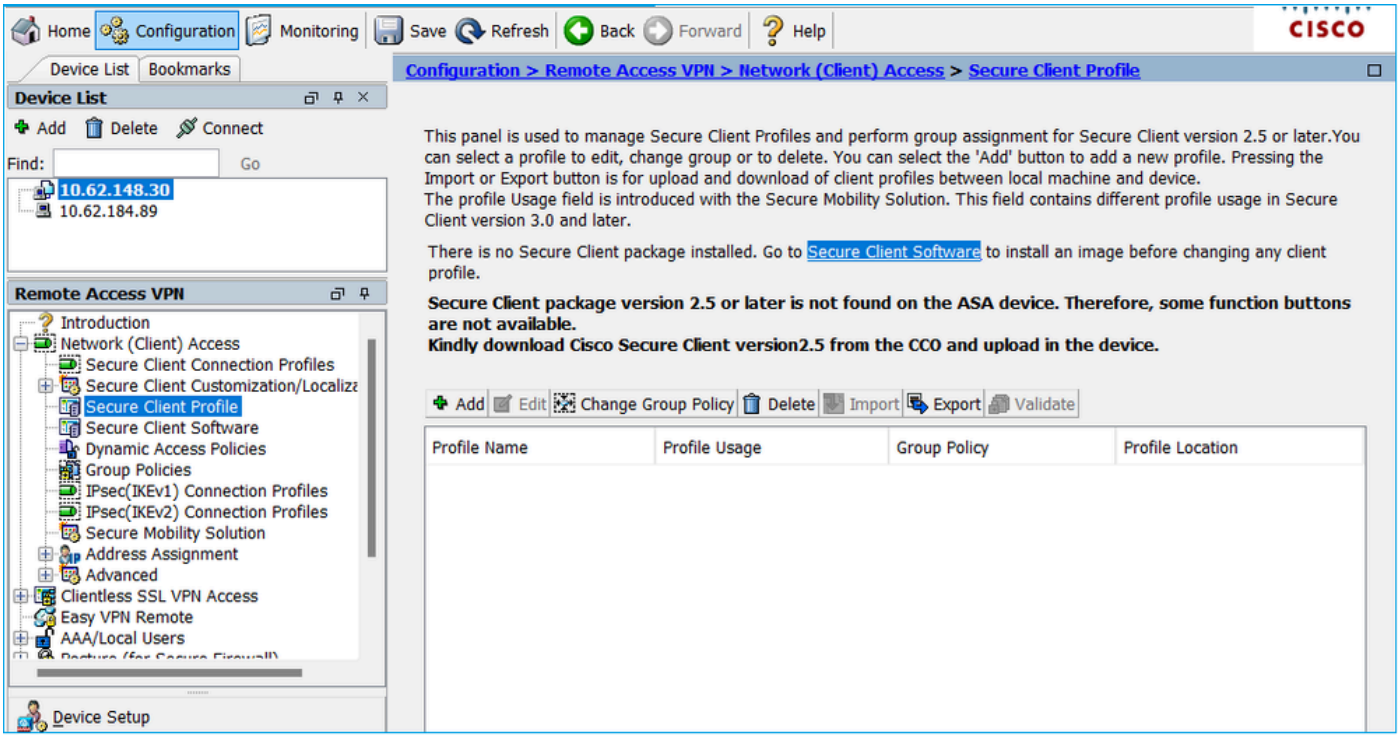
Fehlerbehebung bei ASDM - Andere Probleme

Problem 1. Kein Zugriff auf sicheres Clientprofil auf ASDM möglich

Die ASDM-Benutzeroberfläche zeigt Folgendes:



