

ASDM 컨피그레이션, 인증 및 기타 문제 해결

목차

[소개](#)

[배경](#)

[ASDM 컨피그레이션 문제 해결](#)

[문제 1. ASDM은 인터페이스에 적용된 ACL\(Access Control List\)을 표시하지 않습니다](#)

[문제 2. ASA CLI와 ASDM UI 간의 히트 수 불일치](#)

[문제 3. "오류: % 'x' 마커에서 잘못된 입력이 감지되었습니다. asdm에서 ACL을 수정할 때 오류 메시지를 표시"](#)

[문제 4. "오류: ACL은 경로 맵과 연결되어 있으며 비활성 상태가 지원되지 않습니다. 대신 특정 경우에 acl" 오류 메시지를 제거하십시오.](#)

[문제 5. 암시적으로 거부된 연결에 대한 ASDM Real-Time Log Viewer의 로그가 없습니다.](#)

[문제 6. 네트워크 개체 또는 개체 그룹을 수정하려고 하면 ASDM이 중지됩니다.](#)

[문제 7. ASDM은 다른 인터페이스에 대한 추가 액세스 제어 목록 규칙을 표시할 수 있습니다](#)

[문제 8. 실시간 로그 뷰어에서 실시간 로그를 사용할 수 없습니다.](#)

[문제 9. 실시간 로그 뷰어의 날짜 및 시간 열이 비어 있습니다. 문제 해결 - 권장 작업](#)

[문제 10. 다중 컨텍스트 ASA에서 다른 컨텍스트로 전환한 후 ASDM에 로그인할 수 없습니다](#)

*

[문제 11. 다른 컨텍스트 간에 전환할 때 ASDM 세션이 갑자기 종료되었습니다.](#)

[문제 12. ASDM이 임의로 종료/종료됩니다. 메시지: "ASDM이 연결을 끊기 위해 ASA 디바이스에서 메시지를 받았습니다. 이제 ASDM이 종료됩니다."](#)

[문제 13. ASDM 로드가 "Authentication Domain login\(인증 Firepower 로그인\)" 메시지와 함께 중단됩니다.](#)

[문제 14. ASDM에 Firepower 모듈 관리/구성이 표시되지 않습니다](#)

[문제 15. ASDM에서 보안 클라이언트 프로파일에 액세스할 수 없습니다.](#)

[문제 16. ASDM에서 보안 클라이언트 프로파일 XML 프로파일을 편집할 수 없습니다.](#)

[문제 17. 컨피그레이션 변경 후 보안 클라이언트 이미지가 없습니다.](#)

[문제 18. 비효율적인 http server session-timeout 및 http server idle-timeout 명령](#)

[문제 19. ASDM에서 Dap.xml 복사 실패](#)

[문제 20. ASDM에 IKE 정책 및 IPSEC 제안서가 표시되지 않음](#)

[문제 21. ASDM에 "The enable password is not set. 지금 설정하십시오."](#)

[문제 22. ASDM UI를 새로 고침 후 ASDN 개체가 사라집니다.](#)

[문제 23. 4.5 이전 버전의 AnyConnect 클라이언트 프로파일을 편집할 수 없습니다.](#)

[문제 24. Edit Service Policy\(서비스 정책 수정\) > Rule Actions\(규칙 작업\) > ASA Firepower Inspection\(ASA 검사\) 탭으로 이동할 수 없습니다.](#)

[문제 25. ASDM의 AnyConnect 이미지 버전 5.1 및 AnyConnect 프로파일 편집기](#)

[문제 26. AAA 특성 유형\(Radius/LDAP\)이 ASDM에 표시되지 않습니다.](#)

[문제 27. ASDM에 'Post Quantum key cannot be empty' 오류가 표시됩니다.](#)

[문제 28. ASDM은 "where used" 옵션을 사용할 때 어떤 결과도 표시하지 않습니다.](#)

[문제 29. 네트워크 개체를 삭제할 때 "\[네트워크 개체\]는 다음에 사용되므로 삭제할 수 없습니다." 경고 메시지가 표시됩니다](#)

[문제 30. ASDM의 Network Objects/Group\(네트워크 개체/그룹\) 탭의 사용성 문제](#)

[ASDM 인증 문제 해결](#)

