Troubleshoot ASDM Configuration, Authentication and Other Problems

Contents

Introduction

This document describes the troubleshooting process for Adaptive Security Appliance Device Manager (ASDM) configuration, authentication and other problems.

Background

The document is part of the ASDM troubleshoot series along with these documents:

- Troubleshoot ASDM Launch Problems
- Troubleshoot ASDM License, Upgrade and Compatibility Problems
- Troubleshoot ASDM TLS Security, Certificate and Vulnerability Problems

Troubleshoot ASDM Configuration Problems

Problem 1. ASDM does not display any access control lists (ACL) applied to an interface

ASDM does not display any access control lists (ACL) applied to an interface, even though there is a valid access-group applied to the interface in question. The message instead reads "0 incoming rules". These symptoms are observed L3 and L2 ACL both configured in access group config for an interface:

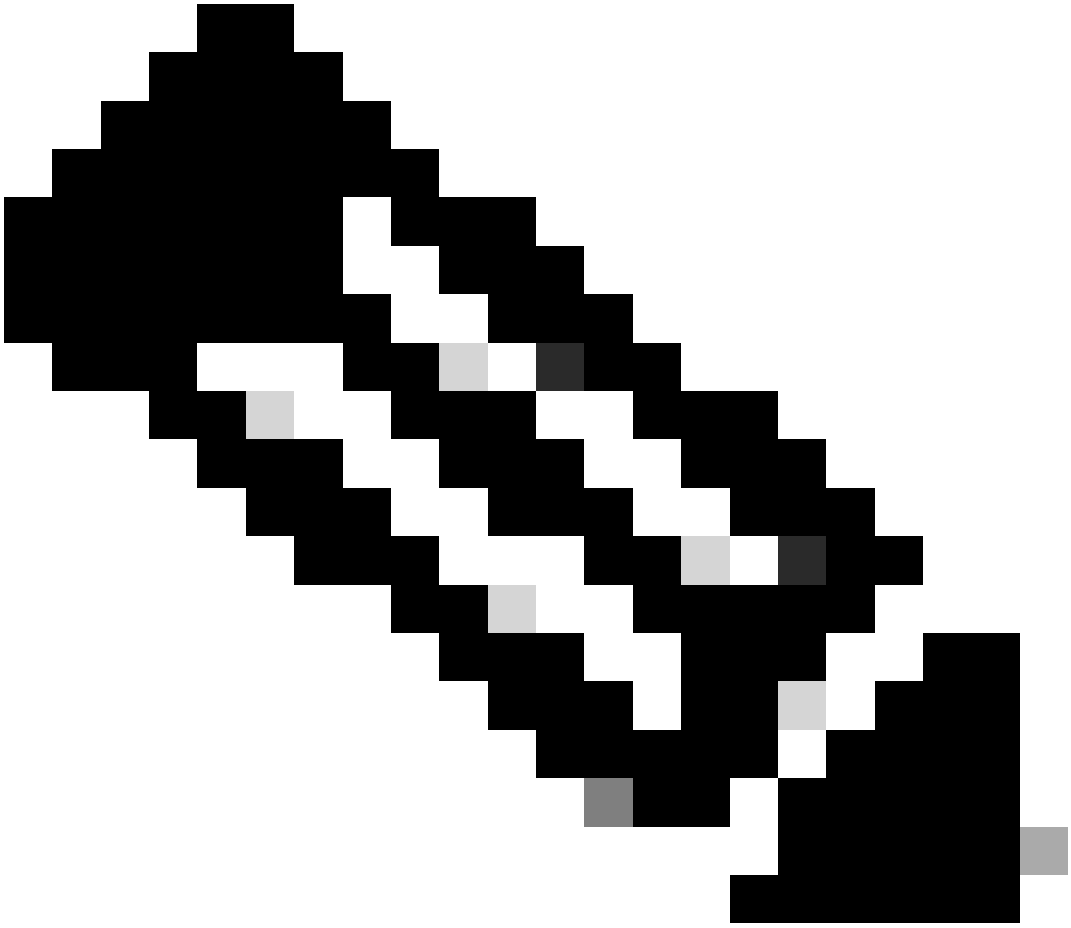
<#root>

```
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
```

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwj14147 “ASDM fails to load access-group config if L2 and L3 acl's are mixed.”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 2. Hit count inconsistency between ASA CLI and ASDM UI

The hit-count entries in the ASDM are not consistent with the access-list hit counts as reported by the **show access-list** command on output of the firewall.

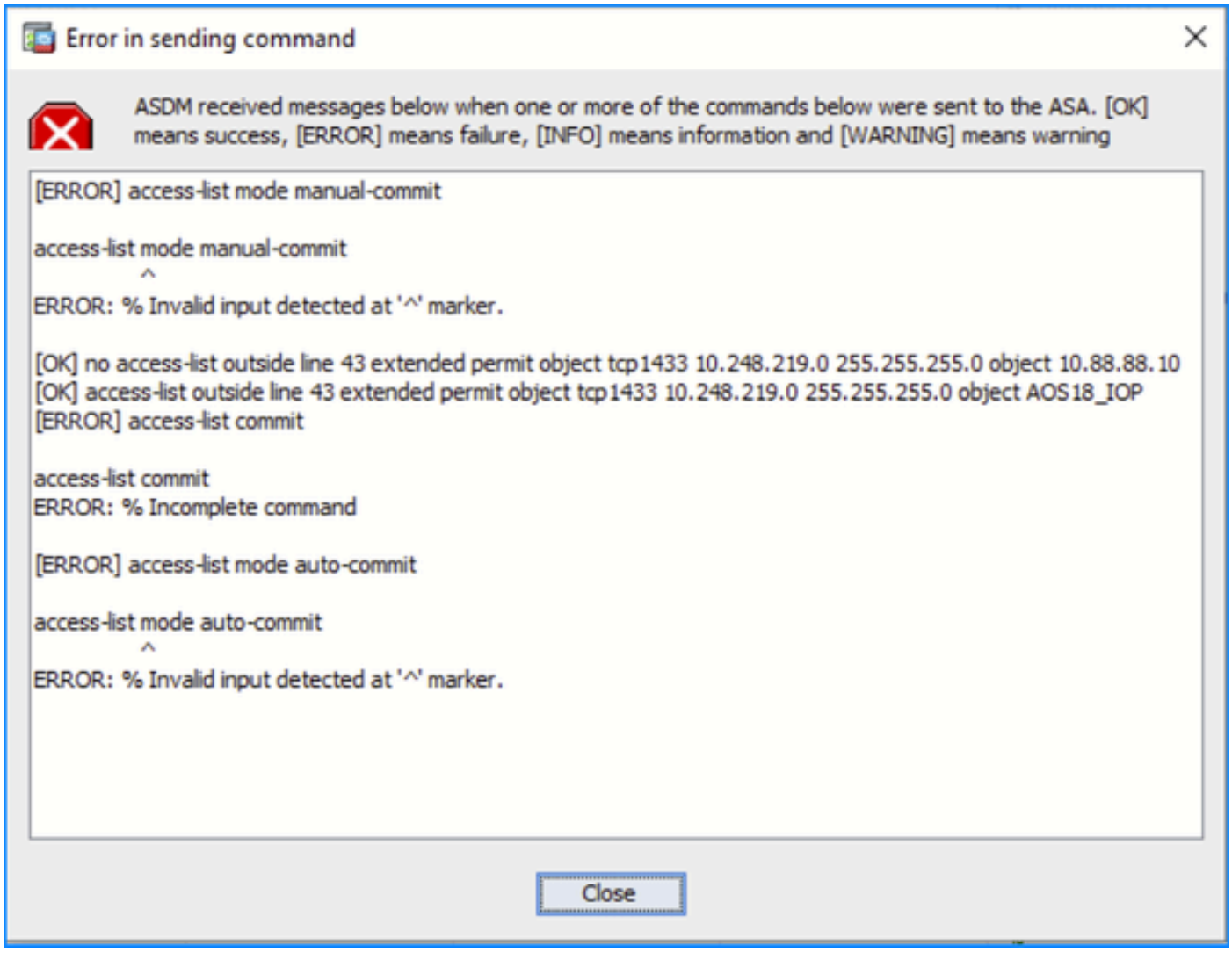
Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCtq38377 “ENH: ASDM should use ACL hash calc'd on the ASA and not calc'd locally” and Cisco bug ID CSCtq38405“ENH: ASA needs mechanism to provide ACL Hash info to ASD”

Problem 3. “ERROR: % Invalid input detected at '^' marker.” error message when editing an ACL in ASDM

The “ERROR: % Invalid input detected at '^' marker.” error message is shown when editing an ACL in ASDM:

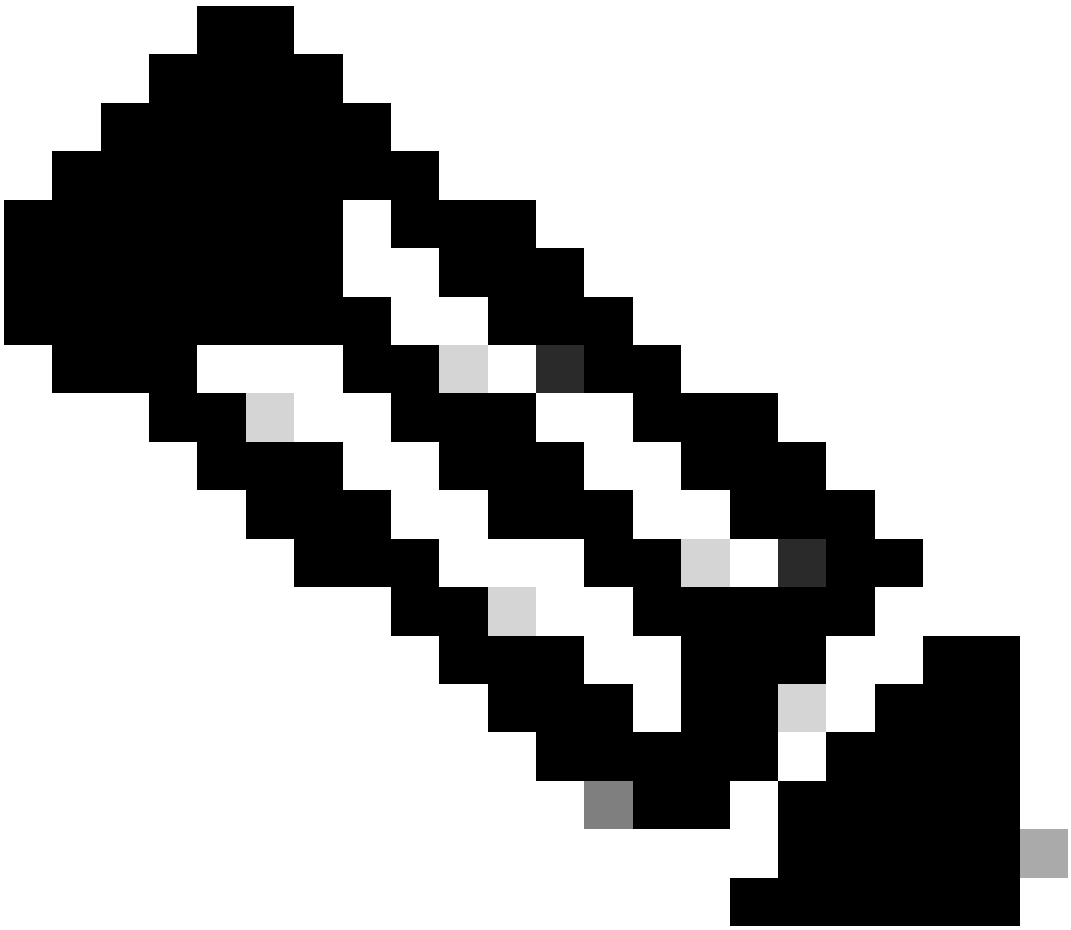
```
[ERROR] access-list mode manual-commit access-list mode manual-commit
                      ^
ERROR: % Invalid input detected at '^' marker.
[OK] no access-list ACL1 line 1 extended permit tcp object my-obj-1 object my-obj-2 eq 12345
[ERROR] access-list commit access-list commit
ERROR: % Incomplete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



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCvq05064 “Edit an entry (ACL) from ASDM gives an error. When

using ASDM with OpenJRE/Oracle - version 7.12.2” and Cisco bug ID CSCvp88926 “Sending addition commands while deleting access-list”.



Note: These defects have been fixed in recent ASDM software releases. Check the defect details for more information.

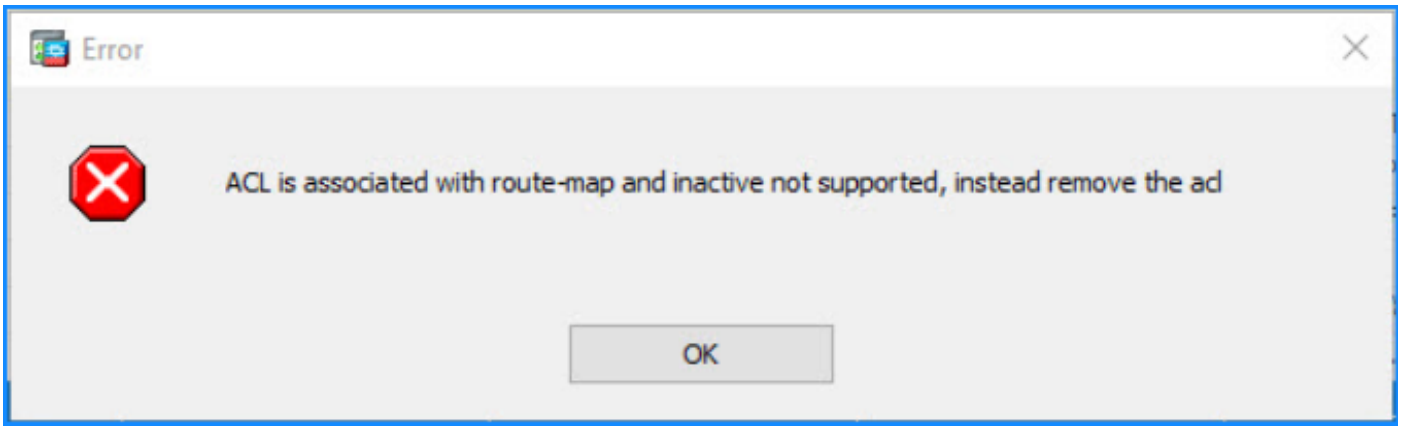
Problem 4. The “ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl” error message in specific cases

The “ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl” error message is shown in one of these cases:

1. Edit an ACL in ASDM used in a policy based-routing configuration:

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

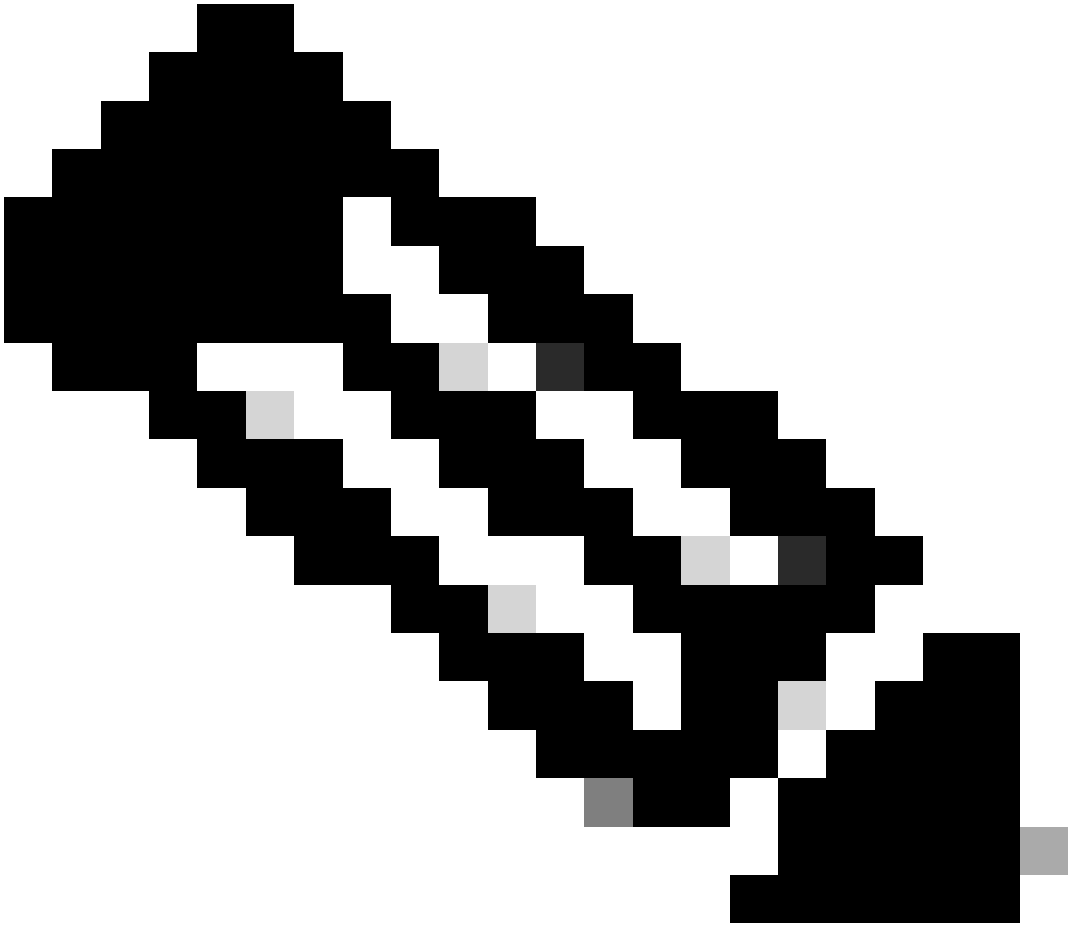
ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl



2. Edit an ACL ASDM > **Configuration** -> **Remote Access VPN** -> **Network (Client) Access** > **Dynamic Access policy**

Troubleshoot – Recommended Actions

1. Refer to the software Cisco bug ID CSCwb57615 “Configuring pbr access-list with line number failed.”. The workaround is to exclude the “line” parameter from the configuration.
2. Refer to the software Cisco bug ID CSCwe34665 “Unable to Edit the ACL objects if it is already in use, getting the exception”.



Note: These defects have been fixed in recent ASA software releases. Check the defect details for more information.

Problem 5. No logs in ASDM Real-Time Log Viewer for implicitly denied connections

ASDM Real-Time Log Viewer does not show logs for implicitly denied connections.

Troubleshoot – Recommended Actions

The implicit deny at the end of the access-list does not generate syslog. If you want all denied traffic to generate syslog, add rule with the **log** keyword at the end of the ACL.

Problem 6. ASDM freezes when trying to modify any network object or object-group

ASDM freezes when trying to modify any network object or object-group from the **Configuration** > **Firewall** > **Access Rules** page under the **Addresses** tab. The user is not be able to edit any of the parameters in the network object window when this issue is encountered.

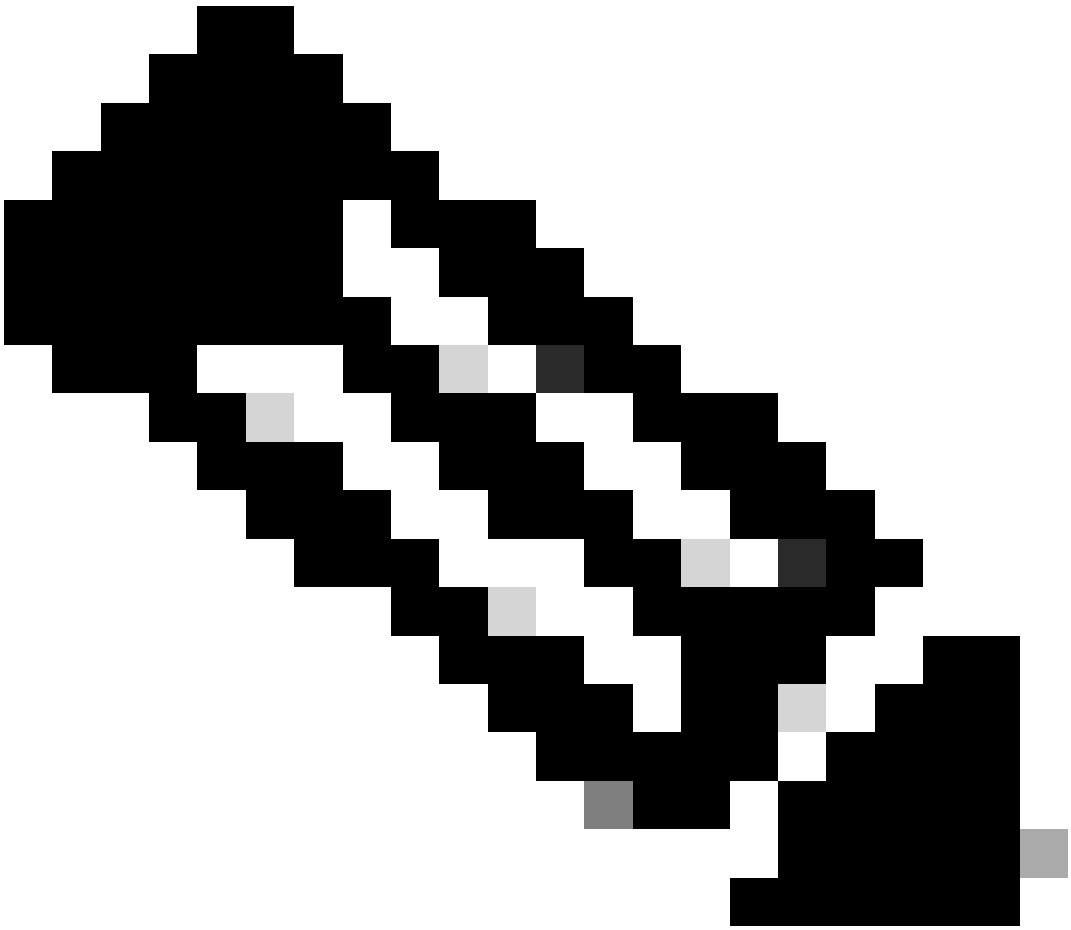
Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwj12250 “ASDM freezes when editing network objects or network object-groups”. The workaround is to disable the topN host statistics collection:

<#root>