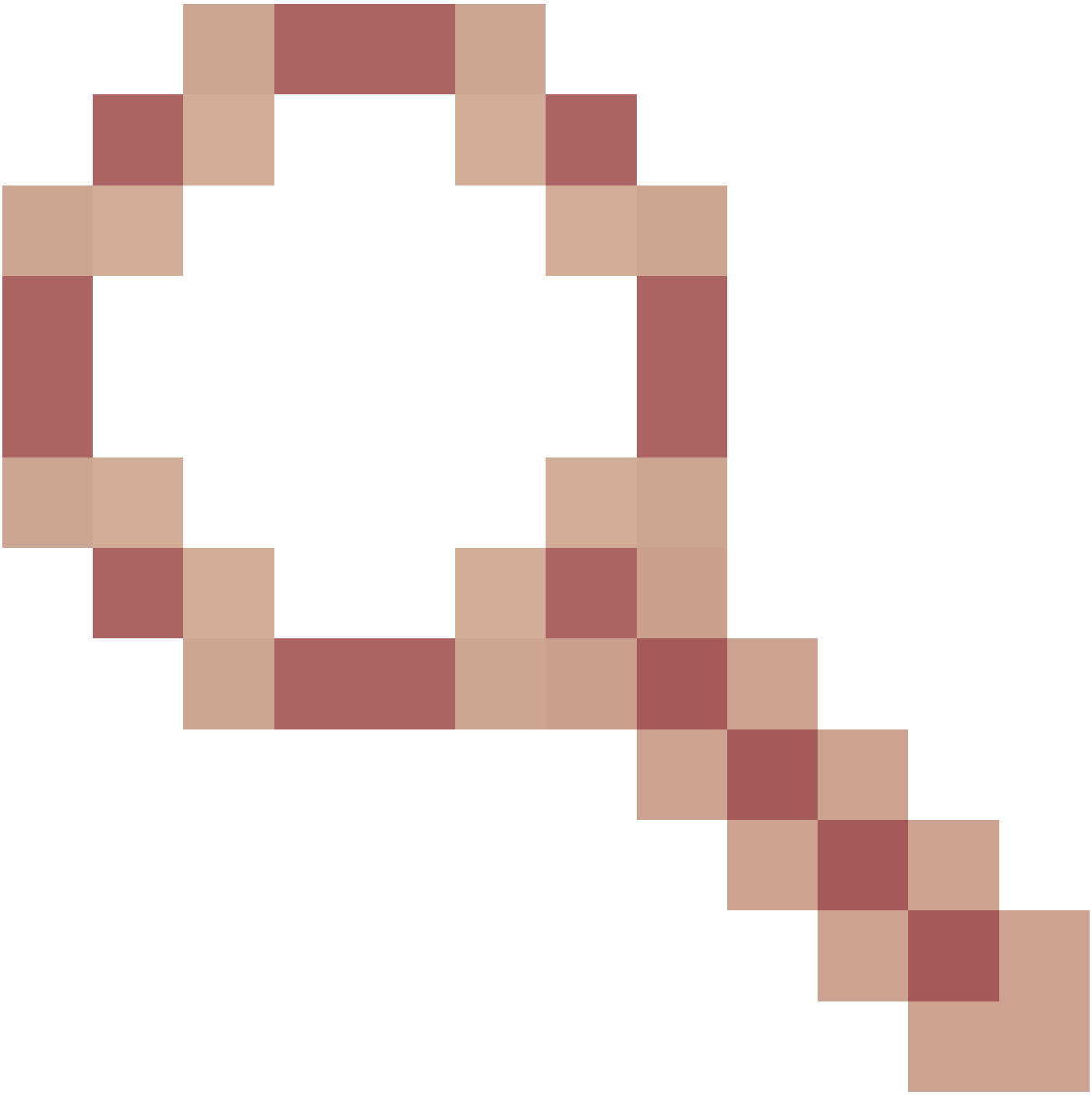
Die erwartete Ausgabe der Benutzeroberfläche ist:



Fehlerbehebung - Empfohlene Schritte

Dies ist ein bekannter Fehler:

Cisco Bug-ID CSCwi56155



Zugriff auf sicheres Clientprofil auf ASDM nicht möglich

Problemumgehungen:

Downgrade von AnyConnect

Oder

ASDM-Upgrade auf Version 7.20.2

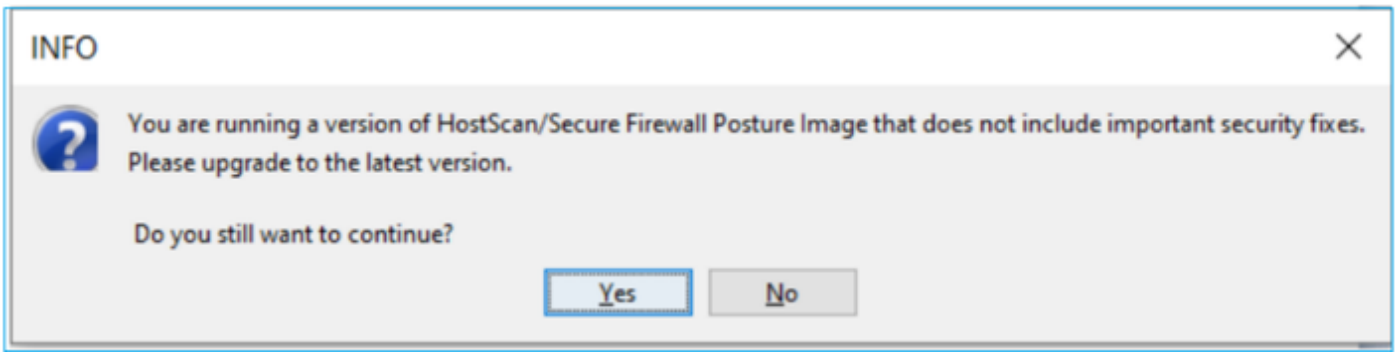
Weitere Informationen finden Sie in den Fehlerhinweisen. Darüber hinaus können Sie den Fehler abonnieren, sodass Sie eine Benachrichtigung über Defekt-Updates erhalten.