[문제 1. ASDM 로그인 실패](#)

[문제 2. ASDM 명령 권한 부여에 실패했습니다.](#)

[문제 3. ASDM 읽기 전용 액세스 구성](#)

[문제 4. ASDM MFA\(Multi-Factor Authentication\)](#)

[문제 5. ASDM 외부 인증 컨피그레이션](#)

[문제 6. ASDM 로컬 인증에 실패했습니다.](#)

[문제 7. ASDM 일회용 비밀번호](#)

[문제 8. 연결 프로파일에 모든 방법이 표시되지 않음](#)

[문제 9. ASDM 세션이 시간 초과되지 않습니다.](#)

[문제 10. ASDM LDAP 인증에 실패했습니다.](#)

[문제 11. ASDM Webvpn DAP 구성이 없습니다.](#)

ASDM 기타 문제 해결

[문제 1. ASDM에서 보안 클라이언트 프로파일에 액세스할 수 없습니다.](#)

[문제 2. ASDM에서 hostscan 팝업을 표시합니다. 이미지에 중요한 보안 수정 사항이 포함되어 있지 않습니다.](#)

[문제 3. ASDM을 통해 이미지를 복사할 때 ASDM "서버에 요청 본문을 쓰는 중 오류"](#)

소개

이 문서에서는 ASDM(Adaptive Security Appliance Device Manager) 컨피그레이션, 인증 및 기타 문제에 대한 트러블슈팅 프로세스에 대해 설명합니다.

배경

이 문서는 다음 문서와 함께 ASDM 문제 해결 시리즈의 일부입니다.

[링크1<>](#)

[링크2<>](#)

[링크3<>](#)

ASDM 컨피그레이션 문제 해결

문제 1. ASDM은 인터페이스에 적용된 ACL(Access Control List)을 표시하지 않습니다

ASDM은 해당 인터페이스에 적용된 유효한 access-group이 있더라도 인터페이스에 적용된 ACL(Access Control List)을 표시하지 않습니다. 대신 메시지는 "0 incoming rules"입니다. 인터페이스에 대한 액세스 그룹 컨피그레이션에 구성된 L3 및 L2 ACL에서 다음 증상이 관찰됩니다.

<#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)#
```

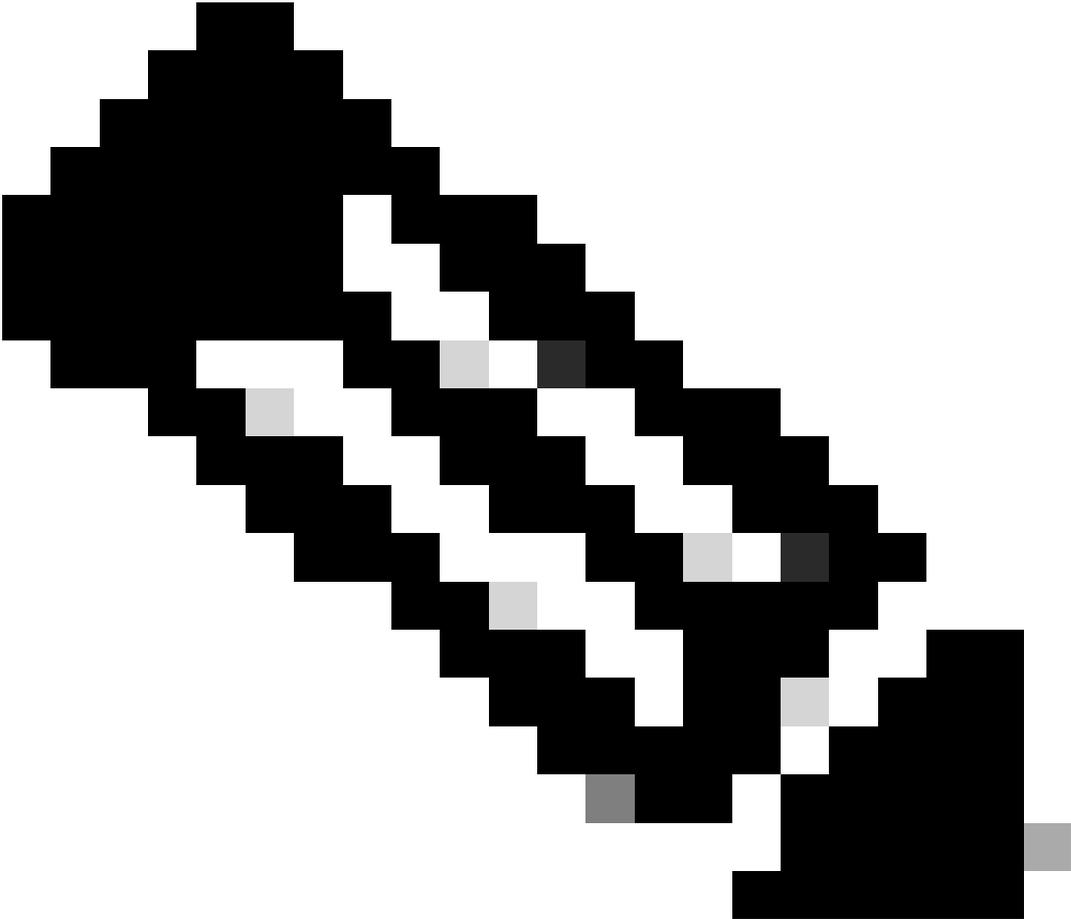
```
access-group 1 in interface inside
```