```
ASA(config)#
```

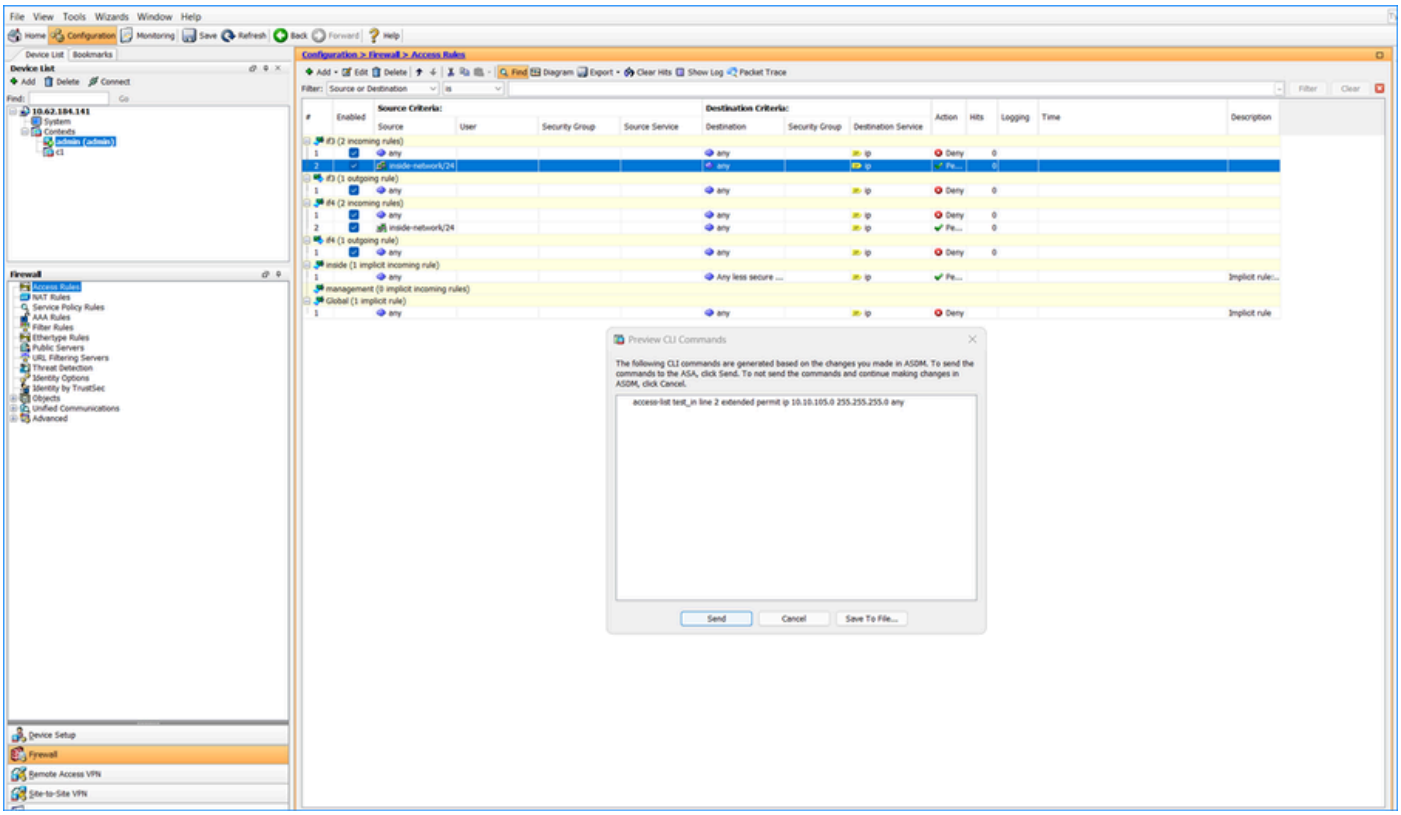
```
no hpm topN enable
```



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 7. ASDM can show extra access control list rules for different interfaces

ASDM can show additional access control list rules for different interfaces if an interface-level access control list is modified. In this example, an incoming rule#2 was added to interface **if3** ACL. ASDM also shows #2 for the interface **if4**, whereas this rule was not configured by the user. The command preview correctly shows a single pending change. This is a user interface display issue.



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwm71434 “ASDM may display duplicate interface access-list entries”.

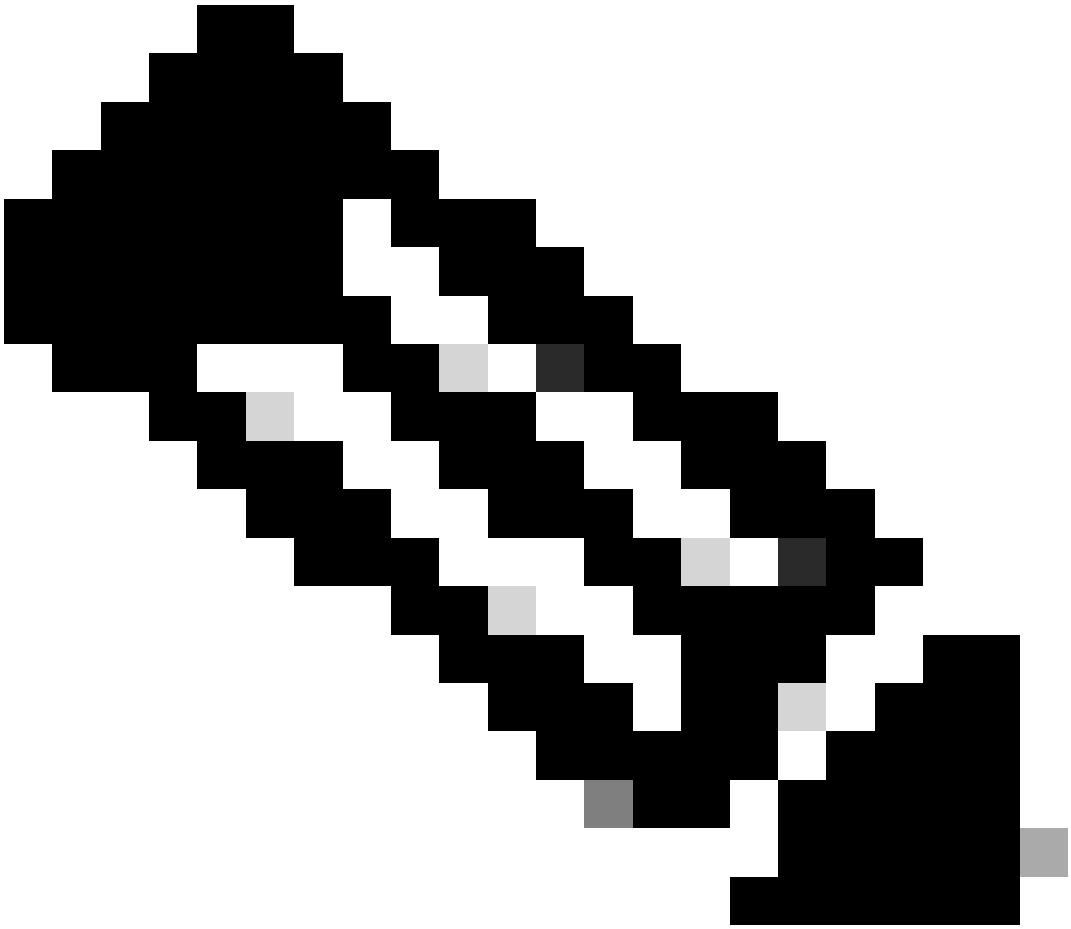
Problem 8. Real-time logs are unavailable in the Real Time Log Viewer

No logs are shown in the Real Time Log Viewer

Troubleshoot – Recommended Actions

1. Ensure logging is configured. Refer to the ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.22, Chapter: Logging.
2. Refer to the software Cisco bug ID CSCvf82966 “ASDM - Logging: Unable to View Real-Time

logs”.

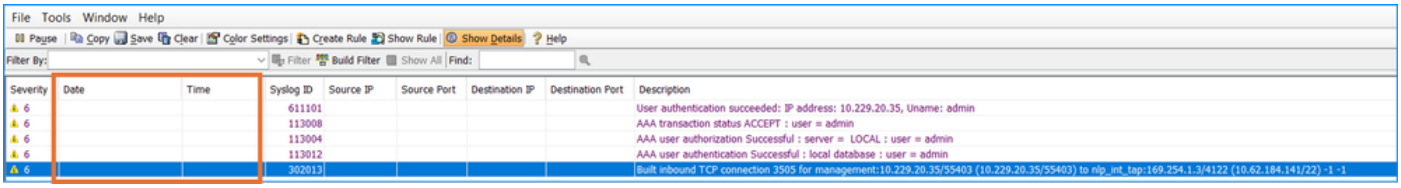


Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

References

- ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.22, Chapter: Logging.

Problem 9. The Date and Time columns are empty in the Real Time log Viewer



Troubleshoot – Recommended Actions

1. Check if RFC5424 logging timestamp format is used:

<#root>

#

show run logging

logging enable

logging timestamp rfc5424

2. If RFC5424 logging timestamp format is used, refer to the software Cisco bug ID CSCvs52212 “ASDM ENH: capability for Event Log Viewers to display ASA syslogs with rfc5424 timestamp format”. The workaround is to avoid using the RFC5424 format:

<#root>

firewall(config)#

no logging timestamp rfc5424

firewall(config)#

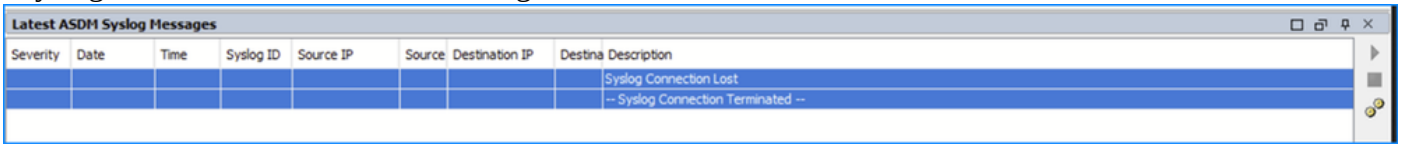
logging timestamp

3. Additionally, refer to the software defect Cisco bug ID CSCwh70323 “Timestamp entry missing for some syslog messages sent to syslog server”.

Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

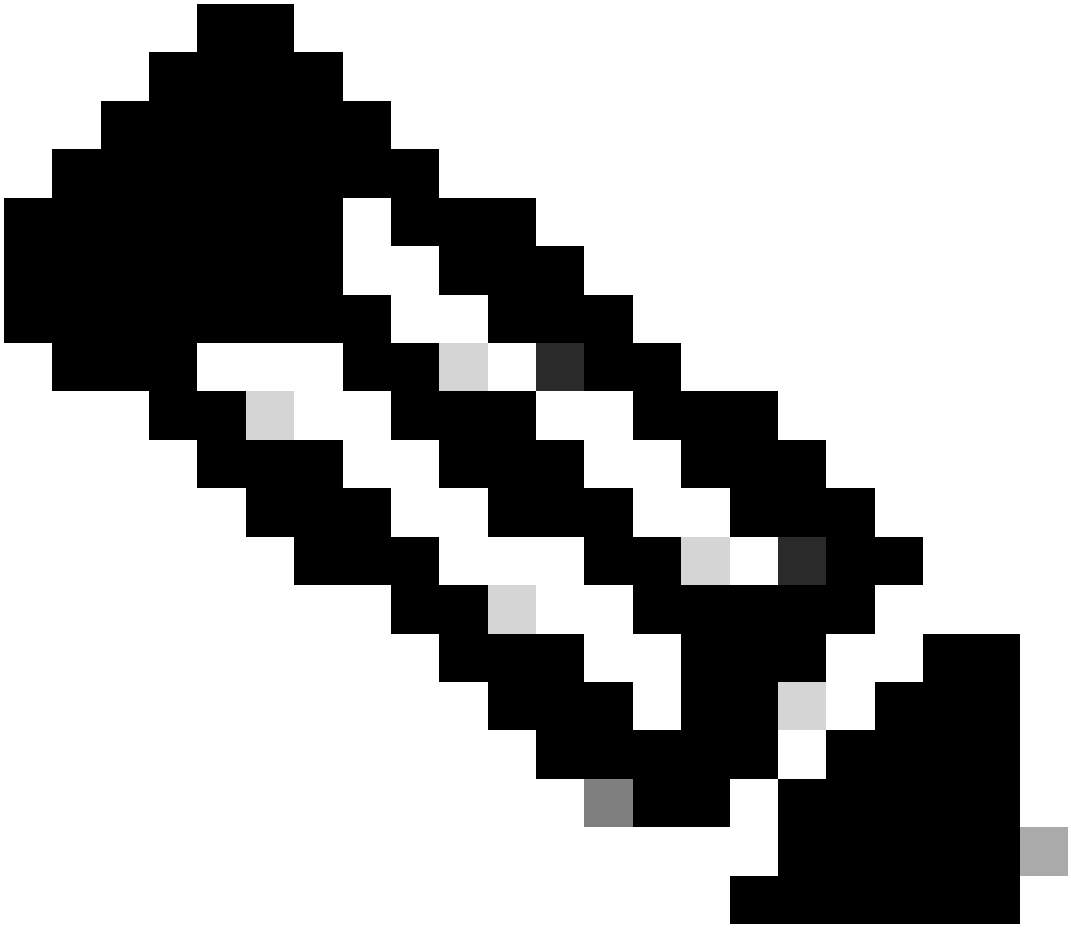
Problem 10. Logging to ASDM can fail after switching to a different context in a multi-context ASA

The **Latest ASDM Syslog Messages** tab in the **Home** page shows the “Syslog Connection Lost” and “Syslog Connection Terminated” messages:



Troubleshoot – Recommended Actions

Ensure logging is configured. Refer to the software Cisco bug ID CSCvz15404 “ASA: Multiple context mode : ASDM logging stops, when switched to a different context”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 11. ASDM session abruptly terminated when switching between different contexts

ASDM session abruptly terminated when switching between different contexts with the error message “The maximum number of management sessions for protocol http or user already exists. Please try again later”. These logs are shown in the syslog messages:

```
%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
```

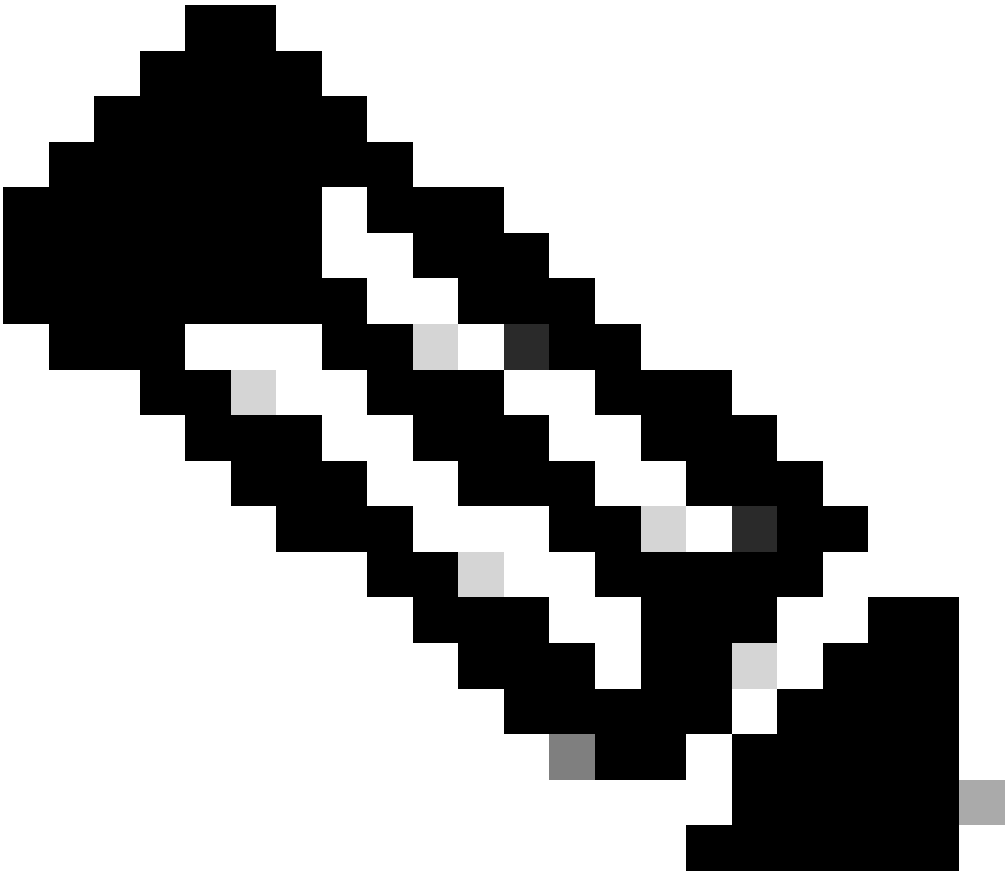
Troubleshoot – Recommended Actions

1. Check if the **Current** ASDM resource usage has reached the **Limit**. In this case the **Denied** counter increases:

<#root>

```
firewall #
show resource usage resource ASDM

Resource                  Current        Peak      Limit        Denied Context
ASDM
5
            5
5


10
 admin
```

2. Refer to the software Cisco bug ID CSCvs72378 “ASDM session being abruptly terminated when switching between different contexts”.



Note: This defect has been fixed in recent ASA software releases. Check the defect details for more information.

3. If the software version has the fix for the Cisco bug ID CSCvs72378, and the current resource reached the limit, disconnect some of existing ASDM sessions. You can close the ASDM or, alternatively, clear HTTPS connections for the IP address of the host running ASDM. In this example, it is assumed that the HTTP server on ASDM runs on the default HTTPS port 443:

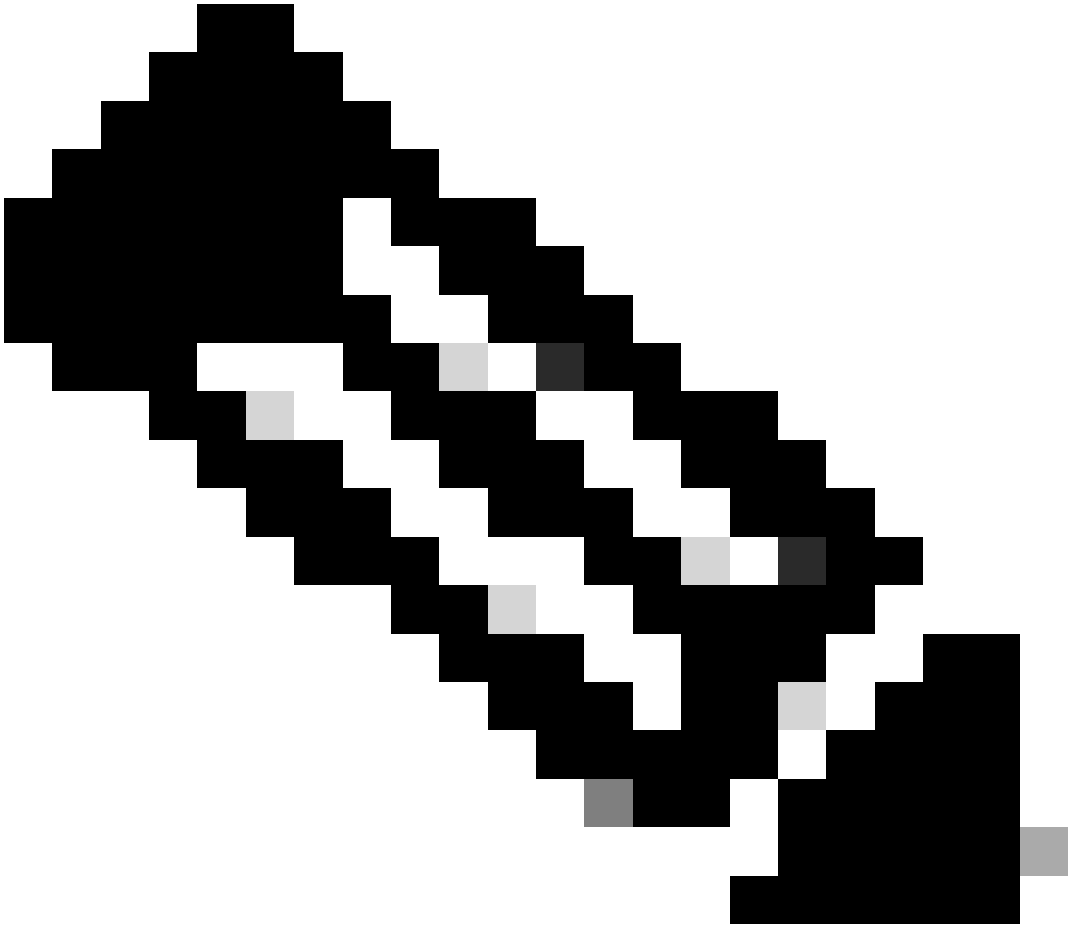
```
<#root>