Problem 2. ASDM zeigt Popup-Fenster für Hostscan - Image enthält keine wichtigen

Sicherheitskorrekturen

Die ASDM-Benutzeroberfläche zeigt Folgendes:

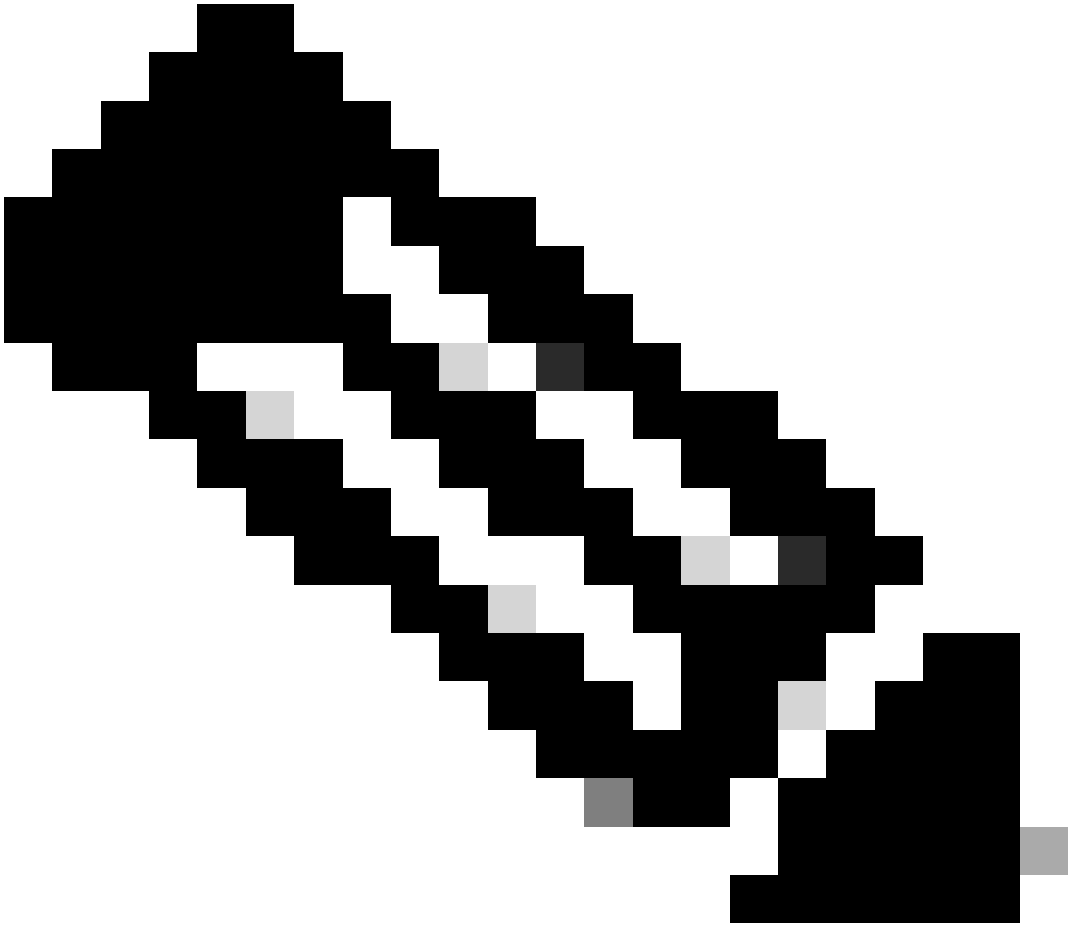
"Sie führen eine Version des HostScan/SecureFirewall Posture-Images aus, die keine wichtigen Sicherheitskorrekturen enthält. Führen Sie ein Upgrade auf die neueste Version durch. Möchten Sie trotzdem fortfahren?"