```
firewall(config)#
```

```
access-group 2 in interface outside
```

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwj14147 "L2 및 L3 acl이 혼합된 경우 ASDM에서 access-group config를 로드하지 못합니다."를 참조하십시오.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 2. ASA CLI와 ASDM UI 간의 히트 수 불일치

ASDM의 적중 횟수 항목은 방화벽 출력에서 `show access-list` 명령에 의해 보고된 `access-list` 적중 횟수와 일치하지 않습니다.

문제 해결 - 권장 조치

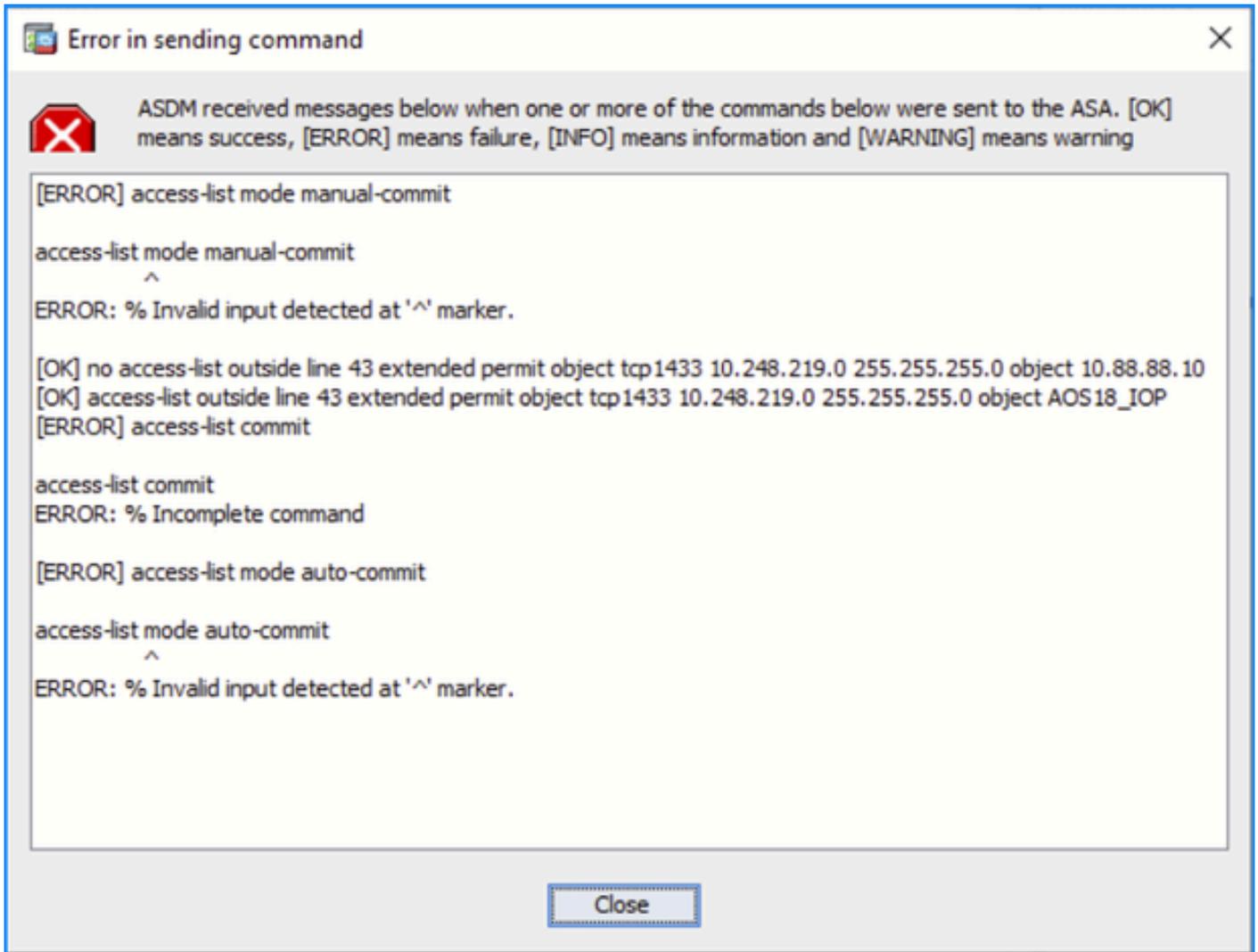
소프트웨어 Cisco 버그 ID CSCtq38377 "[ENH](#): ASDM은 ASA에서 ACL 해시 계산을 사용하고 로컬로 계산하지 않아야 함" 및 Cisco 버그 ID CSCtq38405 "ENH: ASA에는 ASD에 ACL 해시 정보를 제공하는 메커니즘이 필요합니다."

문제 3. "오류: % ' ' 마커에서 잘못된 입력이 감지되었습니다. asdm에서 ACL을 수정

할 때 오류 메시지 표시

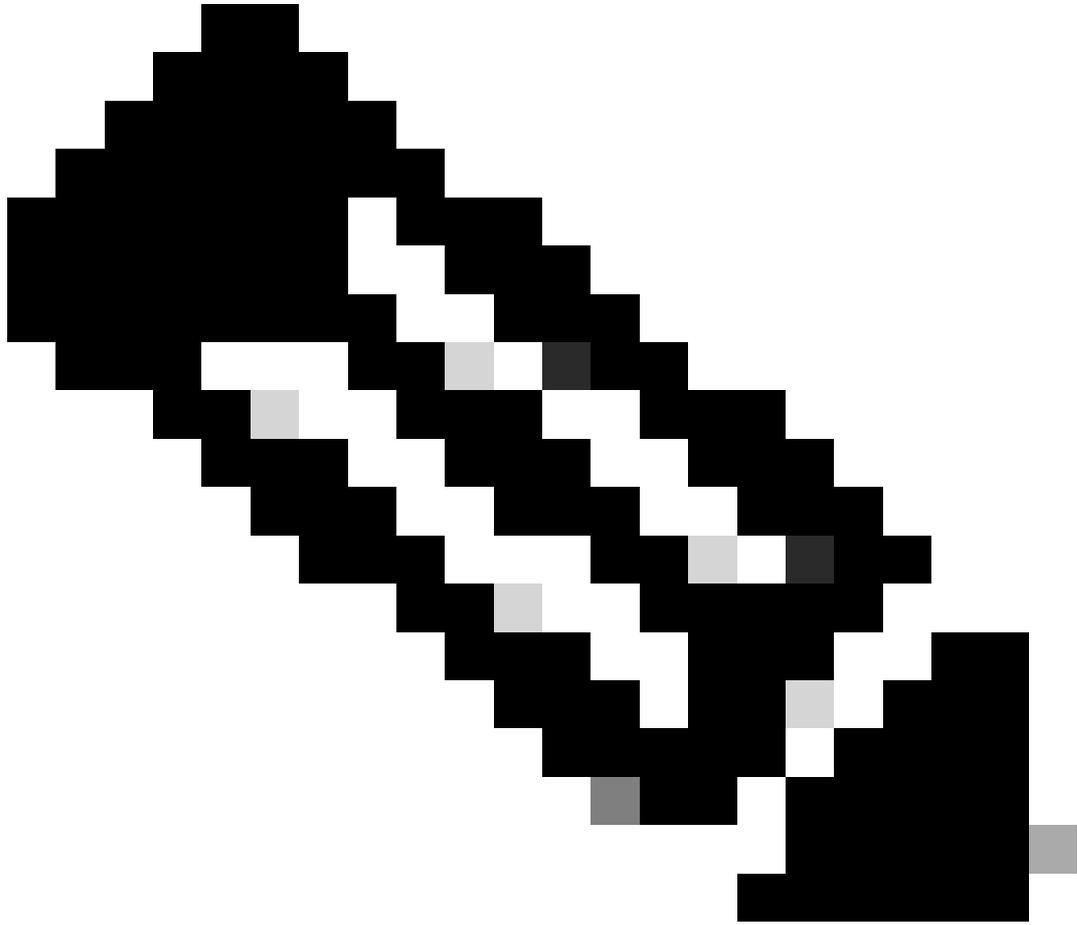
"오류: % '^' 마커에서 잘못된 입력이 감지되었습니다. asdm에서 ACL을 수정할 때 오류 메시지가 표시됩니다.