#

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
```

Problem 12. ASDM randomly exits/terminates with message “ASDM received a message from the ASA device to disconnect. ASDM will now exit.”

On multi-context ASA, ASDM randomly exits/terminates with the message “ASDM received a message from the ASA device to disconnect. ASDM will now exit.”.

Troubleshoot – Recommended Actions

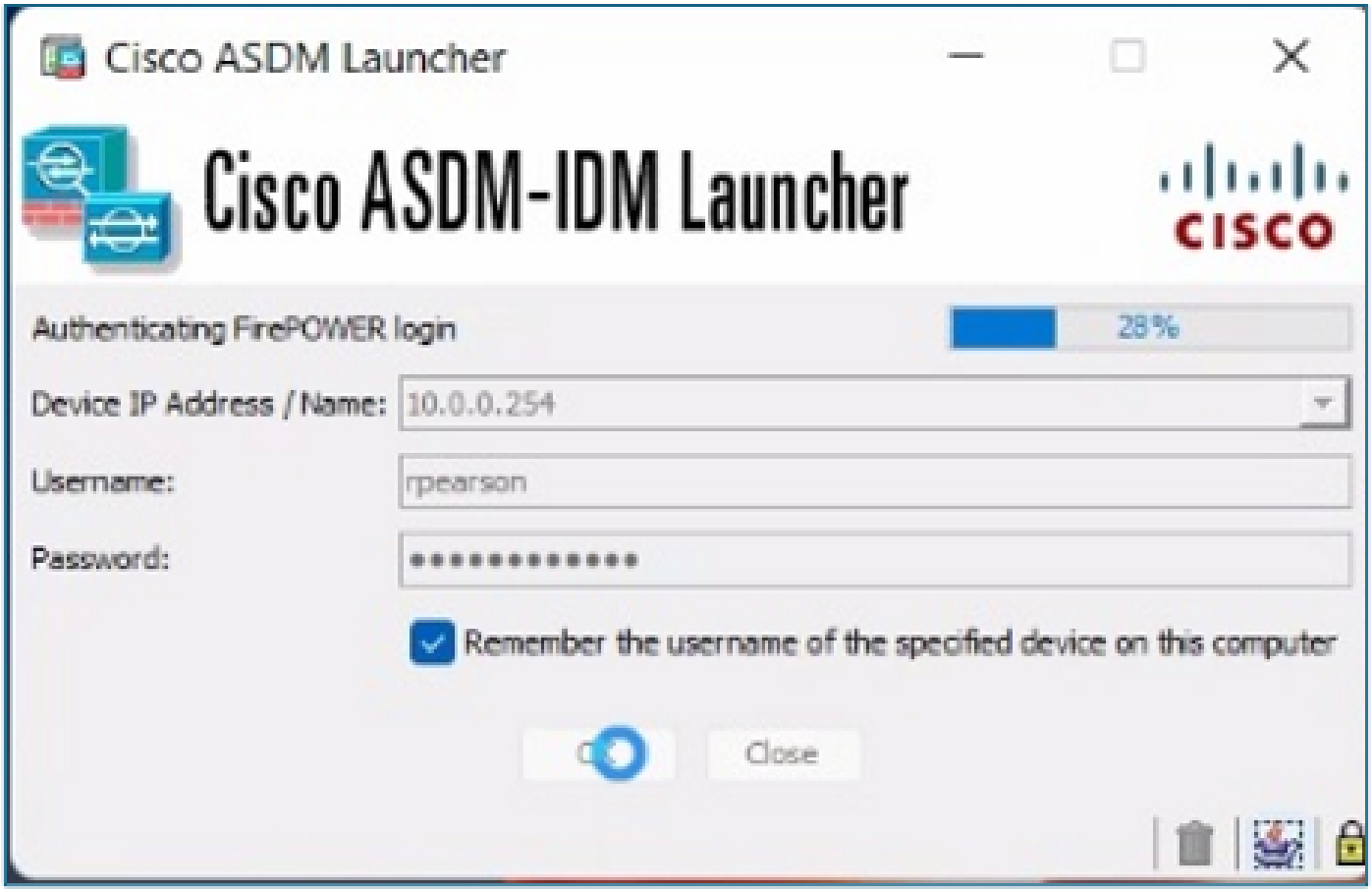
Refer to the software defect Cisco bug ID CSCwh04395 “ASDM application randomly exits/terminates with an alert message on multi-context setup”.



Note: This defect has been fixed in recent ASA software releases. Check the defect details for more information.

Problem 13. ASDM load hangs with the message “Authentication FirePOWER login”

ASDM load hangs with the message “Authentication FirePOWER login”:



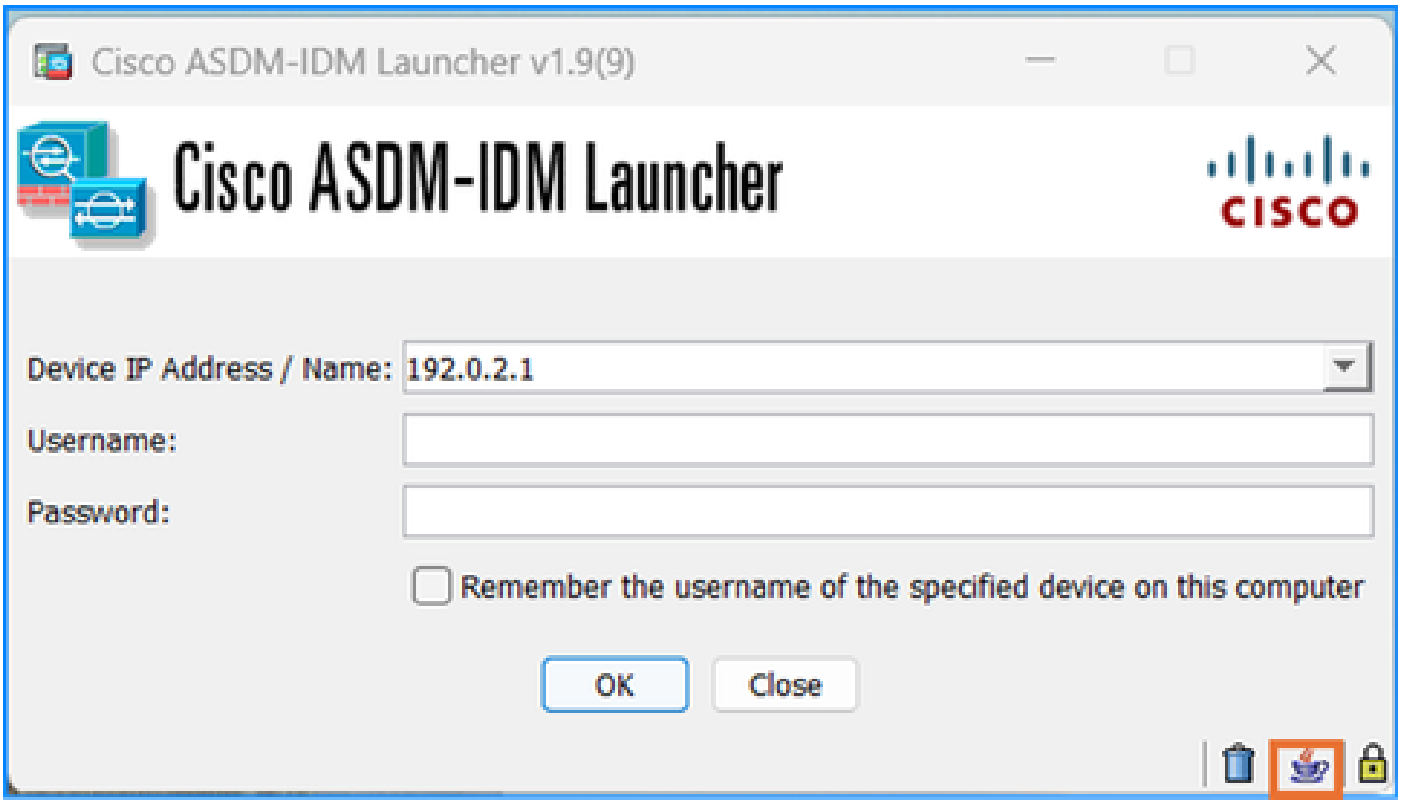
The Java console logs show the “Failed to connect to FirePower, continuing without it” message:

<#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)
```

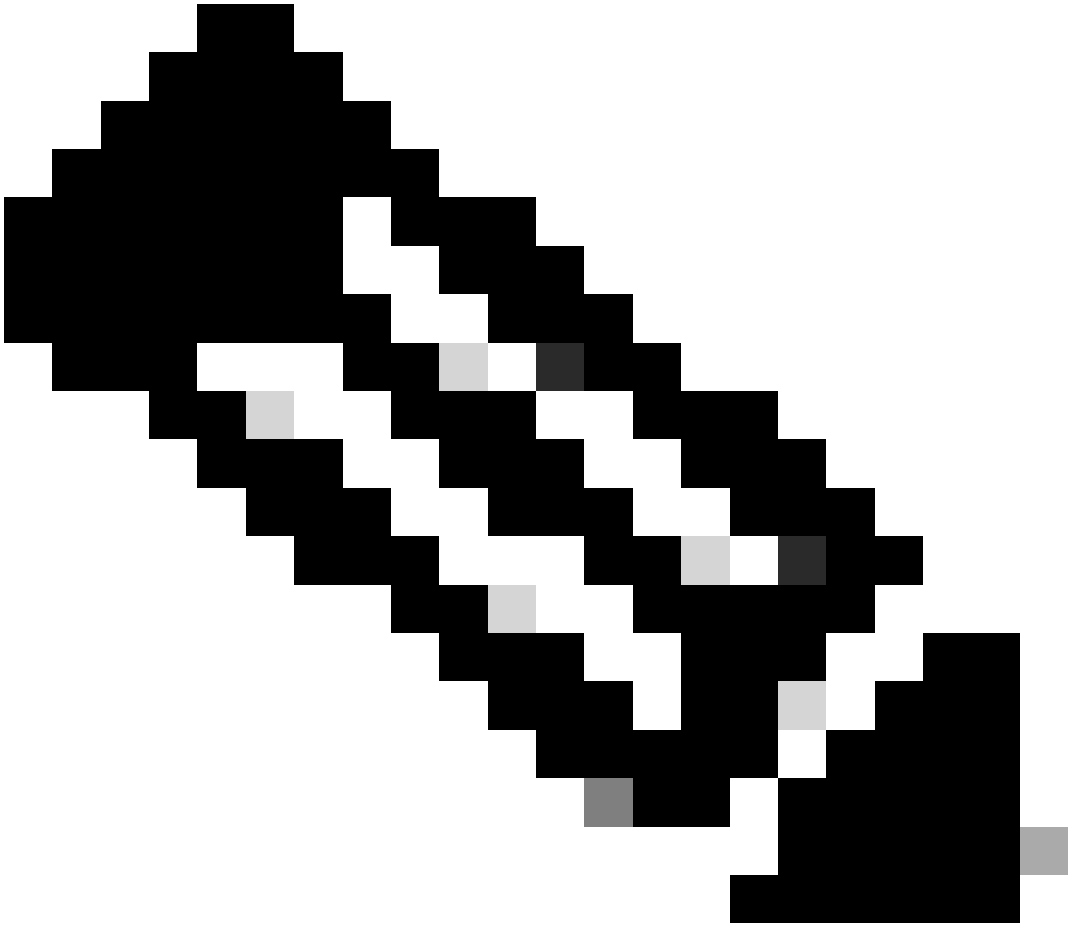
To verify this symptom, enable Java console logs:



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwe15164 “ASA: ASDM cannot display SFR tabs until it's "woken up" through its CLI.”. Workaround steps:

1. Close the ASDM manager.
2. Get SSH access to the SFR and switch user to root (**sudo su**).
3. After doing the steps above, re-launch the ASDM once again and it can be able to load the Firepower (SFR) tabs.



Note: This defect has been fixed in recent Firepower software releases. Check the defect details for more information.

Problem 14. ASDM does not show the Firepower module management/configuration

The Firepower module configuration is unavailable on ASDM.

Troubleshoot – Recommended Actions

1. Ensure that the ASA, ASDM, Firepower module and operating system versions are compatible. Refer to the Cisco Secure Firewall ASA Release Notes, Cisco Secure Firewall ASDM Release Notes, Cisco Secure Firewall ASA Compatibility:

- ASA 9.14/ASDM 7.14/Firepower 6.6 is the final version for the ASA FirePOWER module on the ASA 5525-X, 5545-X, and 5555-X.
- ASA 9.12/ASDM 7.12/Firepower 6.4.0 is the final version for the ASA FirePOWER module on the ASA 5515-X and 5585-X.

- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 is the final version for the ASA FirePOWER module on the ASA 5506-X series and 5512-X.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1).
- ASDM is not supported for FirePOWER module management with ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+, and 9.16(3.19)+; you have to use FMC to manage the module with these releases. These ASA releases require ASDM 7.18(1.152) or later, but ASDM support for the ASA FirePOWER module ended with 7.16.
- ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

2. If the versions are compatible, check if the module is up and running:

```
<#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
```

If the module is down, the **sw-module module reset** command can be used to reset the module and then reload the module software.

References

- Cisco Secure Firewall ASA Release Notes
- Cisco Secure Firewall ASDM Release Notes
- Cisco Secure Firewall ASA Compatibility

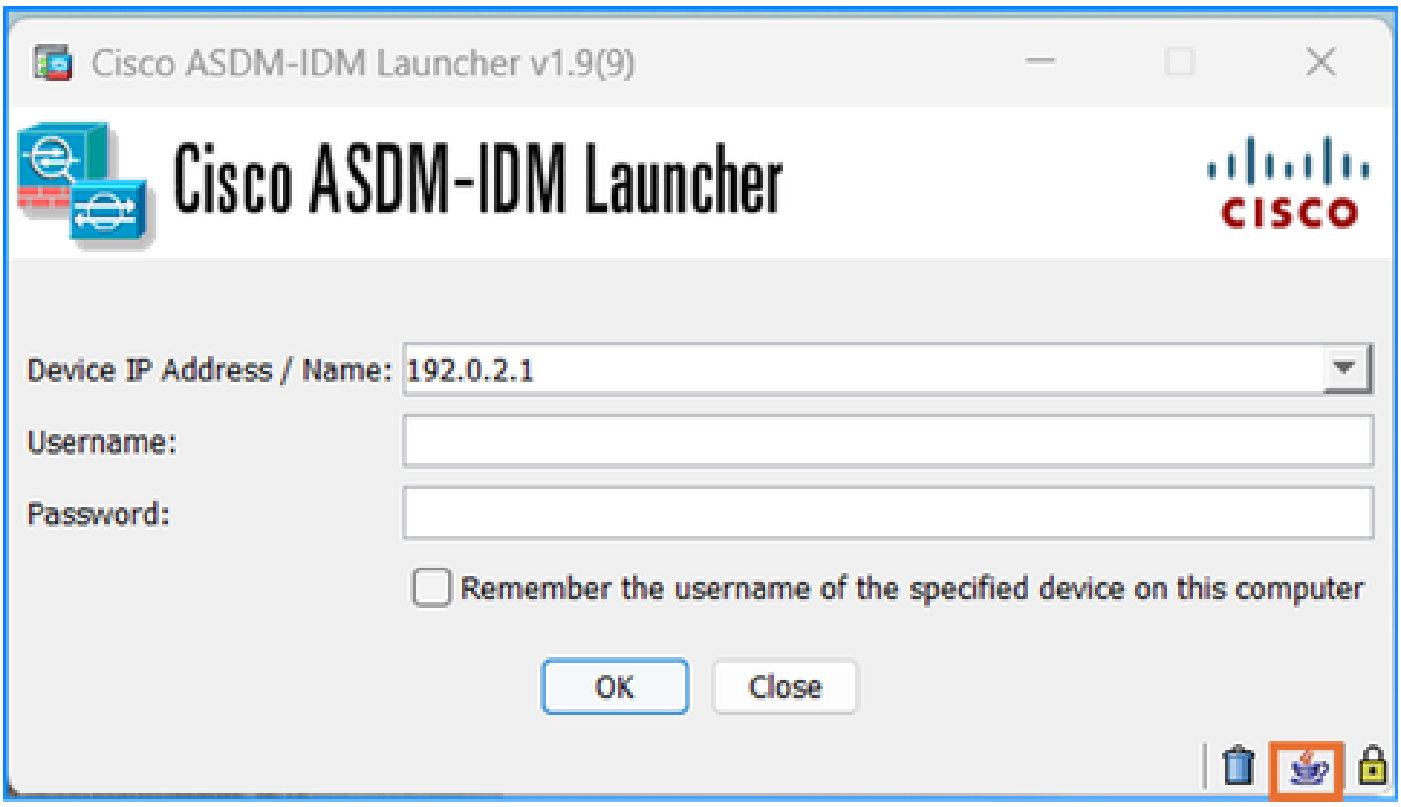
Problem 15. The Secure Client Profiles are inaccessible on ASDM

Java console logs show the “java.lang.ArrayIndexOutOfBoundsException: 3” error message:

<#root>

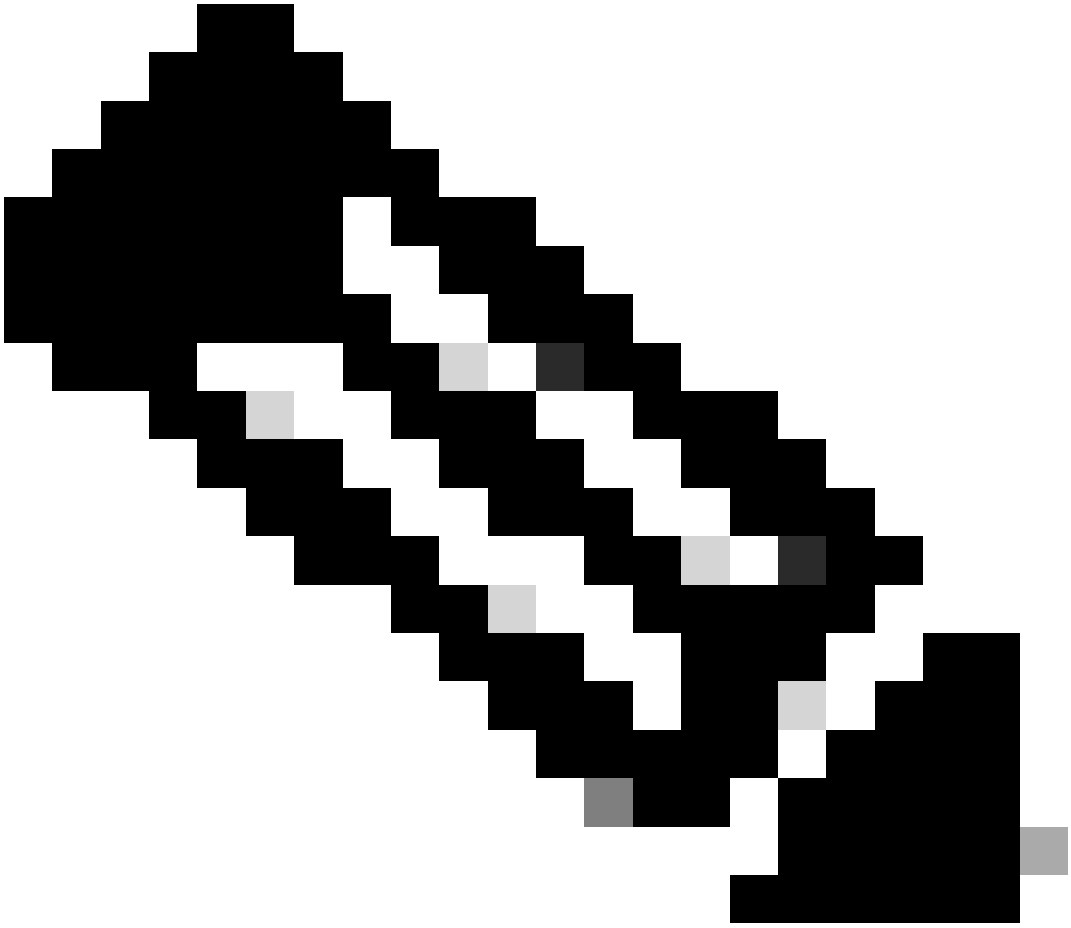
```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige

java.lang.ArrayIndexOutOfBoundsException: 3


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

To verify this symptom, enable Java console logs:



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwi56155 “Unable to access Secure Client Profile on ASDM”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

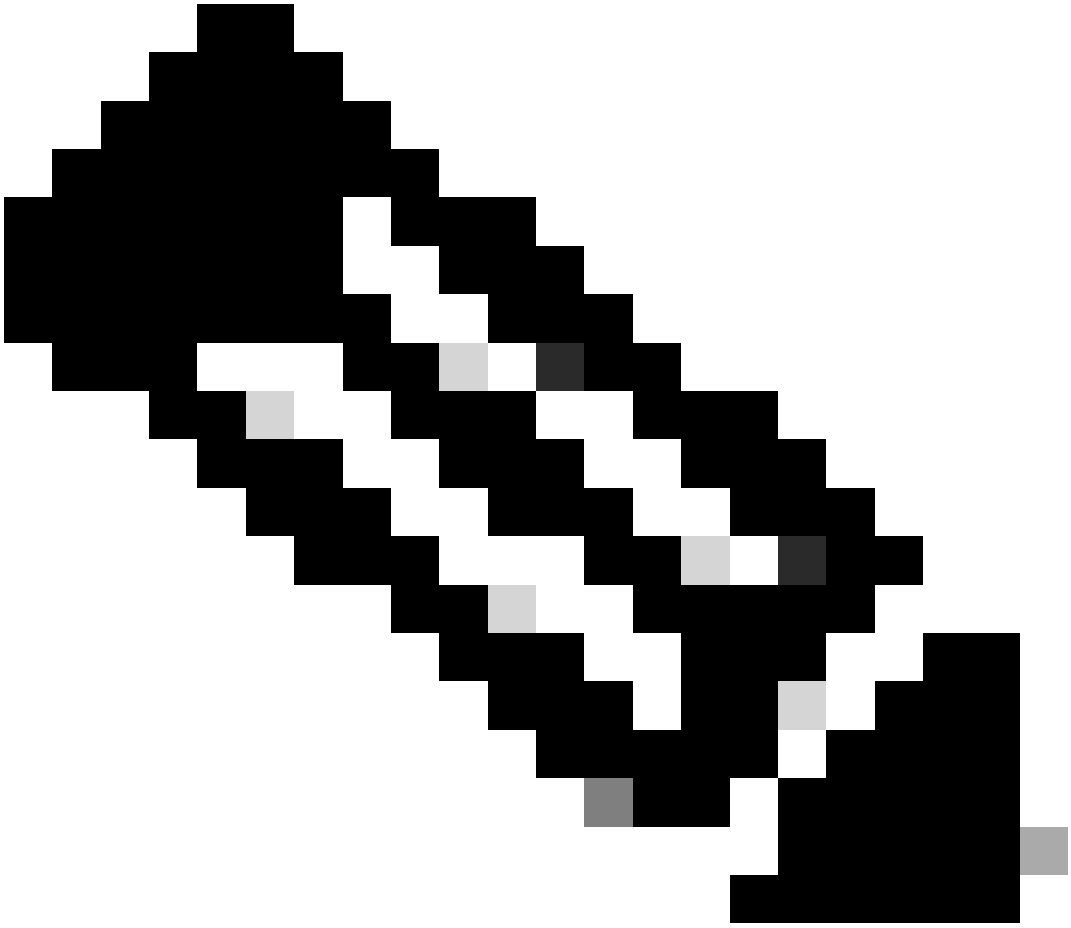
Problem 16. Unable to edit Secure Client Profile XML profiles on ASDM

The Secure Client Profile XML profiles in ASDM **Configuration** > **Remote Access VPN** > **Network (Client) Access** cannot be edited on an ASA device if there is an AnyConnect image present on the disk that is older than version 4.8.

The error message “There is no profile editor plugin in your Secure Client Image on the device. Please go to Network (Client) Access > Secure Client Software and install the Secure Client Image version 2.5 or later and then try again” is shown.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwk64399 “ASDM- Unable to edit Secure Client Profile”. The workaround is to set another AnyConnect image with a lower priority.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 17. Secure Client images are missing after configuration changes

After making changes in ASDM **Configuration** > **Network (Client) Access** > **Secure Client Profile**, the images in **Configuration** > **Network (Client) Access > Secure Client Software** are missing.

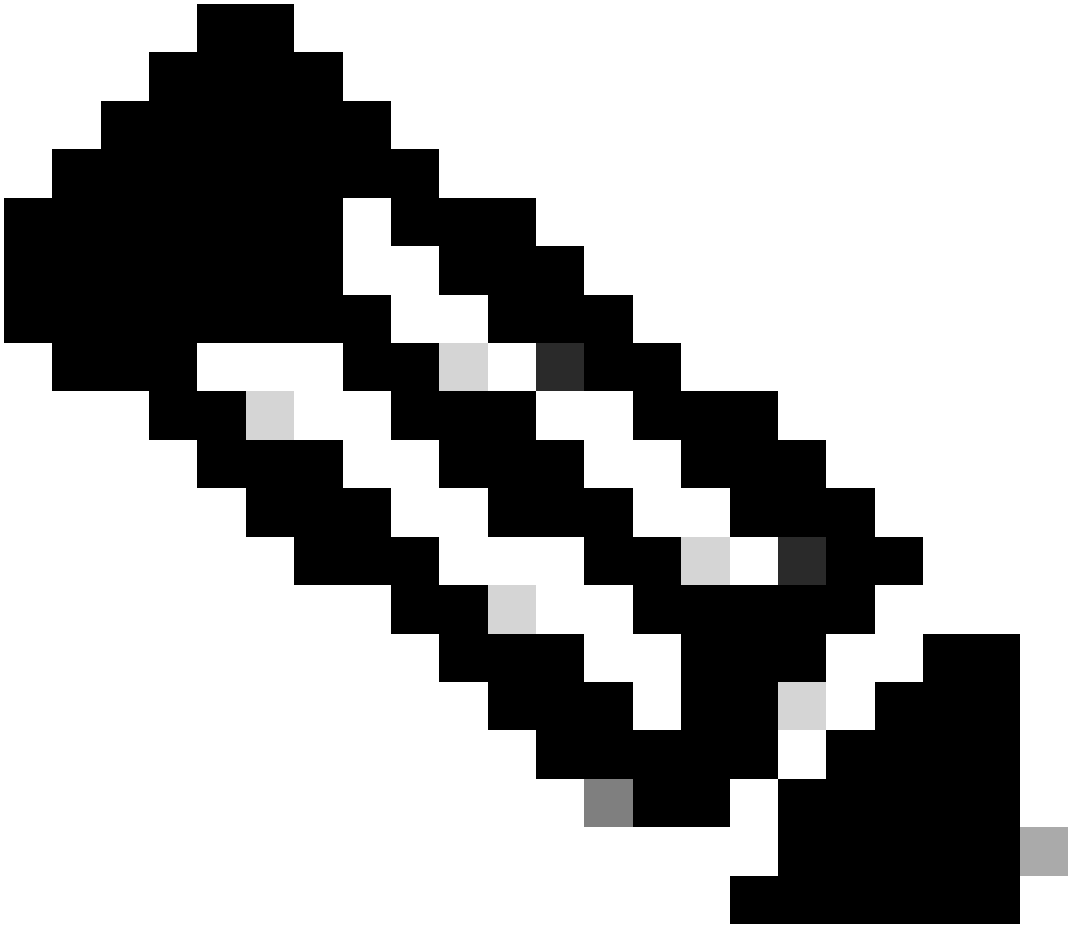
Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwf23826 “Secure Client Software is not displayed after modifying the Secure Client Profile Editor in ASDM”. The workaround options:

- Click the Refresh icon in ASDM

Or

- Close and reopen ASDM



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 18. Ineffective http server session-timeout and http server idle-timeout commands

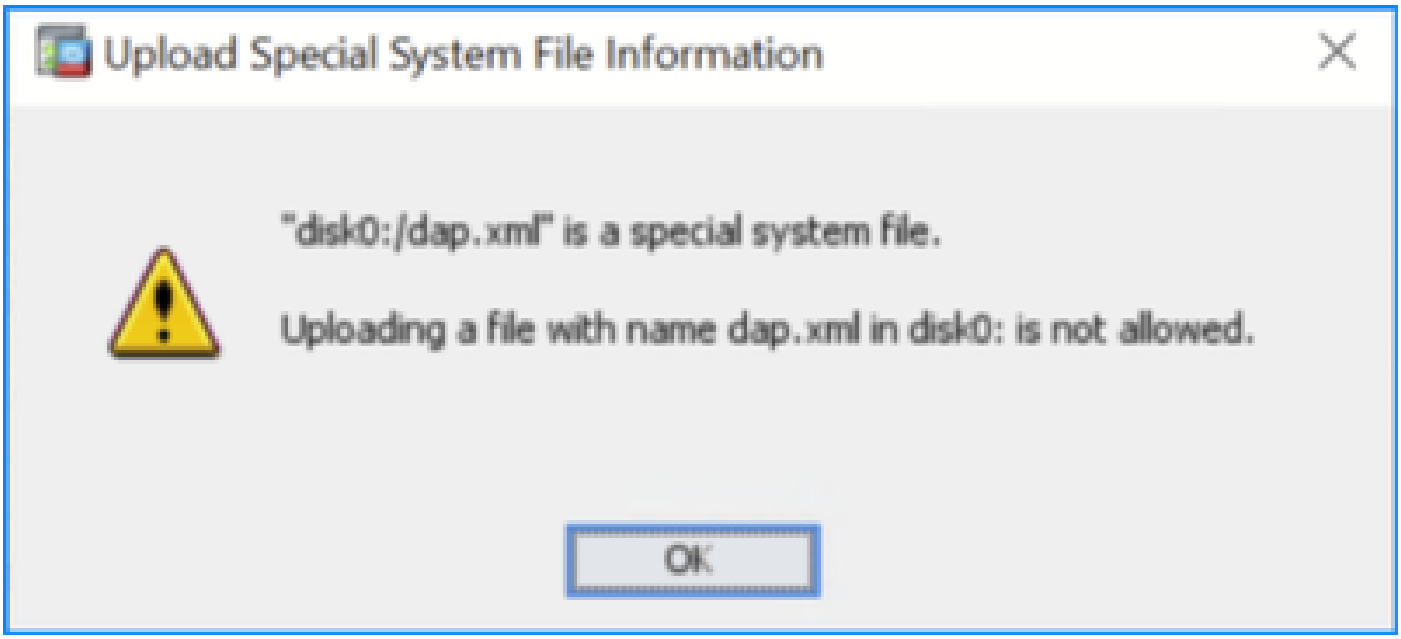
The commands **http server session-timeout** and **http server idle-timeout** have no effect in multi-context mode ASA.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCtx41707 “Support for http server timeout command in multi-context mode”. The commands are configurable however the values have no effect.

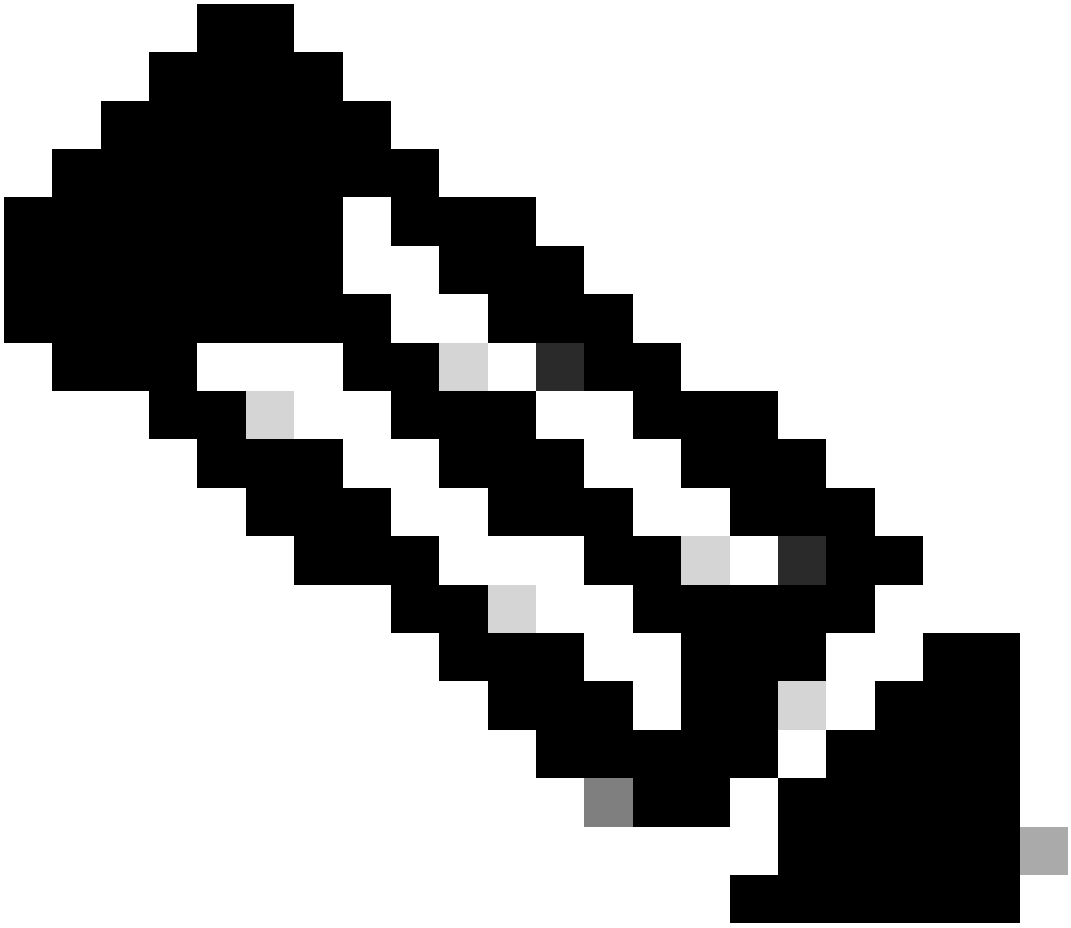
Problem 19. Dap.xml copy failure on ASDM

The copy of dap.xml to ASA via the File Management window in ASDM fails with the error “disk0:/dap.xml is a special system file. Uploading a file the name dap.xml in disk0: is not allowed”:



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCvt62162 “Cannot copy dap.xml using File Management in ASDM 7.13.1”. The workaround is to copy the file directly to the ASA using protocols like FTP or TFTP.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 20. No IKE policies and IPSEC proposals visible on ASDM

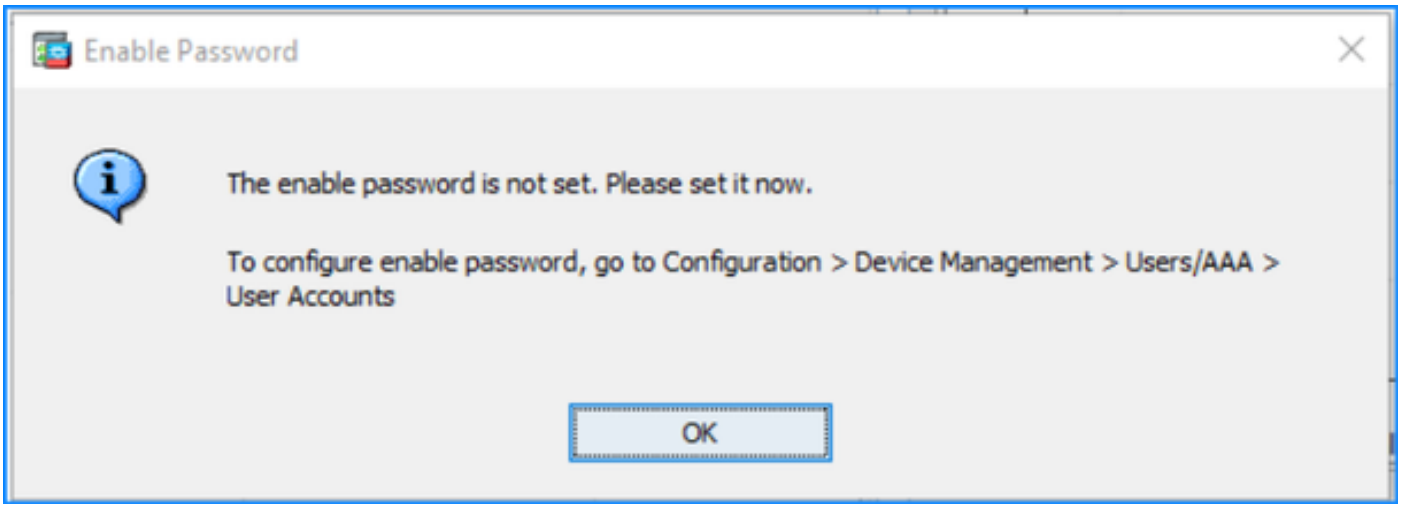
ASDM does not display IKE policies and IPSEC proposals in **Configurations** > **Site-to-Site VPN** window.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwm42701 “ASDM display blank in IKE policies and IPSEC proposals tab”.

Problem 21. ASDM displays the message “The enable password is not set. Please set it now.”

ASDM display the message “The enable password is not set. Please set it now.” after changing the enable password in the command line:



Troubleshoot – Recommended Actions

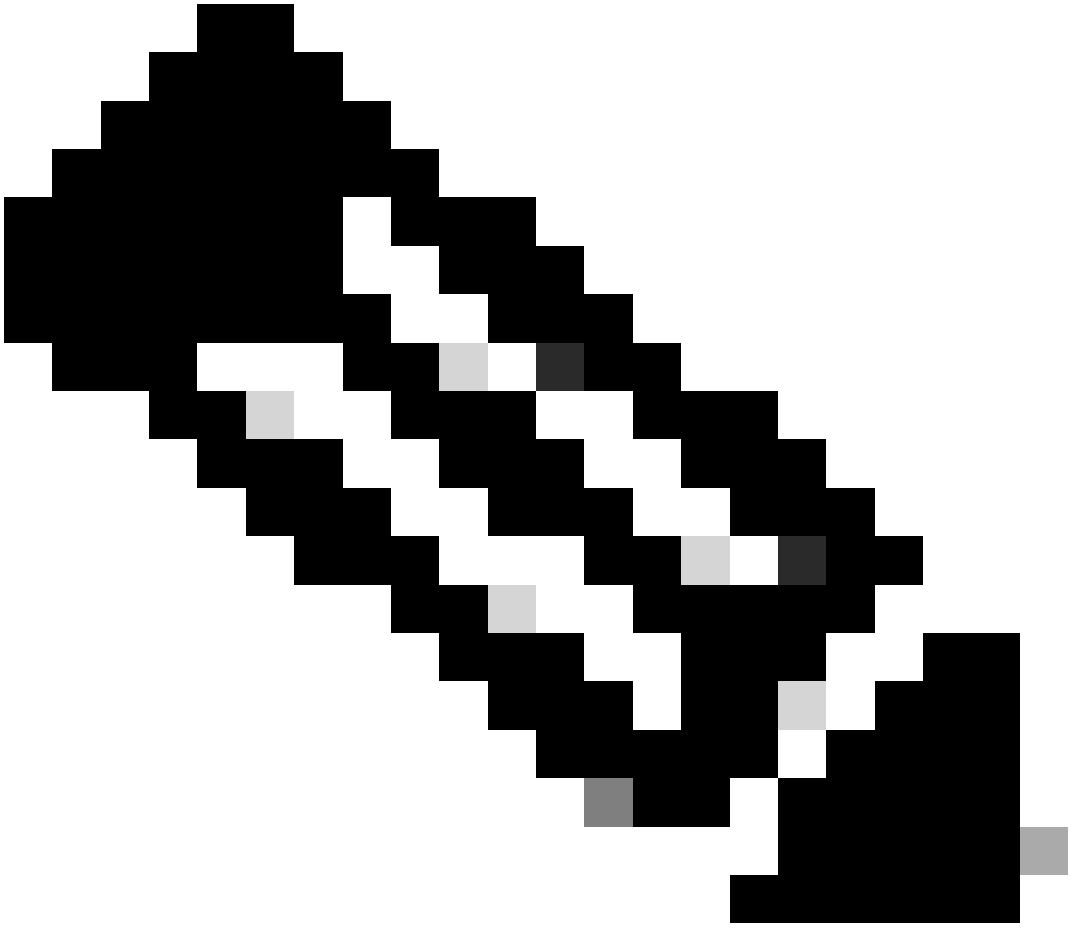
Refer to the software Cisco bug ID CSCvq42317 “ASDM prompts to change enable password after it was set on CLI”.

Problem 22. ASDN object disappear after refreshing ASDM UI

When adding an object group and an object host to an existing object group and after refreshening the ASDM the object group disappears from the ASDM list. The object names must start with numbers for this defect to match.

Troubleshoot – Recommended Actions

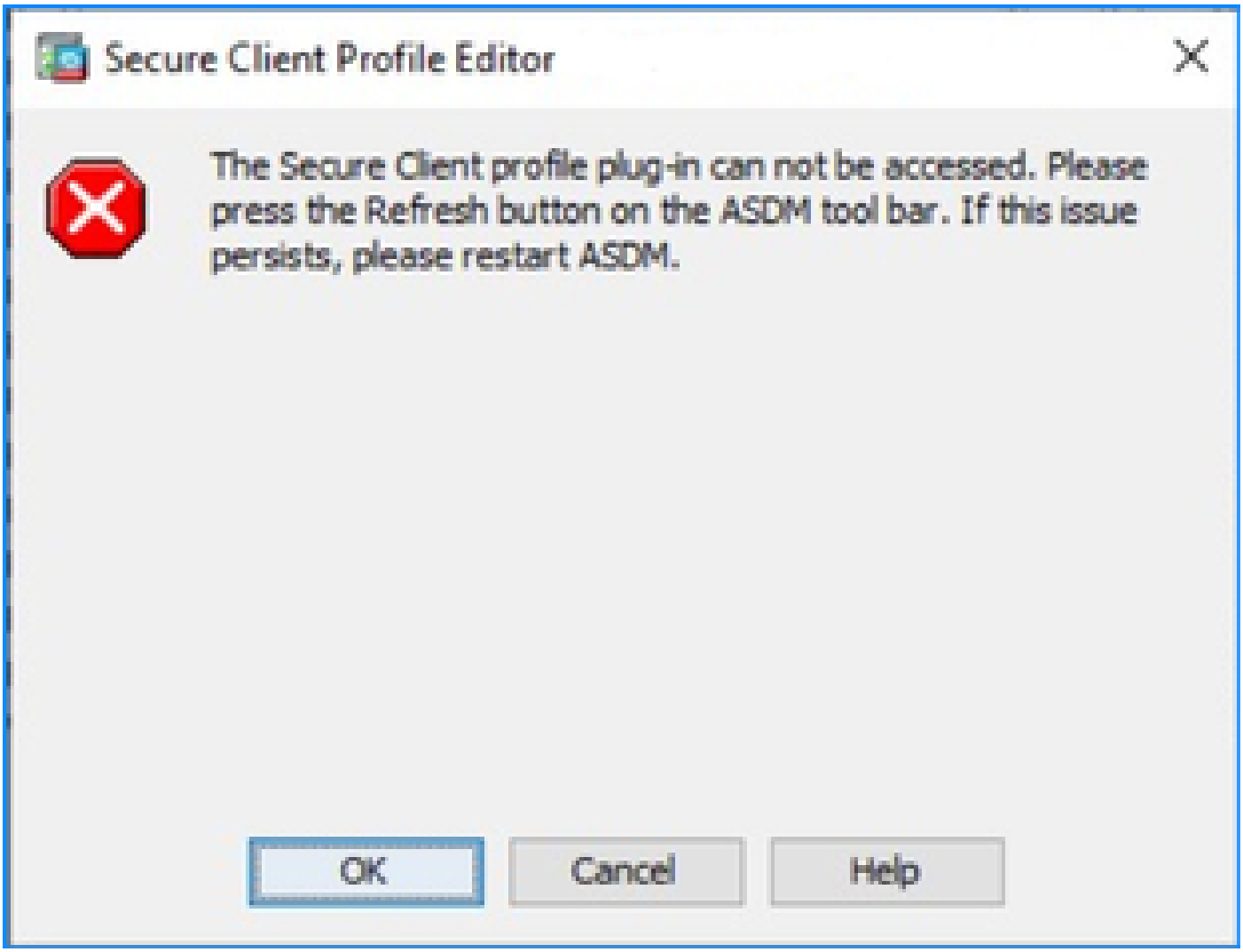
Refer to the software Cisco bug ID CSCwf71723 “ASDM losing configured objects/object groups”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

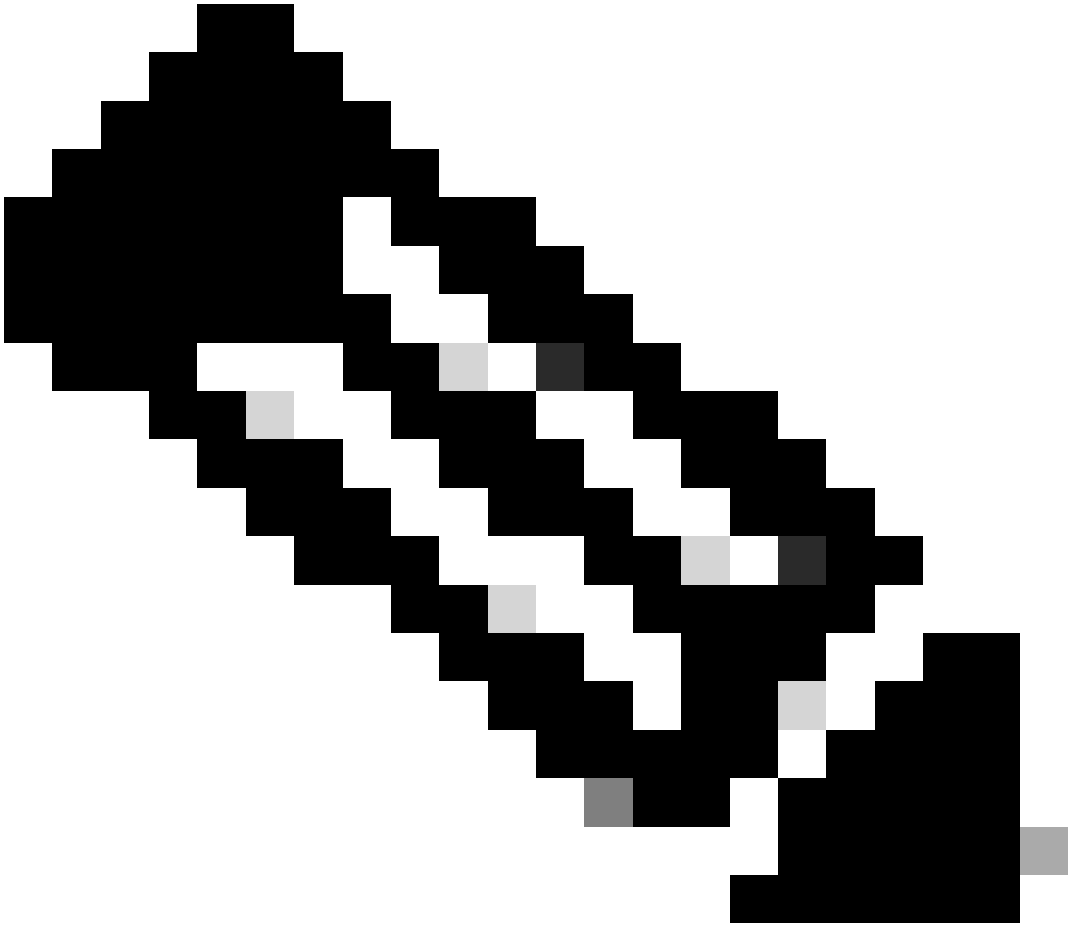
Problem 23. Unable to edit AnyConnect client profiles for versions earlier than 4.5

The AnyConnect client profiles cannot be edited for AnyConnect Profile earlier than version 4.5. The error message is “The Secure Client profile plug-in can not be accessed. Please press Refresh button on the ASDM tool bar. If this issue persists, please restart ASDM.”:



Troubleshoot – Recommended Actions

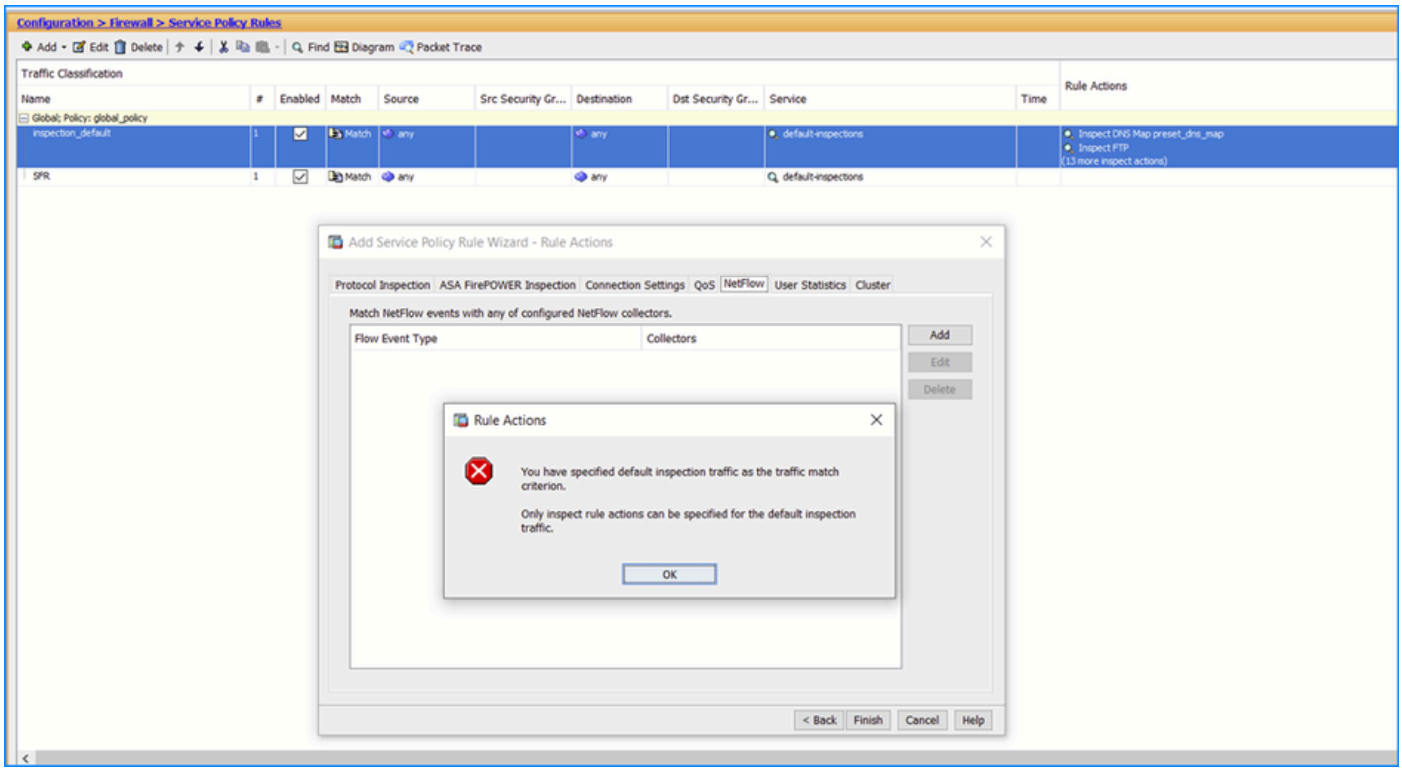
Refer to the software Cisco bug ID CSCwf16947 “ASDM - Unable to load Anyconnect Profile Editor”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

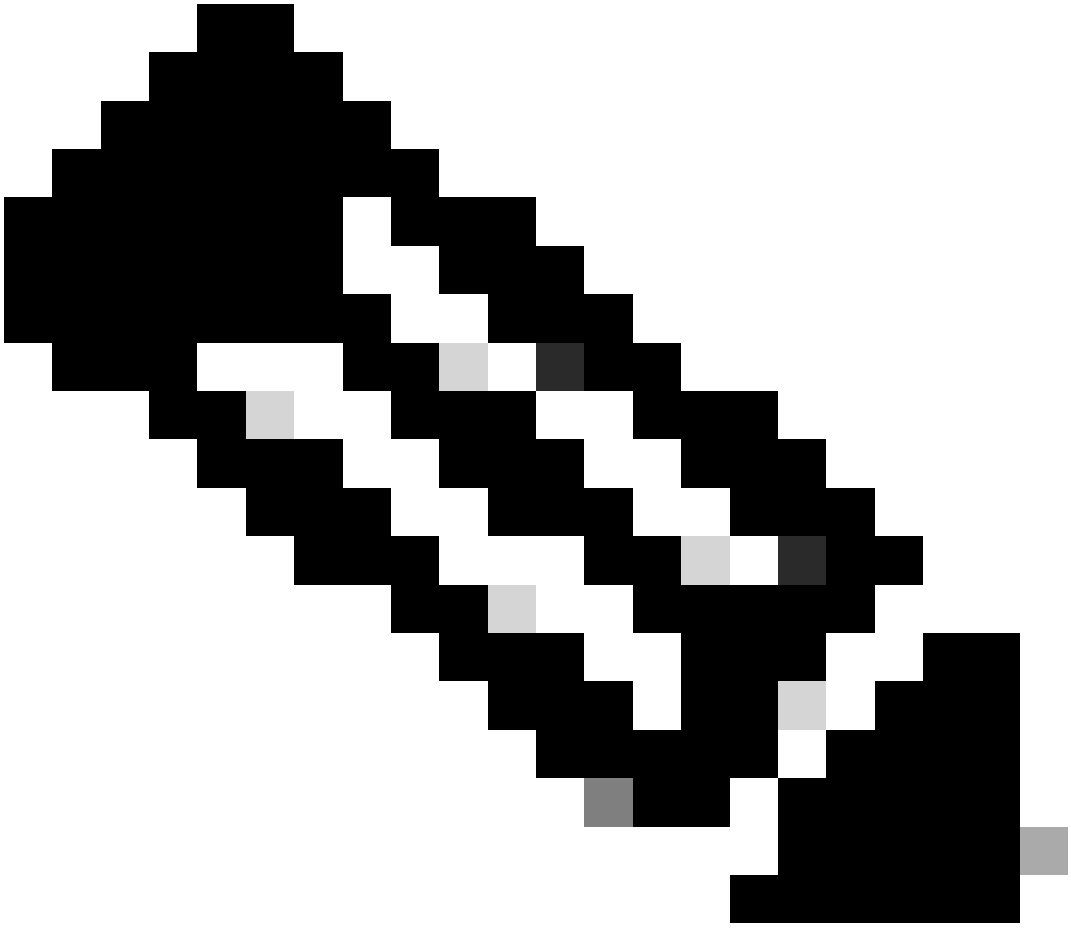
Problem 24. Unable to navigate to the Edit Service Policy > Rule Actions > ASA FirePOWER Inspection tab

In ASDM version 7.8.2, users are unable to navigate to the **Edit Service Policy** > **Rule Actions** > **ASA FirePOWER Inspection** tab and the error is displayed: "You have specified default inspection traffic as the traffic match criterion. Only inspect rule actions can be specified for the default inspection traffic." This occurs even when an ACL has been selected for redirection:



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCvg15782 “ASDM - Unable to view modify SFR traffic redirection after upgrade to version 7.8(2)”. The workaround is to use the CLI to edit the policy-map configuration.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

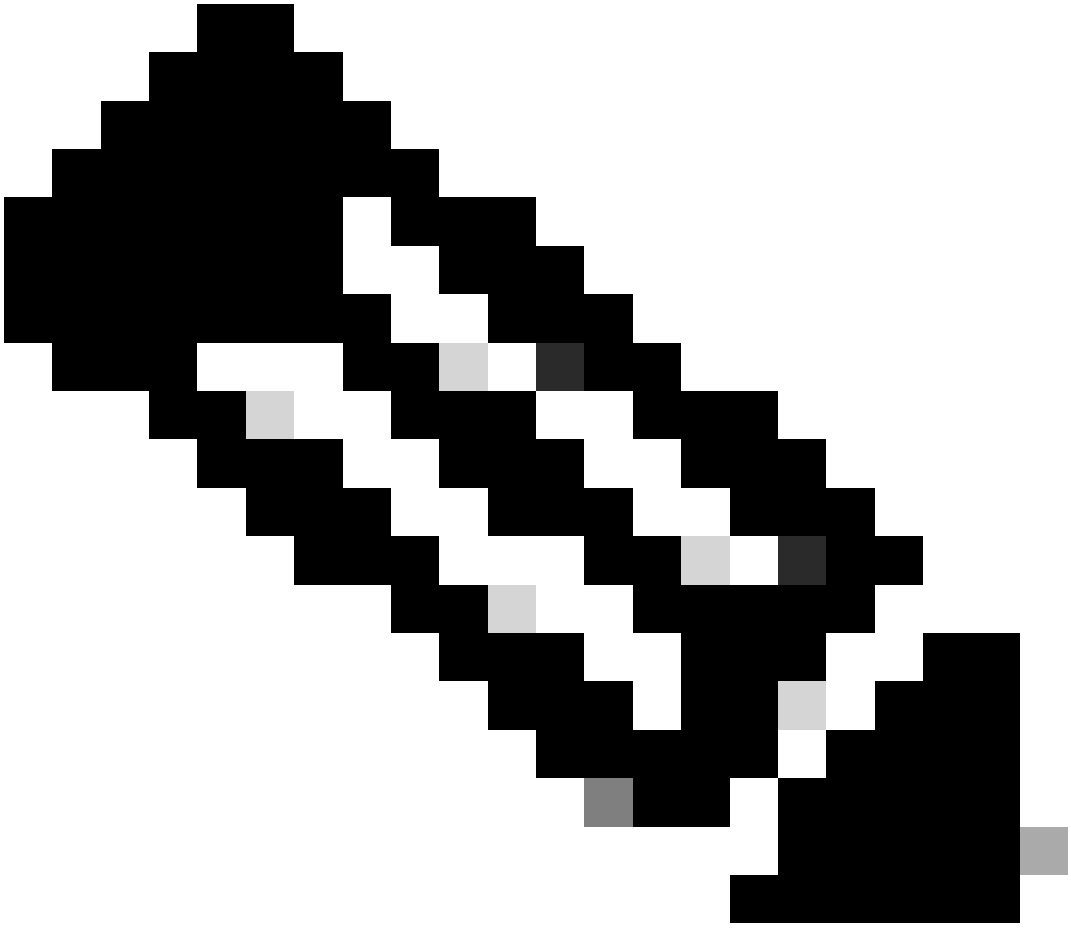
Problem 25. AnyConnect Image version 5.1 and AnyConnect profile editor on ASDM

These symptoms are observed for the Secure Client software version 5.1:

1. The group policy module names not listed when loading the Win/Mac/Linux packages
2. ASDM fails to open AnyConnect Profile Editor.

Troubleshoot – Recommended Actions

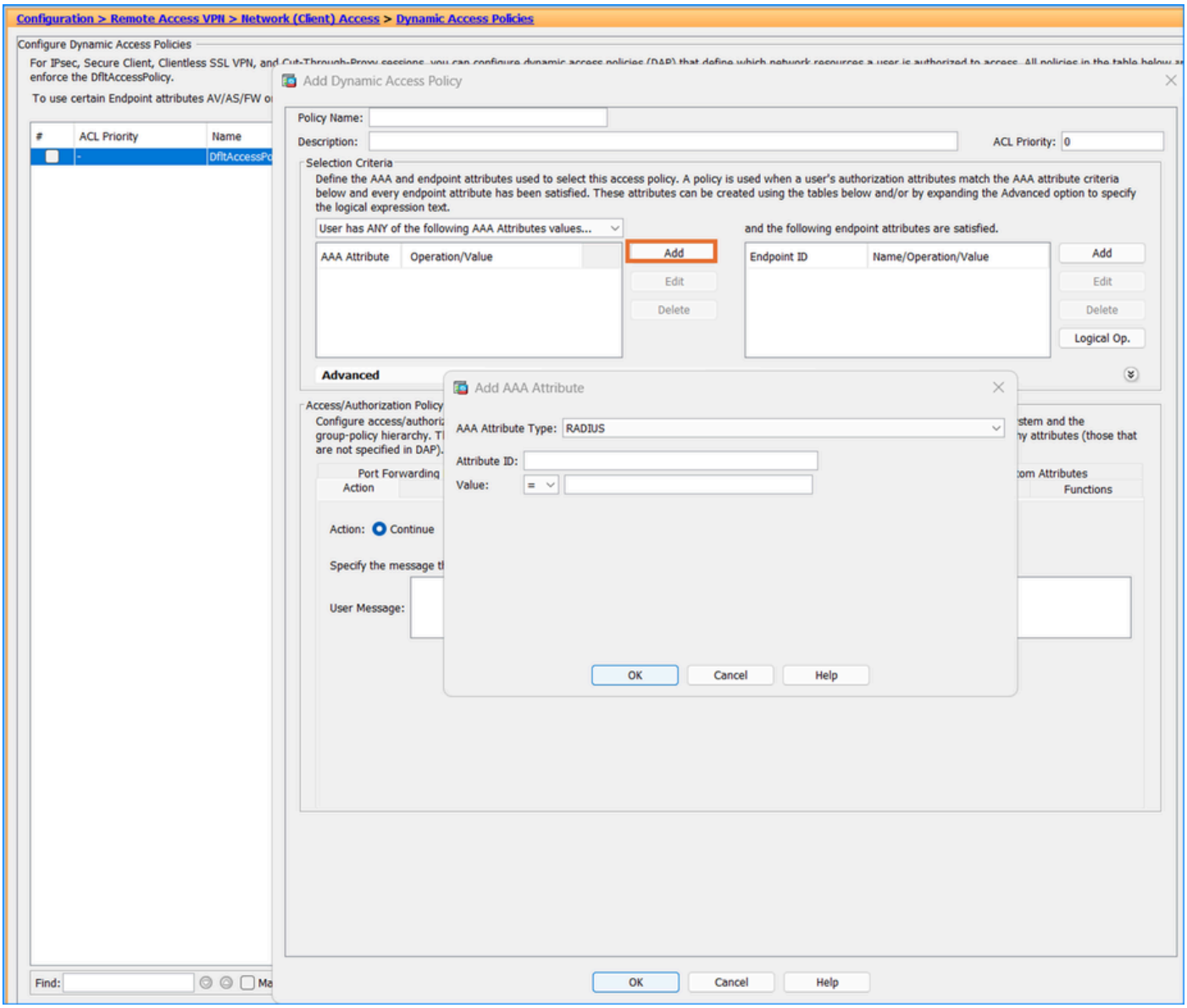
Refer to the software Cisco bug ID CSCwh74417 “ASDM : AnyConnect Profile Editor and Group Policy cannot be loaded when using the CSC Image 5.1”. The workaround is to use lower versions of the Secure Client.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

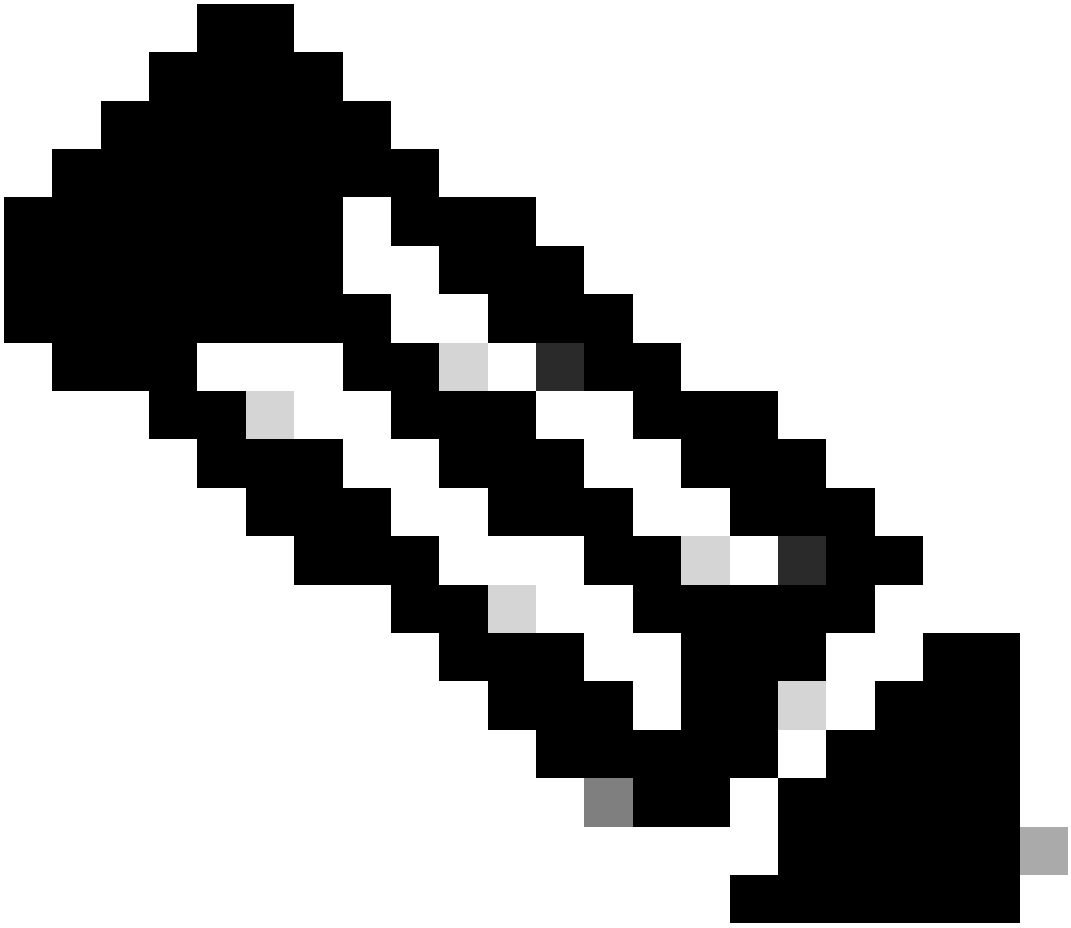
Problem 26. AAA Attributes type (Radius/LDAP) are not visible in ASDM

AAA Attributes type (Radius/LDAP) are not visible in **ASDM** > **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add > On AAA attribute field > Add > Select Radius or LDAP:**



Troubleshoot – Recommended Actions

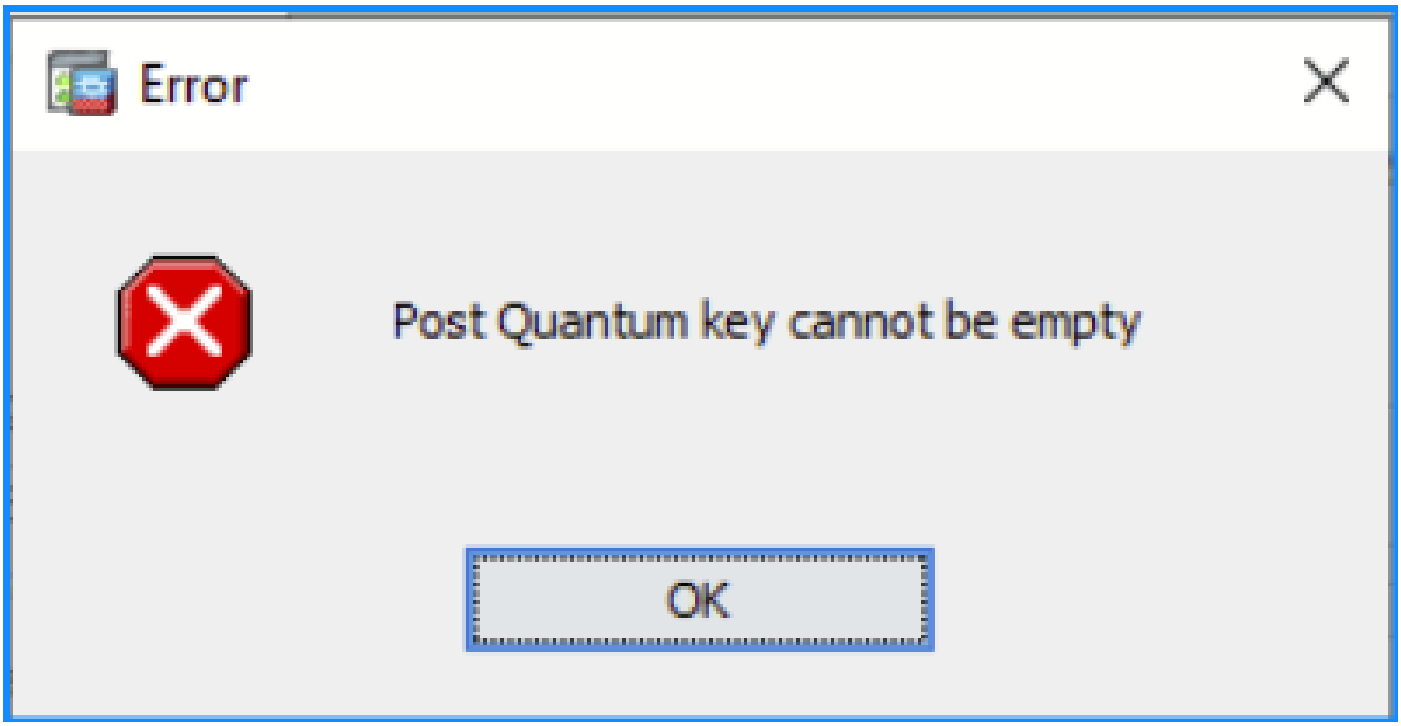
Refer to the software Cisco bug ID CSCwa99370 “ASDM : ASDM:DAP config missing AAA Attributes type (Radius/LDAP)” and Cisco bug ID CSCwd16386 “ASDM:DAP config missing AAA Attributes type (Radius/LDAP)”.



Note: These defects have been fixed in recent ASDM software releases. Check the defect details for more information.

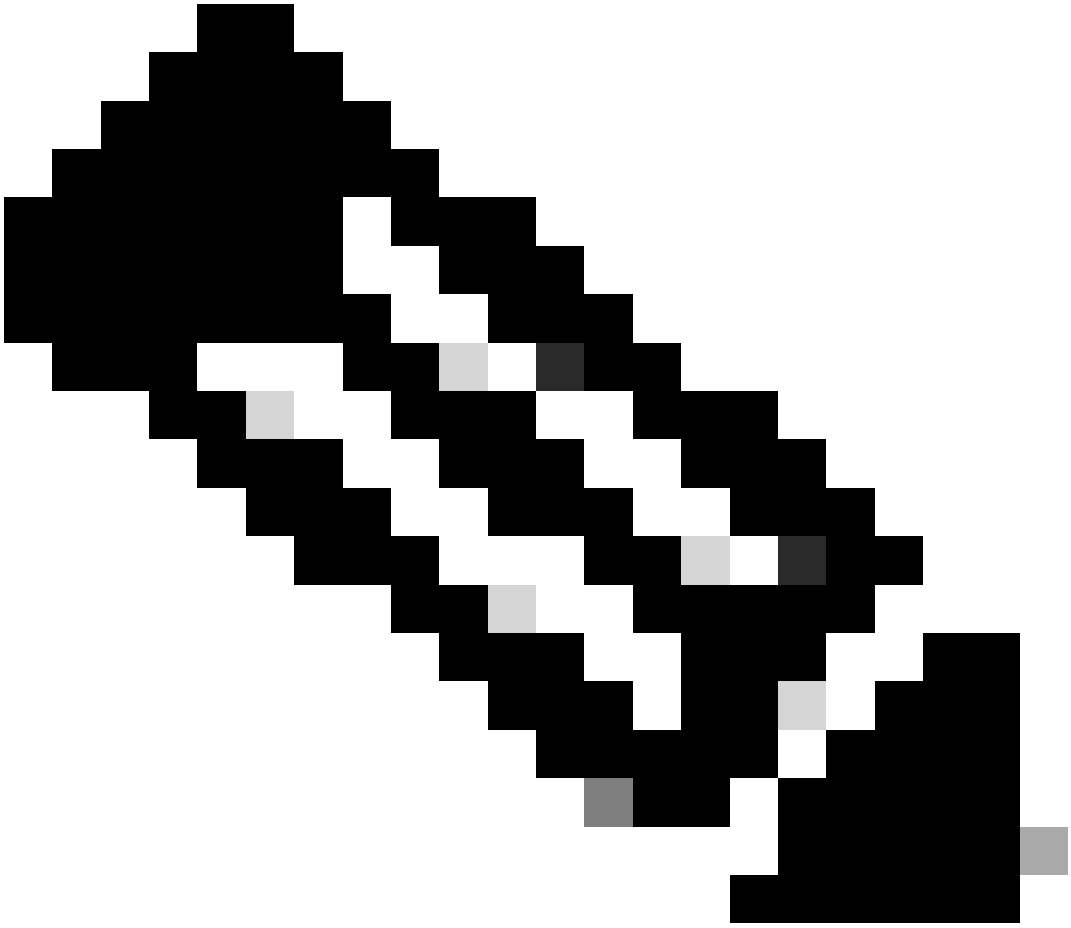
Problem 27. 'Post Quantum key cannot be empty' error is shown on ASDM

The error '**Post Quantum key cannot be empty**' is shown when editing the **Advanced** section in ASDM > **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **IPsec (IKEv2) Connection Profiles':**



Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwe58266 “ASDM IKev2 configuration - Post Quantum Key cannot be empty error message”.



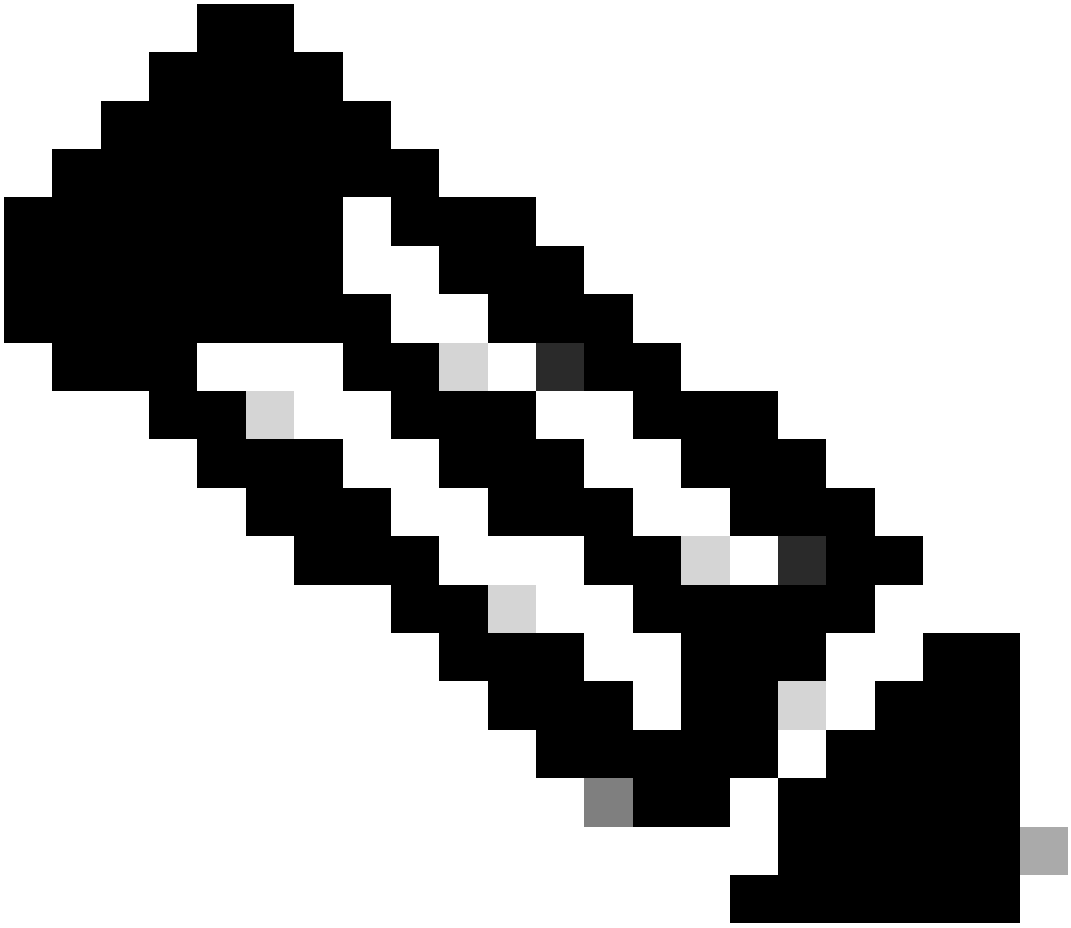
Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 28. ASDM does not display any results when using the option "where used"

ASDM does not display any results when using the option "where used" found by navigating to **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups** and right-clicking to an **Object**.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwd98702 “"Where used" option in ASDM not working”.



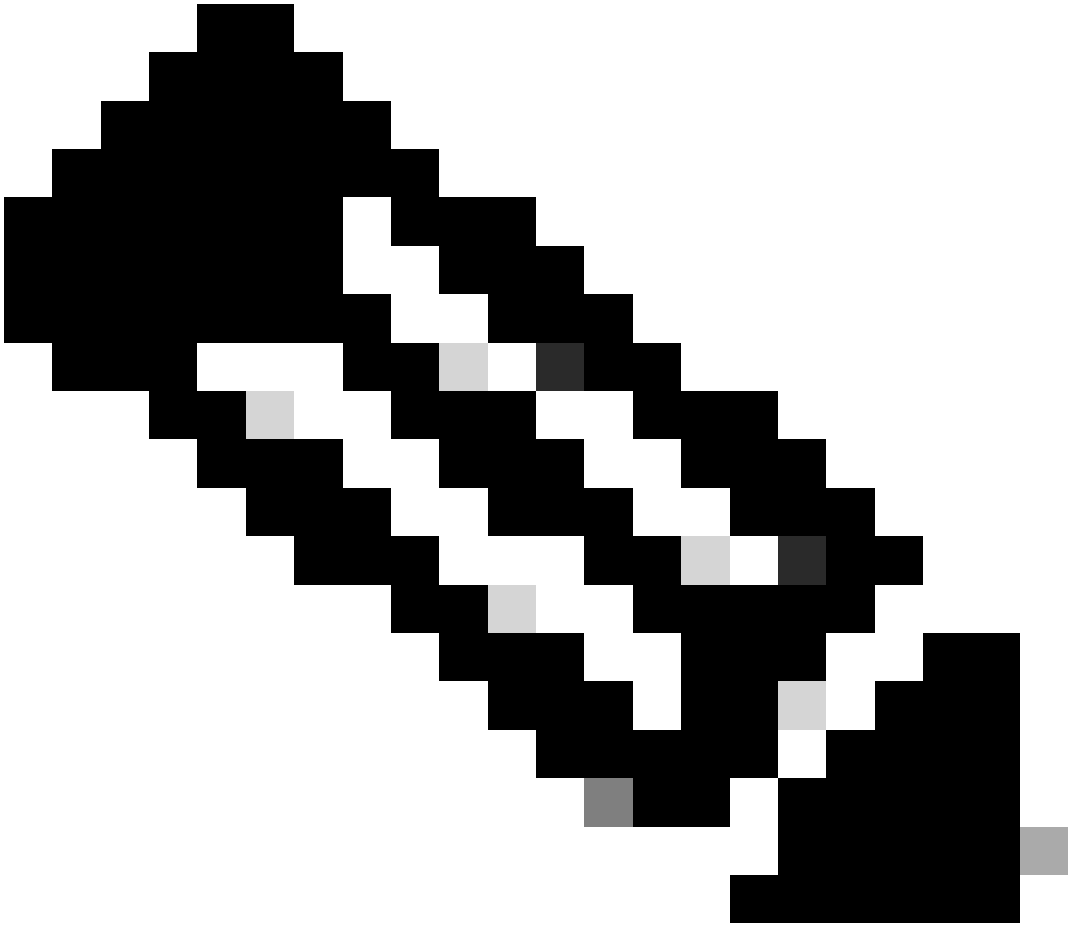
Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 29. Warning message “[Network Object] cannot be deleted because it is used in the following” when deleting a network object

ASDM does not display the warning message “[Network Object] cannot be deleted because it is used in the following” when deleting a network object that is referenced in a network group in **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwe67056 "[Network Object] cannot be deleted because it is used in the following" warning not appearing”.



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Problem 30. Usability problems with Network Objects/Group Tab in ASDM

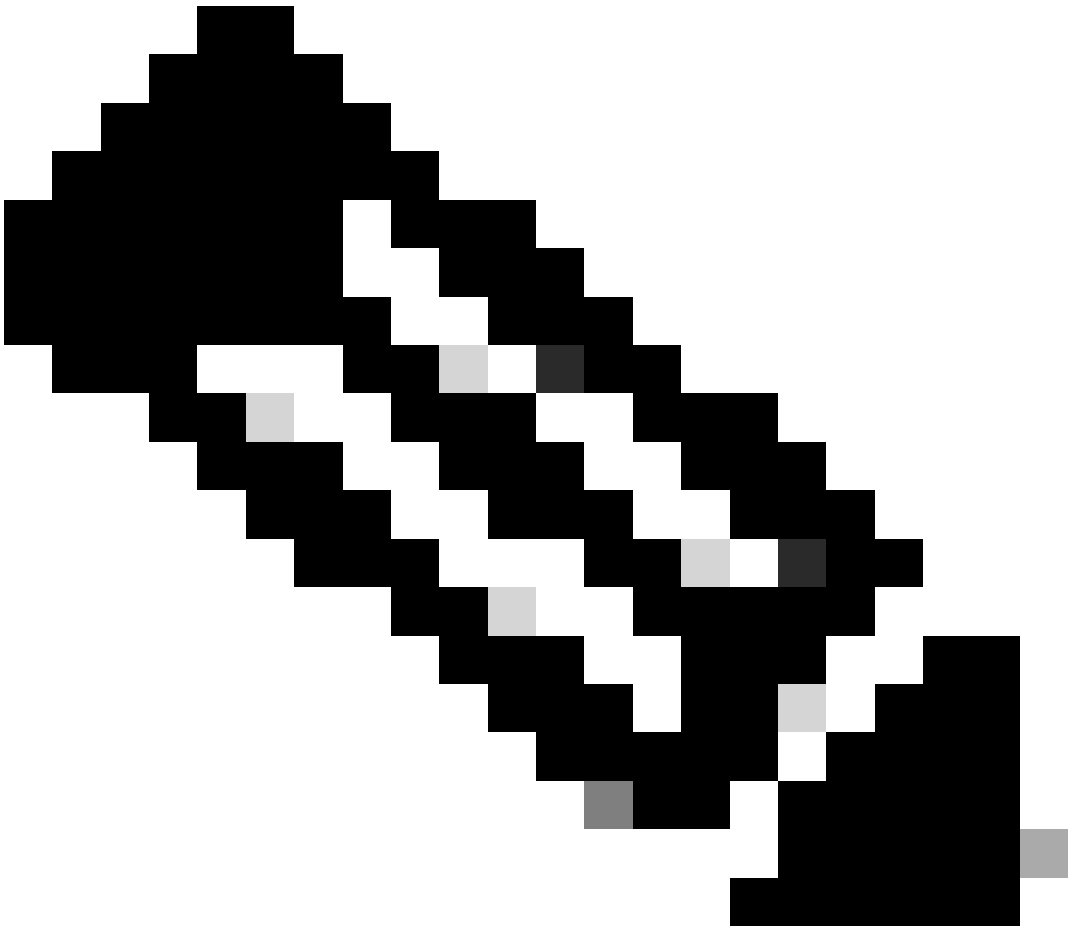
One or more of these symptoms are observed:

- The "Name" Text-Input in the "Create new Object Member" section of the "Add/Edit Object Group Windows" is marked as "optional". However, the "Add>>" button to create and add the object is disabled unless a name is entered.
- The "Usages" Tab that opens when a user clicks the "Where Used..." context menu only lists entities (ACLs, route-maps, object-groups) that directly reference the object. It must also recursively list second, third, and so on. order references (that is an ACL that uses an object group which contains an object must also be listed as "usage" of the Object).
- The "Delete" operation available in the context menu also displays this behavior. It automatically deletes any entity that directly references the object (if the entity would become empty when the object is deleted). It does not operate this way when a second, third, and so on. order reference would become empty because of deleting the object and the first order reference.

The user can be led to believe that ASDM prevents entities that would become empty because of the object deletion from the remaining in configuration. This is however not necessarily the case.

Troubleshoot – Recommended Actions

Refer to the software Cisco bug ID CSCwe86257 “Usability of Network Objects/Group Tab in ASDM”.

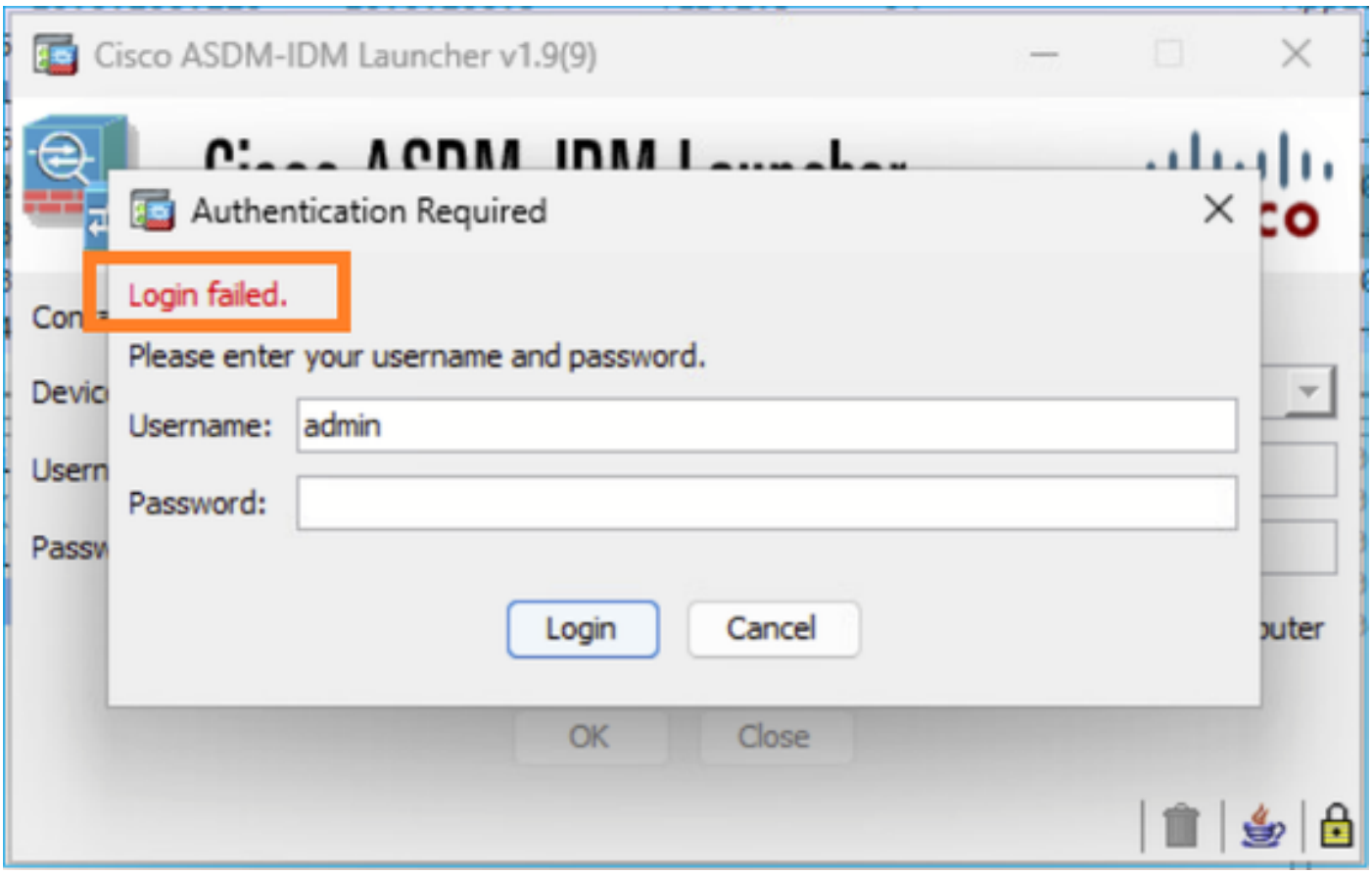


Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Troubleshoot ASDM Authentication Problems

Problem 1. ASDM Login Failed

The error shown on ASDM UI is:



Troubleshoot – Recommended Actions

This error can be seen when you have both HTTP and Webvpn Cisco Secure Client (AnyConnect) enabled on the same interface. Thus, all conditions must be met:

1. AnyConnect/Cisco Secure Client is enabled on an interface
2. HTTP server is enabled on the same interface and same port as AnyConnect/Cisco Secure Client

Example:

```
<#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
```

Troubleshooting Tip: Enable 'debug http 255' and you can see the conflict between ASDM and 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
```

As a side note, despite the login failure, the ASA syslogs show that the Authentication is successful:

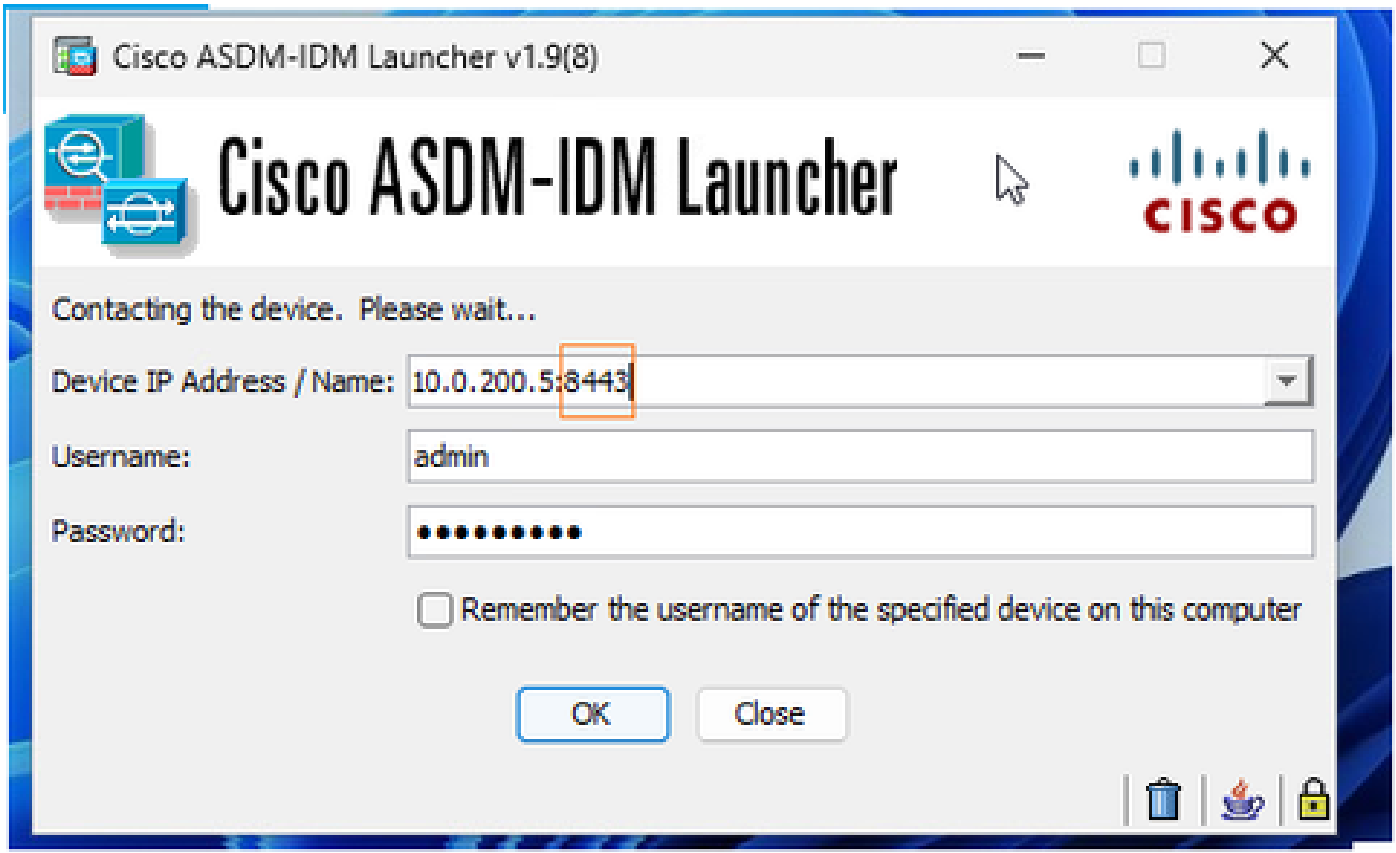
```
<#root>
asa#
show logging

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
```

Workarounds

Workaround 1

Change the TCP port for either the ASA HTTP server, for example:

```
<#root>
ciscoasa#
configure terminal

ciscoasa(config)#
http server enable 8443
```



Workaround 2

Change the TCP port for the AnyConnect/Cisco Secure Client, for example:

```
<#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
```

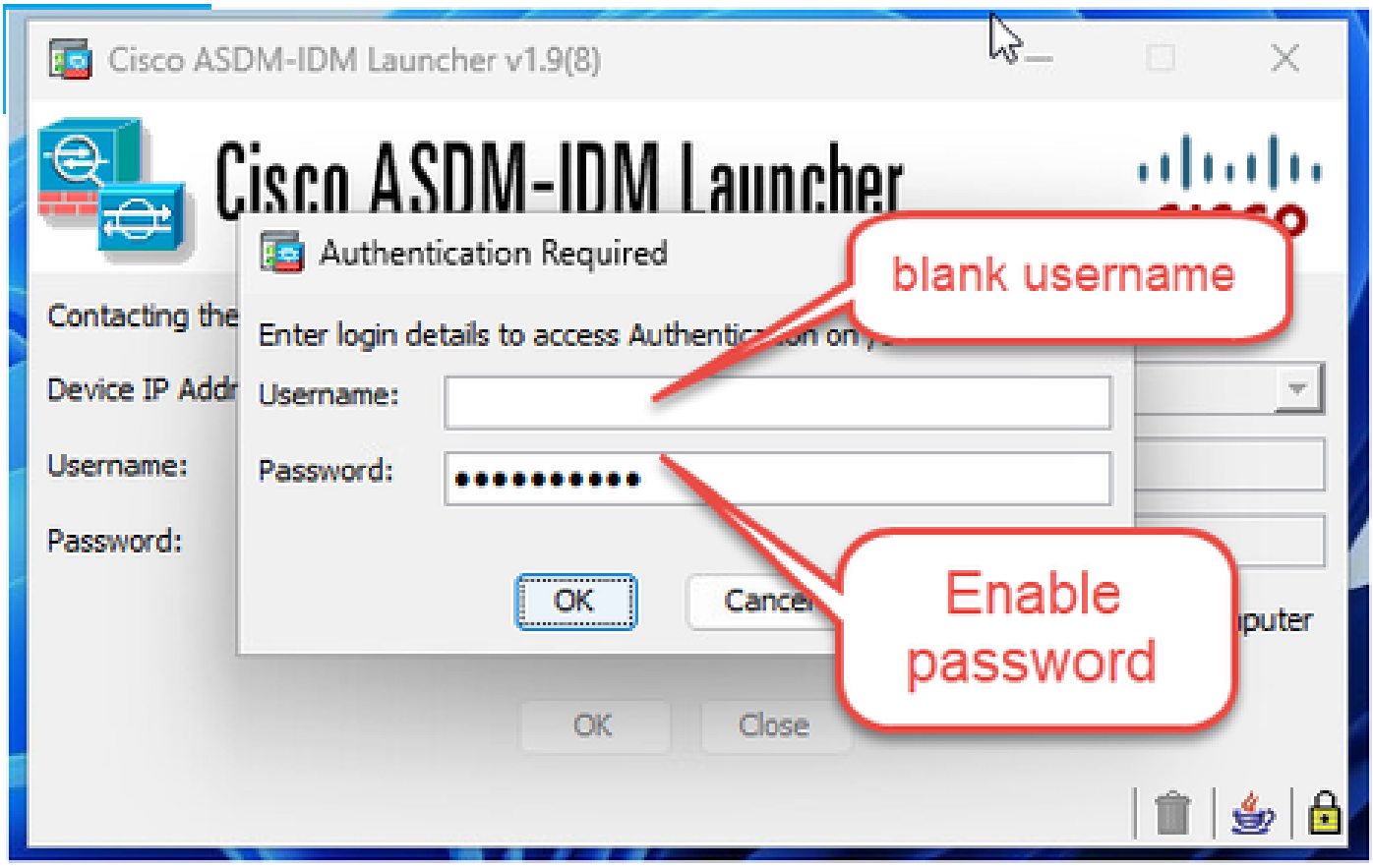
Workaround 3

An alternative workaround is to remove the "aaa authentication http console" configuration:

<#root>

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

In this case, you can login to ASDM by just using the enable password:



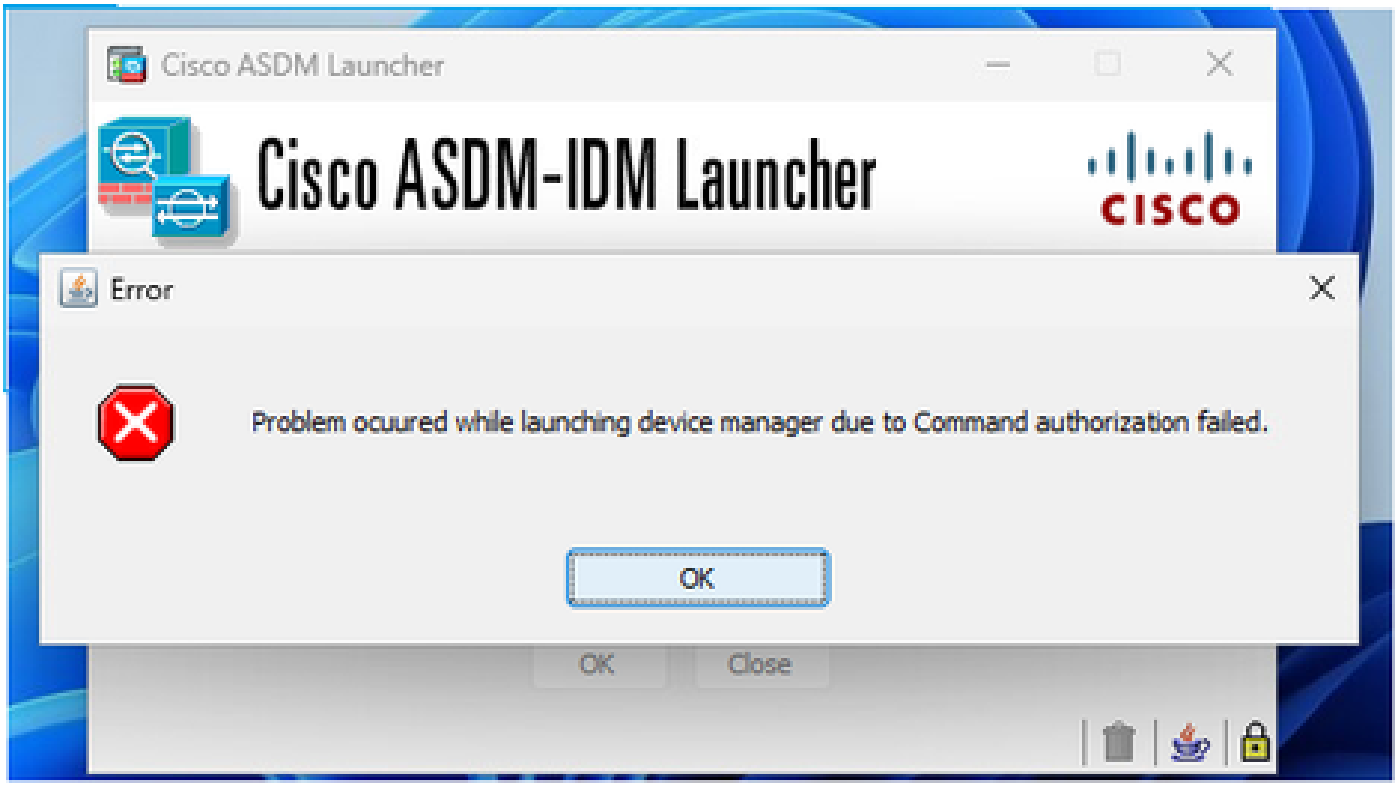
Related Defect

Cisco bug ID CSCwb67583

Add warning when webvpn and ASDM enabled on same interface

Problem 2. ASDM Command authorization failed

The error shown on ASDM UI is:



Troubleshoot – Recommended Steps

Check your AAA configuration on ASA and ensure that:

- You have aaa authentication also configured.
- If you use a remote authentication server, it is reachable and authorizes the commands.

Reference

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

Problem 3. Configure ASDM Read-only access

Sometimes you want to provide read-only access to ASDM users.

Troubleshoot – Recommended Steps

Create a new user with a custom privilege level (5), for example:

<#root>

```
asa(config)#
```

```
username [username] password [password] privilege 5
```

This command creates a user with a privilege level of 5, which is the "monitoring-only" level. Replace `[username]` and `[password]` with the desired username and password.

Details

Local command authorization lets you assign commands to one of 16 privilege levels (0 to 15). By default, each command is assigned either to privilege level 0 or 15. You can define each user to be at a specific privilege level, and each user can enter any command at the assigned privilege level or less. The ASA supports user privilege levels defined in the local database, a RADIUS server, or an LDAP server (if you map LDAP attributes to RADIUS attributes).

Procedure

Step 1	Choose **Configuration > Device Management > Users/AAA > AAA Access > Authorization.**
Step 2	Check the **Enable authorization for ASA command access > Enable** check box.
Step 3	Choose **LOCAL** from the **Server Group** drop-down list.
Step 4	When you enable local command authorization, you have the option of manually assigning privilege levels to individual commands or groups of commands or enabling the predefined user account privileges. · Click **Set ASDM Defined User Roles** to use predefined user account privileges. The **ASDM Defined User Roles Setup** dialog box appears. Click **Yes** to use the predefined user account privileges: **Admin** (privilege level 15, with full access to all CLI commands; **Read Only** (privilege level 5, with read-only access); and **Monitor Only** (privilege level 3, with access to the Monitoring section only). · Click **Configure Command Privileges** to manually configure command levels. The **Command Privileges Setup** dialog box appears. You can view all commands by choosing All Modes from the Command Mode drop-down list, or you can choose a configuration mode to view the commands available in that mode. For example, if you choose context, you can view all commands available in context configuration mode. If a command can be entered in user EXEC or privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The Variant column displays show, clear, or cmd. You can set the privilege only for the show, clear, or configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the show or clear prefix) or as the no form. To change the level of a command, double-click it or click Edit. You can set the level between 0 and 15. You can only configure the privilege level of the main command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately.

	To change the level of all commands that appear, click Select All, then Edit. Click OK to accept your changes.
Step 5	Click **Apply**. The authorization settings are assigned, and the changes are saved to the running configuration.

Reference

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)

Troubleshoot – Recommended Steps

At the time of this writing, ASDM does not support MFA (or 2FA). This limitation includes MFA with solutions like PingID, and so on.

Reference

Cisco Bug id CSCvs85995

ENH: ASDM access with two factor authentication or MFA

Problem 5. ASDM External authentication configuration

Troubleshoot – Recommended Steps

You can use LDAP, RADIUS, RSA SecurID, or TACACS+ to configure external authentication on ASDM.

References

- 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. ASDM LOCAL authentication fails

Troubleshoot – Recommended Steps

In case you use external authentication and LOCAL authentication as a fallback the local authentication works only if your external server is down or not working. Only in this scenario the LOCAL authentication takes over and you can connect with the LOCAL users.

This is because external authentication takes precedence over LOCAL authentication.

Example:

<#root>

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

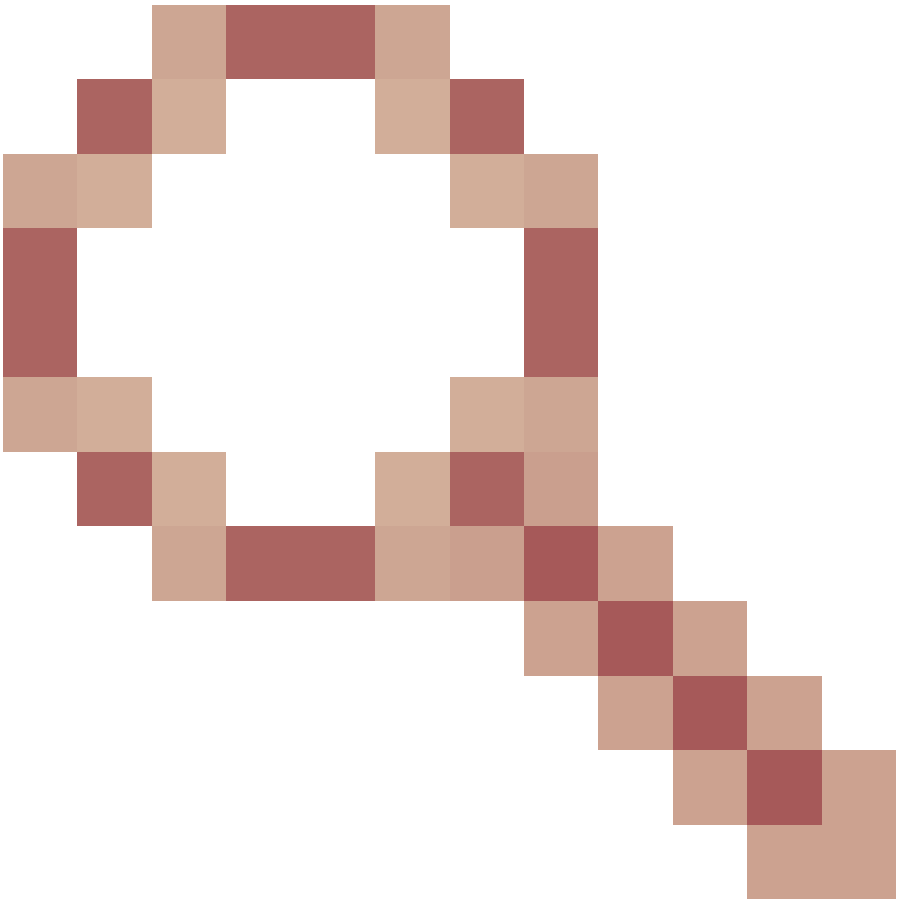
Reference

- 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. ASDM One-Time Password

Troubleshoot – Recommended Steps

- ASDM OTP (one-time-password) authentication support was added in ASA version 8.x - 9.x an in single-routed-mode only.
- ASDM OTP authentication for ASA Firewall transparent mode and/or multi-context mode does not enter into this category.



Refer to the Cisco Bug id CSCtf23419
ENH: ASDM OTP authentication support in multi-context and transparent modes

Problem 8. Connection Profile does not show all methods

The problem in this case is a mismatch between the ASA CLI configuration vs the ASDM UI.

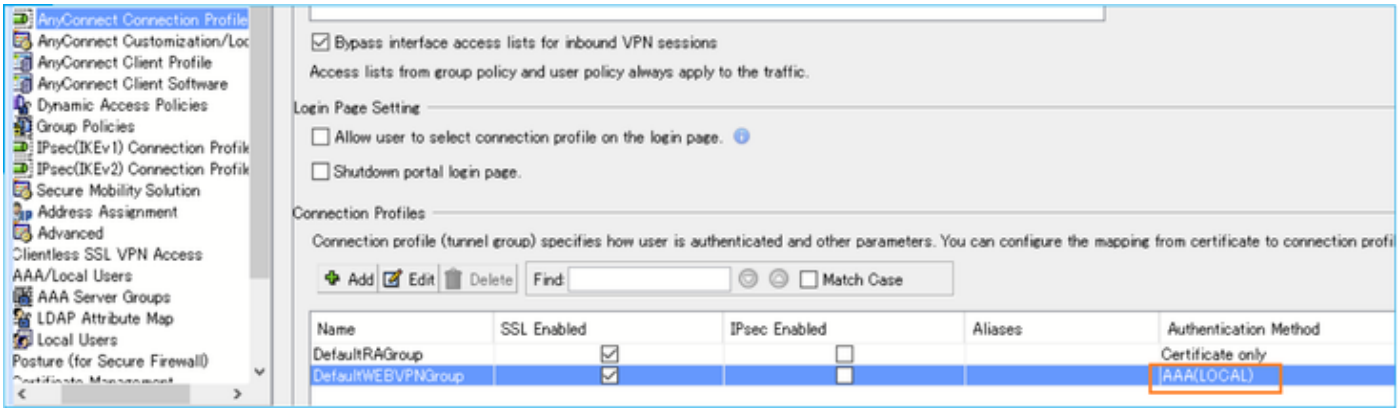
Specifically, the CLI has:

<#root>

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

```
 authentication aaa certificate
```

While the ASDM UI does not mention the certificate method:



Troubleshoot – Recommended Steps

This is a cosmetic issue. The method is not showing up in ASDM, but certificate authentication is used.

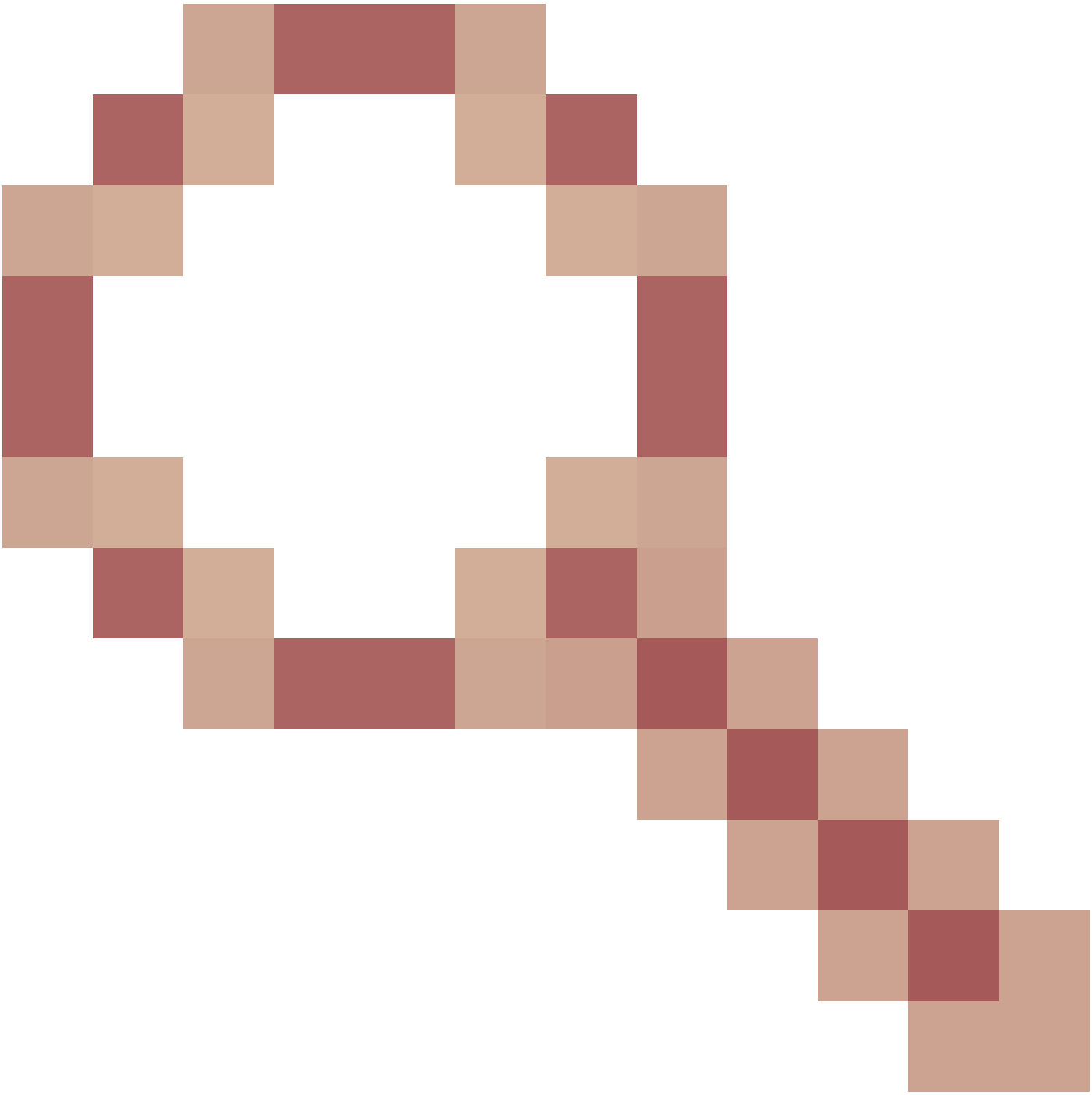
Problem 9. ASDM Session does not Time Out

The symptom is that ASDM GUI session timeout is not taken into account.

Troubleshoot – Recommended Steps

This occurs when the command "**aaa authentication http console LOCAL**" is not set on the managed ASA.

Refer to the Cisco Bug id CSCwj70826



ENH: add a warning: setting session timeout, requires "aaa authentication http console LOCAL"

Workaround

Configure the command ""aaa authentication http console LOCAL" on the managed ASA.

Problem 10. ASDM LDAP authentication fails

Troubleshoot – Recommended Steps

Step 1

Ensure that the configuration is in place, for example:

<#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

Step 2

Check the LDAP server status:

<#root>

asa#

show aaa-server

Good scenario:

<#root>

Server status:

ACTIVE

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

Bad scenario:

<#root>

Server status:

FAILED

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

Step 3

Check the LOCAL authentication works properly by temporarily disabling the LDAP authentication.

Step 4

On ASA run LDAP debugs and try to authenticate the user:

<#root>

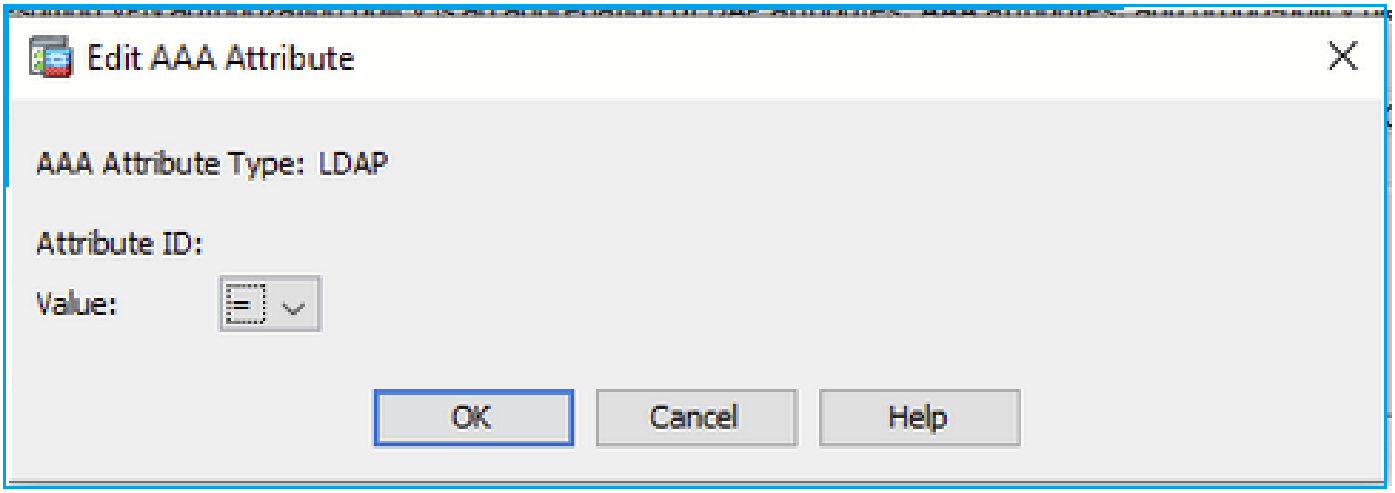
#

debug ldap 255

In the debugs look for lines that contain hints like "Failed".