Fehlerbehebung - Empfohlene Schritte

Dies ist ein bekannter Fehler:

Cisco Bug-ID CSCwc62461
Beim Anmelden beim ASDM-Popup-Fenster für Hostscan - Image enthält keine wichtigen Sicherheitskorrekturen



Anmerkung: Dieser Fehler wurde in den letzten ASDM-Softwareversionen behoben. Weitere Informationen finden Sie in den Fehlerdetails.

Problemumgehung:

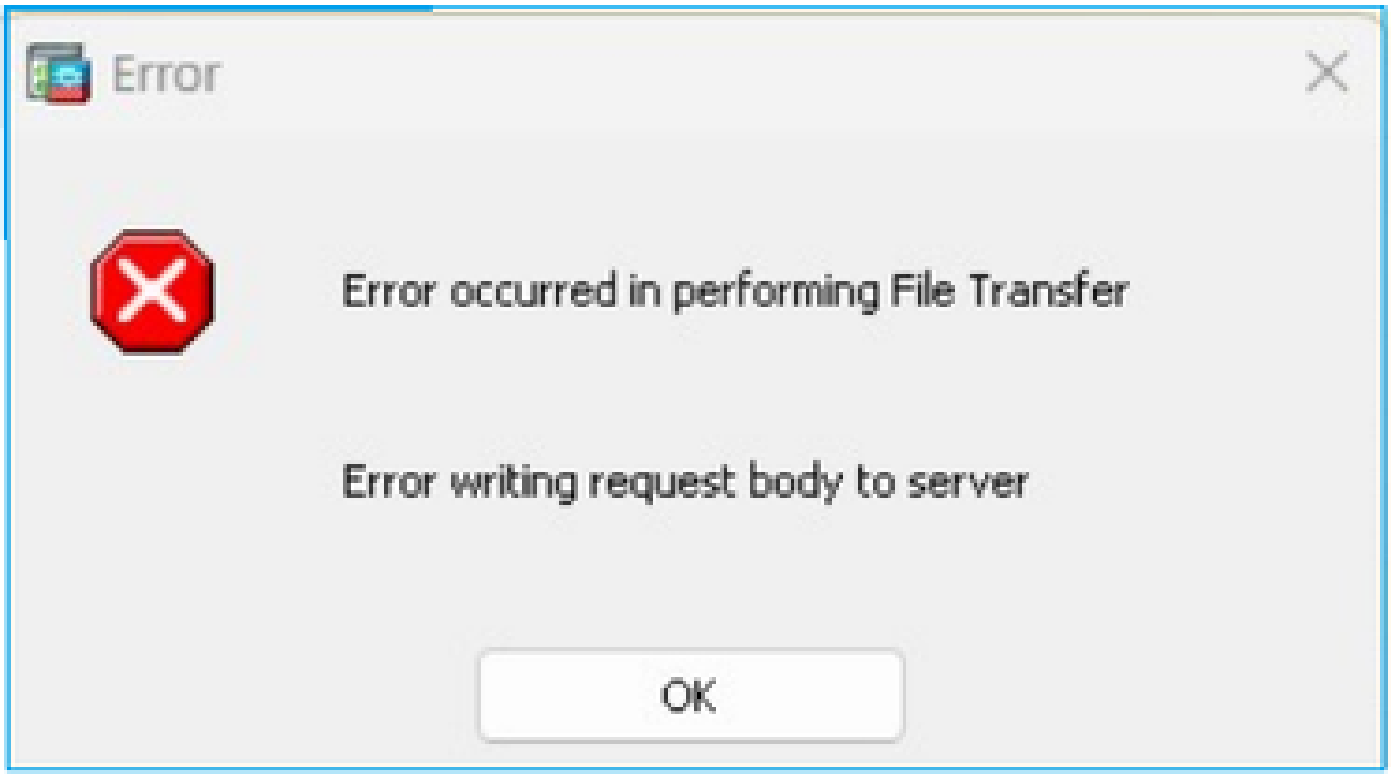
Klicken Sie im Popup-Meldungsfeld auf "Ja", um fortzufahren.

Problem 3: ASDM-Fehler beim Schreiben des Anforderungstexts auf den Server beim Kopieren eines Images über ASDM

Die ASDM-Benutzeroberfläche zeigt Folgendes:

Fehler beim Durchführen der Dateiübertragung

Fehler beim Schreiben des Anforderungstexts auf den Server



Fehlerbehebung - empfohlene Maßnahmen

Dies ist ein bekannter Fehler, der wie folgt aufgespürt wird:

Cisco Bug-ID CSCtf74236

ASDM "Fehler beim Schreiben des Anforderungstexts auf den Server" beim Kopieren des Images

Problemumgehung

Verwenden Sie SCP/TFTP, um die Datei zu übertragen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.