```
[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.
```



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCvq05064 "Edit an entry (ACL) from ASDM gives a error."



참고: 이러한 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

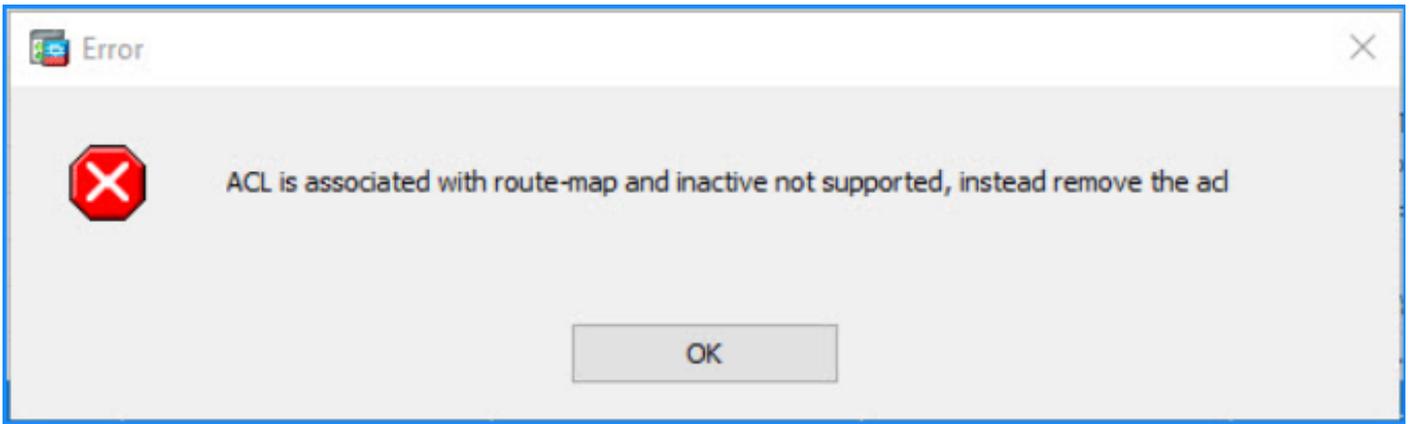
문제 4. "오류: ACL은 경로 맵과 연결되어 있으며 비활성 상태가 지원되지 않습니다. 대신 특정 경우에 acl" 오류 메시지를 제거하십시오.

"오류: ACL은 경로 맵과 연결되어 있으며 비활성 상태가 지원되지 않습니다. 대신 다음 경우 중 하나에 표시된 acl 제거" 오류 메시지가 표시됩니다.

1. 정책 기반 라우팅 컨피그레이션에 사용되는 ASDM에서 ACL을 수정합니다.

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

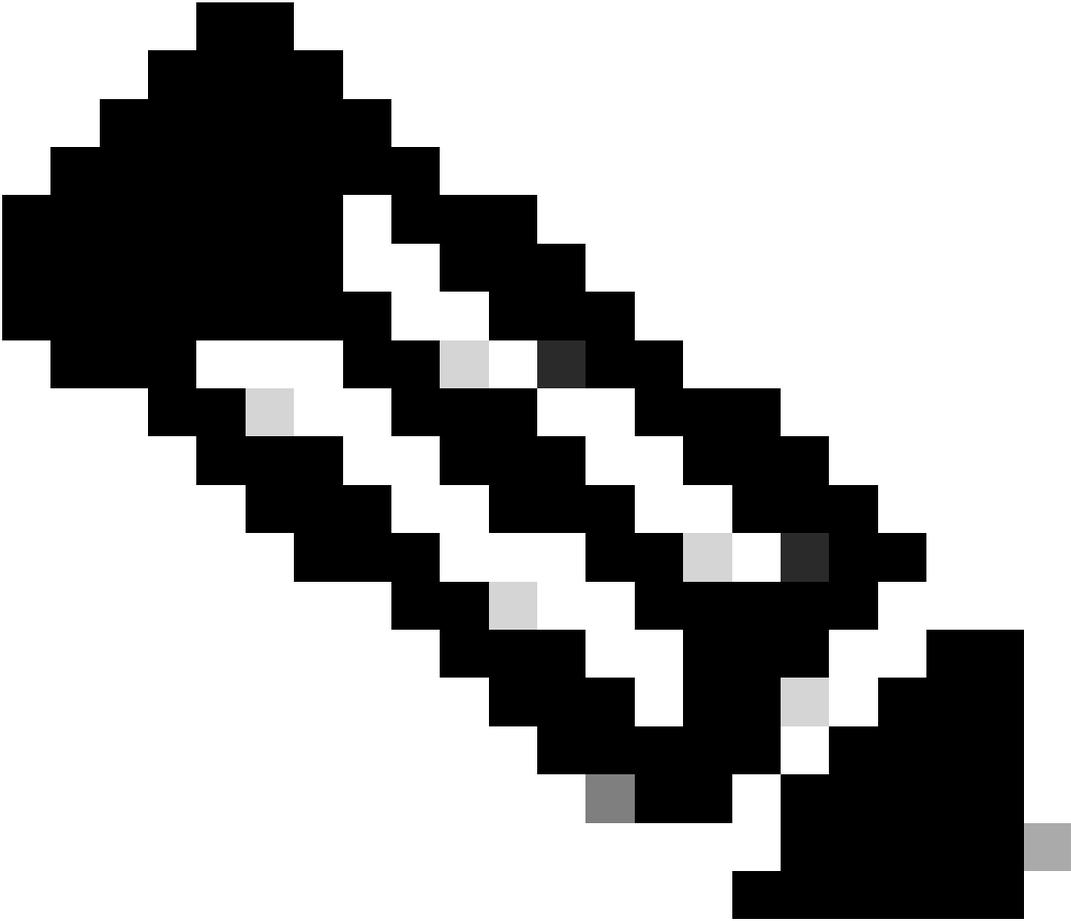