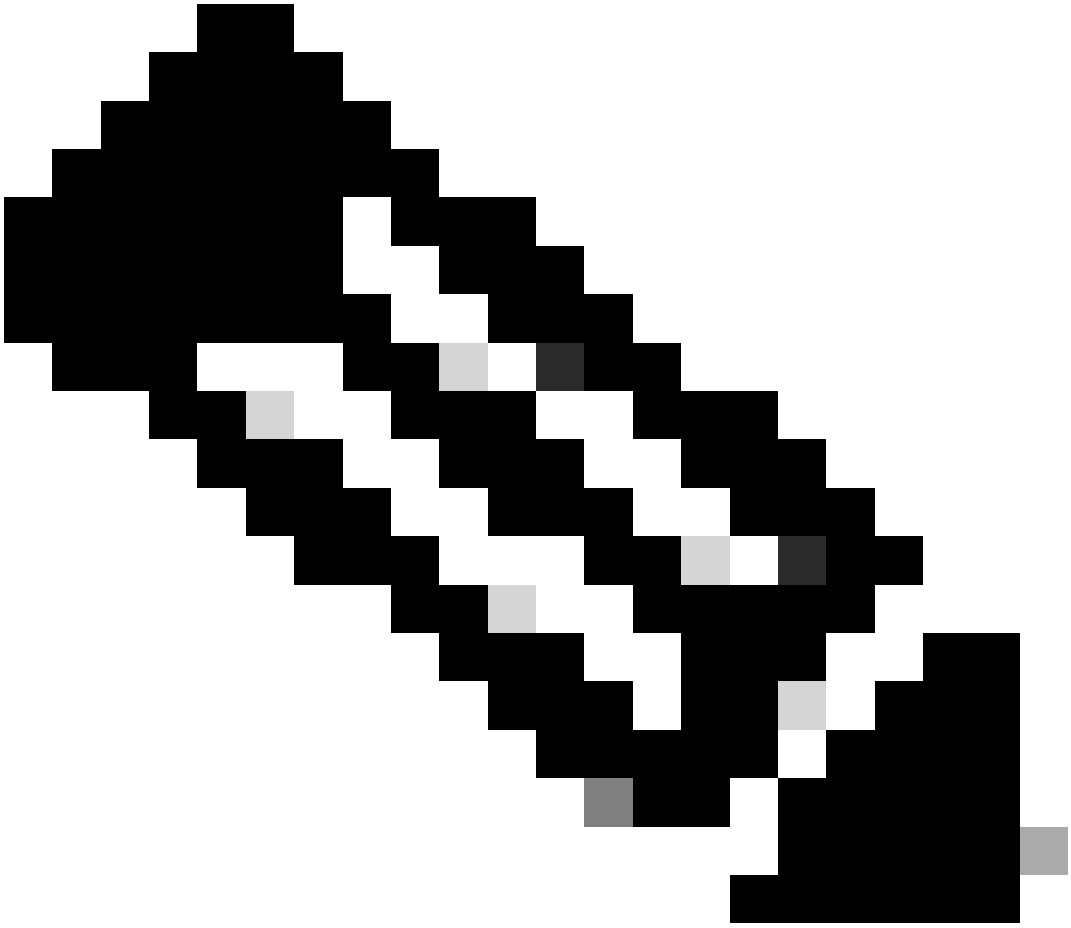
Problem 11. ASDM Webvpn DAP config is missing

Under DAP configuration on ASDM AAA Attributes type (Radius/LDAP) are not visible only seeing = and != on dropdown:



Troubleshoot – Recommended Steps

This is a software defect tracked by Cisco Bug id CSCwa99370
ASDM:DAP config missing AAA Attributes type (Radius/LDAP)

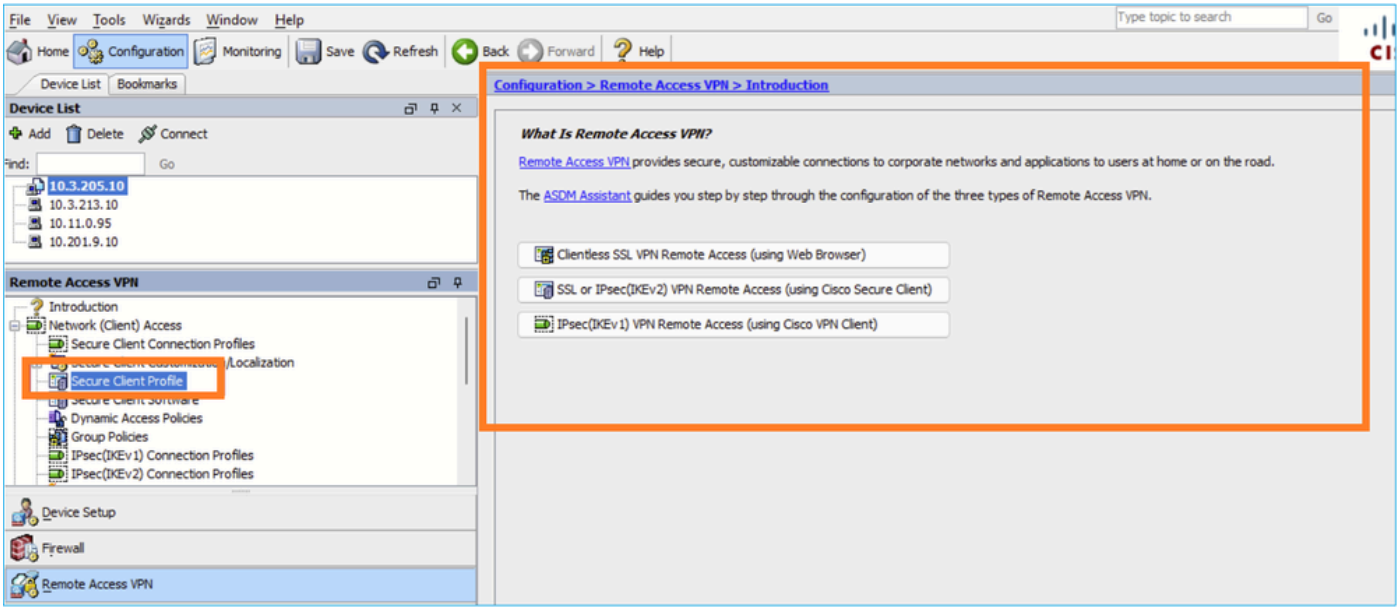


Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

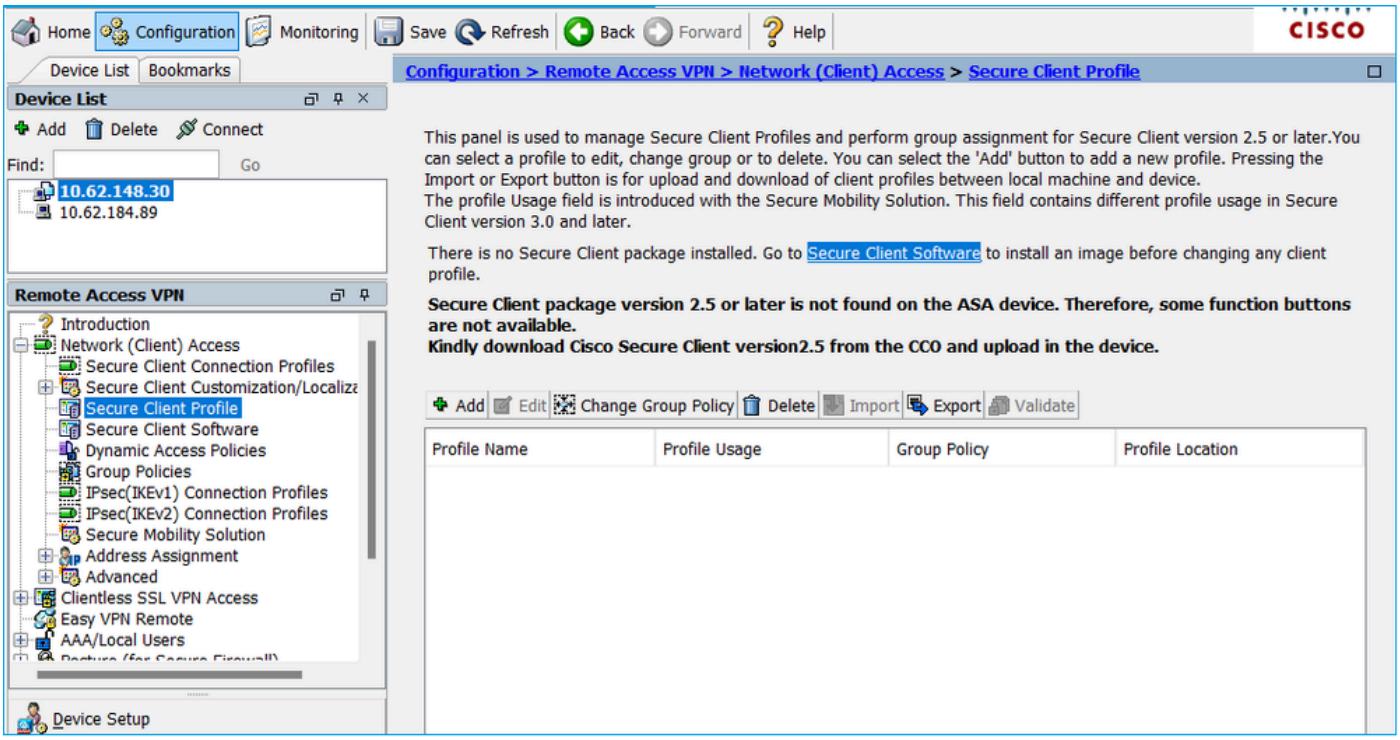
Troubleshoot ASDM Other Problems

Problem 1. Unable to access Secure Client Profile on ASDM

The ASDM UI shows this:



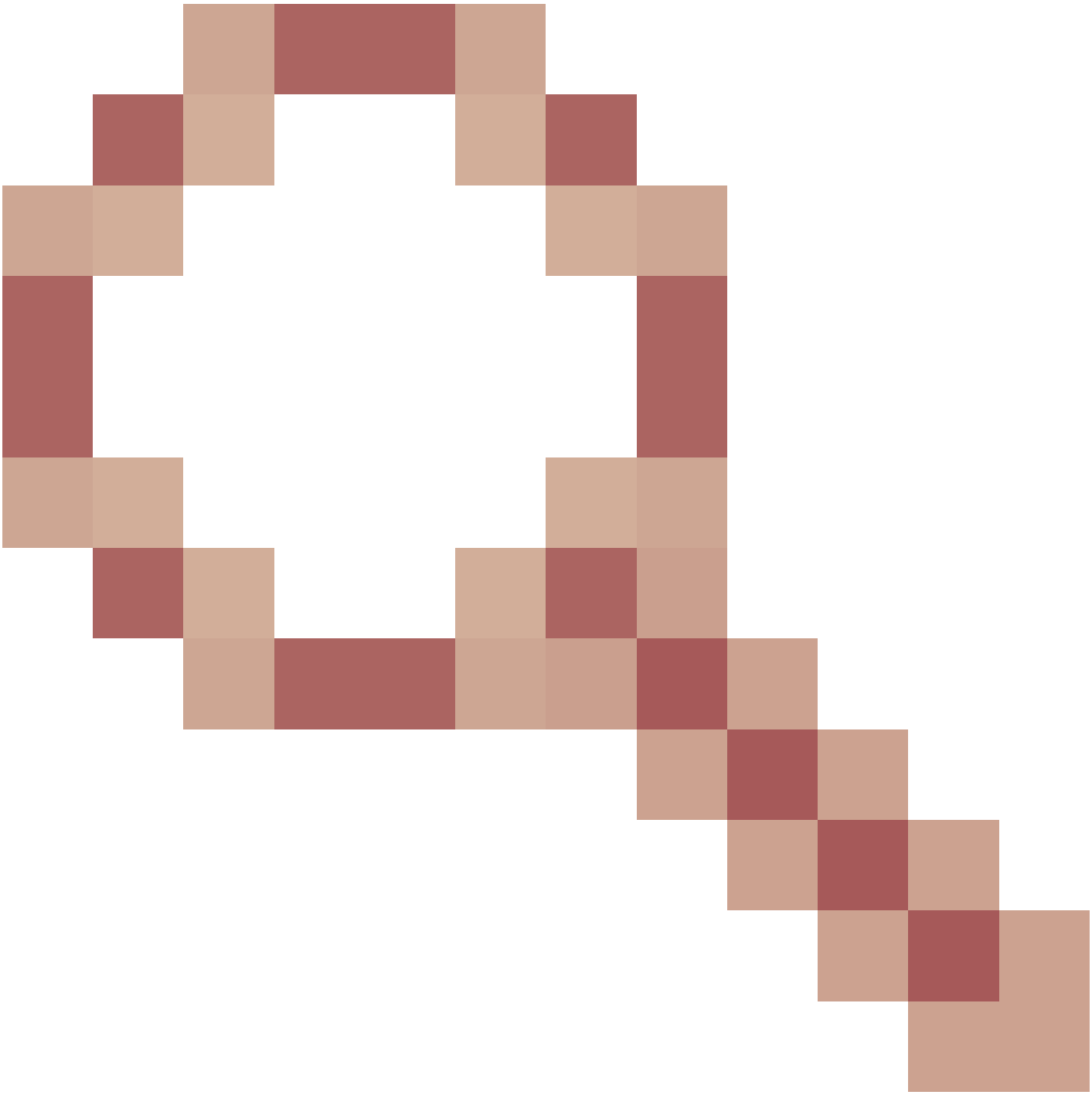
While the expected UI output is:



Troubleshoot – Recommended Steps

This is a known defect:

Cisco Bug id CSCwi56155



Unable to access Secure Client Profile on ASDM

Workarounds:

Downgrade AnyConnect

or

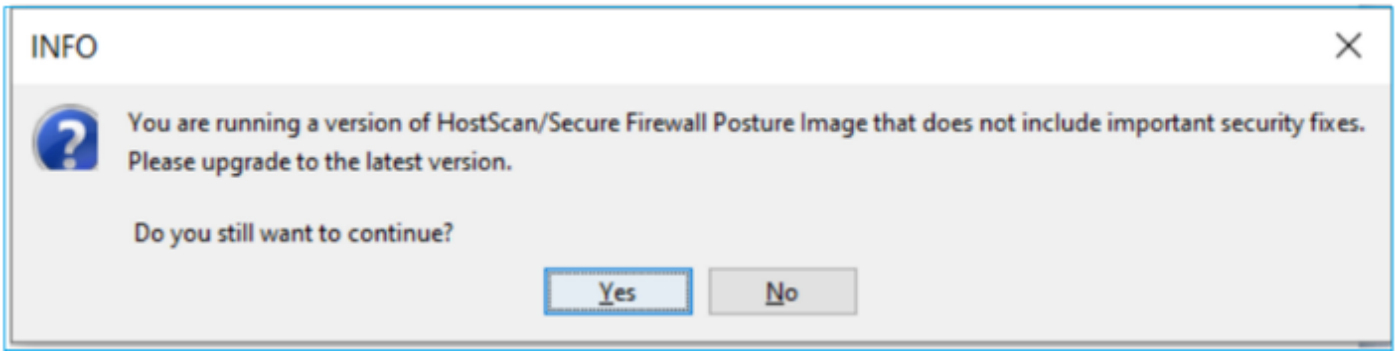
Upgrade ASDM to version 7.20.2

Check the defect notes for more details. Additionally, you can subscribe to the defect, so you receive a notification on defect updates.

Problem 2. ASDM shows pop up for hostscan - image does not include important security fixes

The ASDM UI shows:

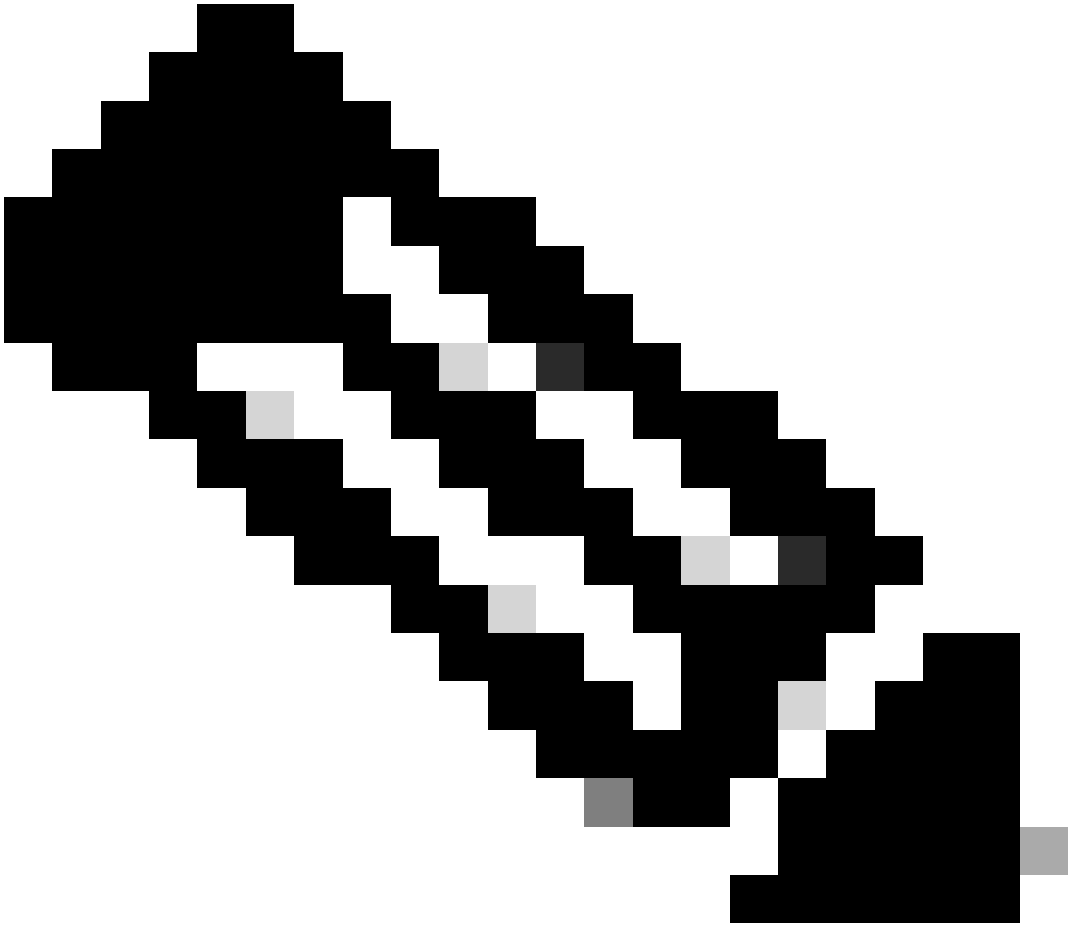
"You are running a version of HostScan/SecureFirewall Posture image that does not include important security fixes. Please upgrade to the latest version. Do you still want to continue?"



Troubleshoot – Recommended Steps

This is a known defect:

Cisco Bug id CSCwc62461
When logging into ASDM pop up for hostscan - image does not include important security fixes



Note: This defect has been fixed in recent ASDM software releases. Check the defect details for more information.

Workaround:

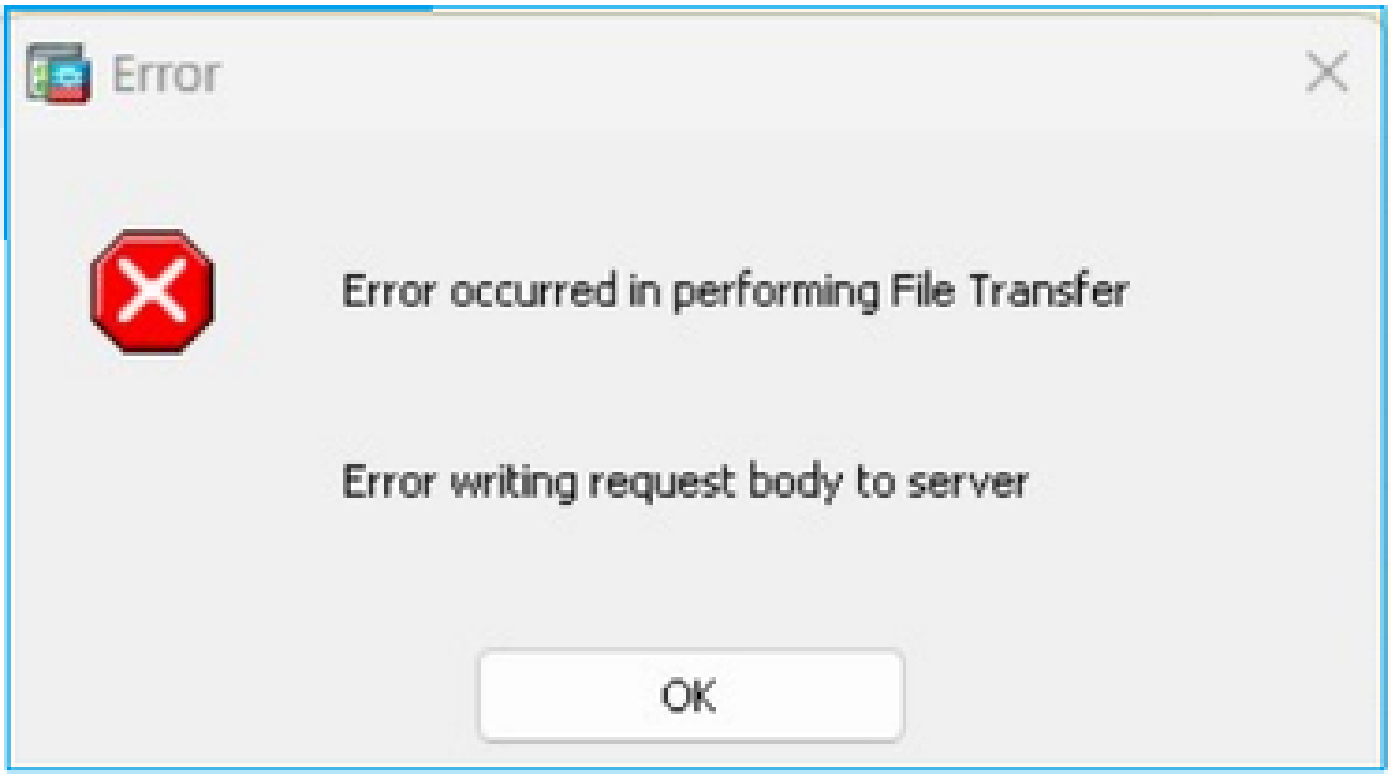
Click 'Yes' on the pop up message box to continue.

Problem 3. ASDM "Error writing request body to server" when copying an image over ASDM

The ASDM UI shows:

Error occurred in performing File Transfer

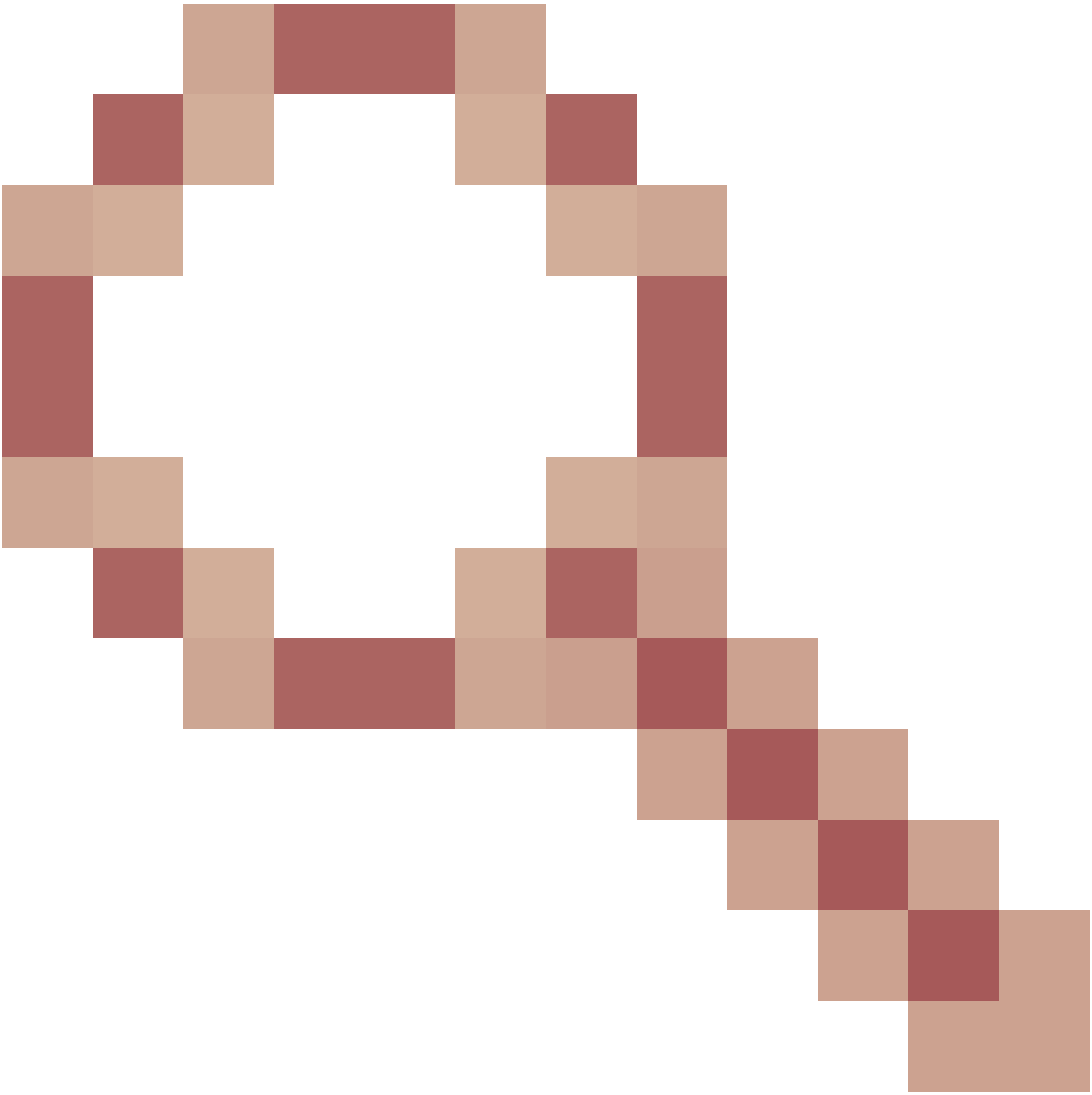
Error writing request body to server



Troubleshoot – Recommended Actions

This is a known defect tracked by:

Cisco Bug id CSCtf74236



ASDM "Error writing request body to server" when copying image

Workaround

Use SCP/TFTP to transfer the file.

References

- ASDM Configuration Guides
- Cisco ASA and ASDM Compatibility per Model