오류: ACL이 경로 맵과 연결되어 있고 비활성 상태이면 지원되지 않습니다. 대신 acl을 제거하십시오



2. ACL ASDM > Configuration -> Remote Access VPN -> Network (Client) Access(네트워크(클라이언트) 액세스) > Dynamic Access(동적 액세스) 정책을 수정합니다.

문제 해결 - 권장 조치

1. 소프트웨어 Cisco 버그 ID CSCwb57615 "Configuring pbr access-list with line number failed."을 참조하십시오. 해결 방법은 "line" 매개변수를 컨피그레이션에서 제외하는 것입니다.
2. 소프트웨어 Cisco 버그 ID CSCwe34665 "Unable to Edit the ACL objects if it is already in use, getting exception"(ACL 객체가 이미 사용 중인 경우 수정할 수 없음, 예외 가져오기)을 참조하십시오.



참고: 이러한 결함은 최근 ASA 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 5. 암시적으로 거부된 연결에 대한 ASDM Real-Time Log Viewer의 로그가 없습니다.

ASDM Real-Time Log Viewer는 암시적으로 거부된 연결에 대한 로그를 표시하지 않습니다.

문제 해결 - 권장 조치

access-list의 끝에 있는 암시적 거부는 syslog를 생성하지 않습니다. 거부된 모든 트래픽이 syslog를 생성하도록 하려면 ACL의 끝에 log 키워드와 함께 규칙을 추가합니다.

문제 6. 네트워크 개체 또는 개체 그룹을 수정하려고 하면 ASDM이 중지됩니다.

ASDM은 Addresses(주소) 탭의 Configuration(컨피그레이션) > Firewall(방화벽) > Access Rules(액세스 규칙) 페이지에서 네트워크 개체 또는 개체 그룹을 수정하려고 시도할 때 고정됩니다. 이 문제가 발생하면 사용자는 네트워크 개체 창의 매개변수를 수정할 수 없습니다.

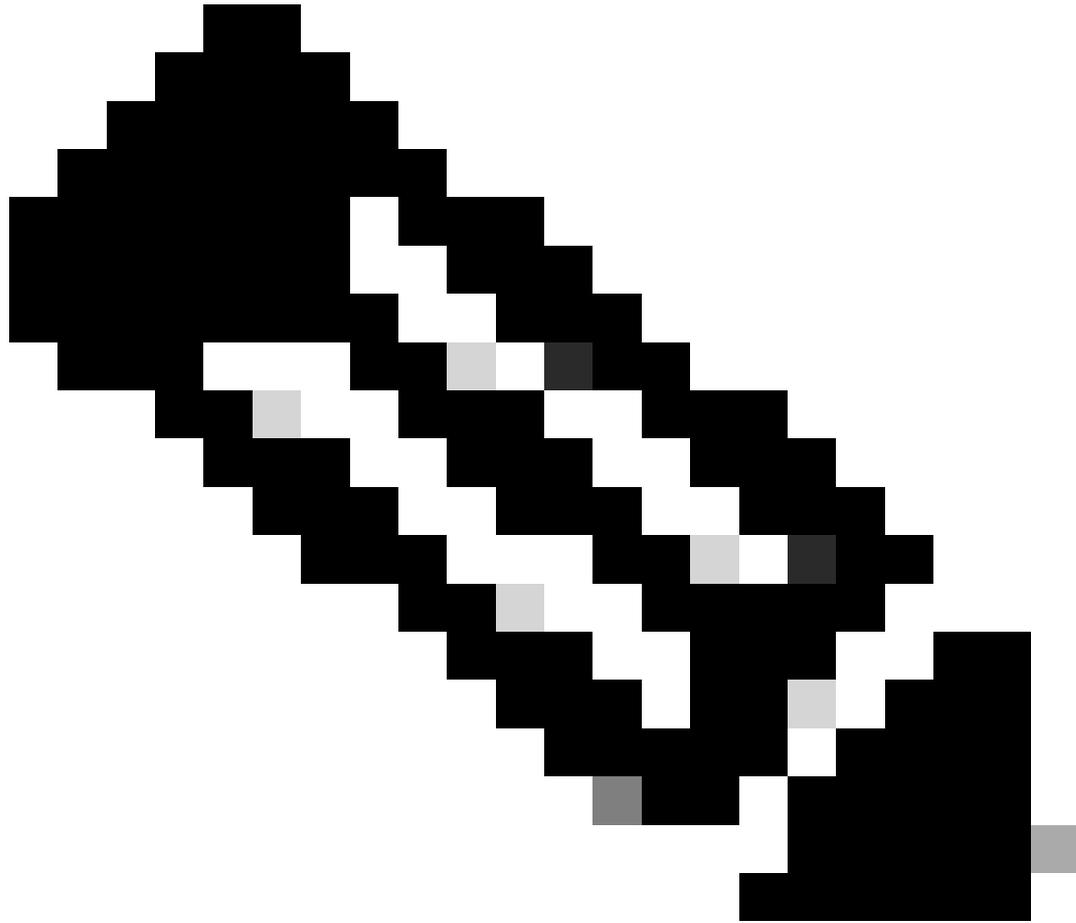
문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwj12250 "ASDM은 네트워크 개체 또는 네트워크 개체 그룹을 편집할 때 고정됩니다."를 참조하십시오. 해결 방법은 topN 호스트 통계 수집을 비활성화하는 것입니다

```
<#root>
```

```
ASA(config)#
```

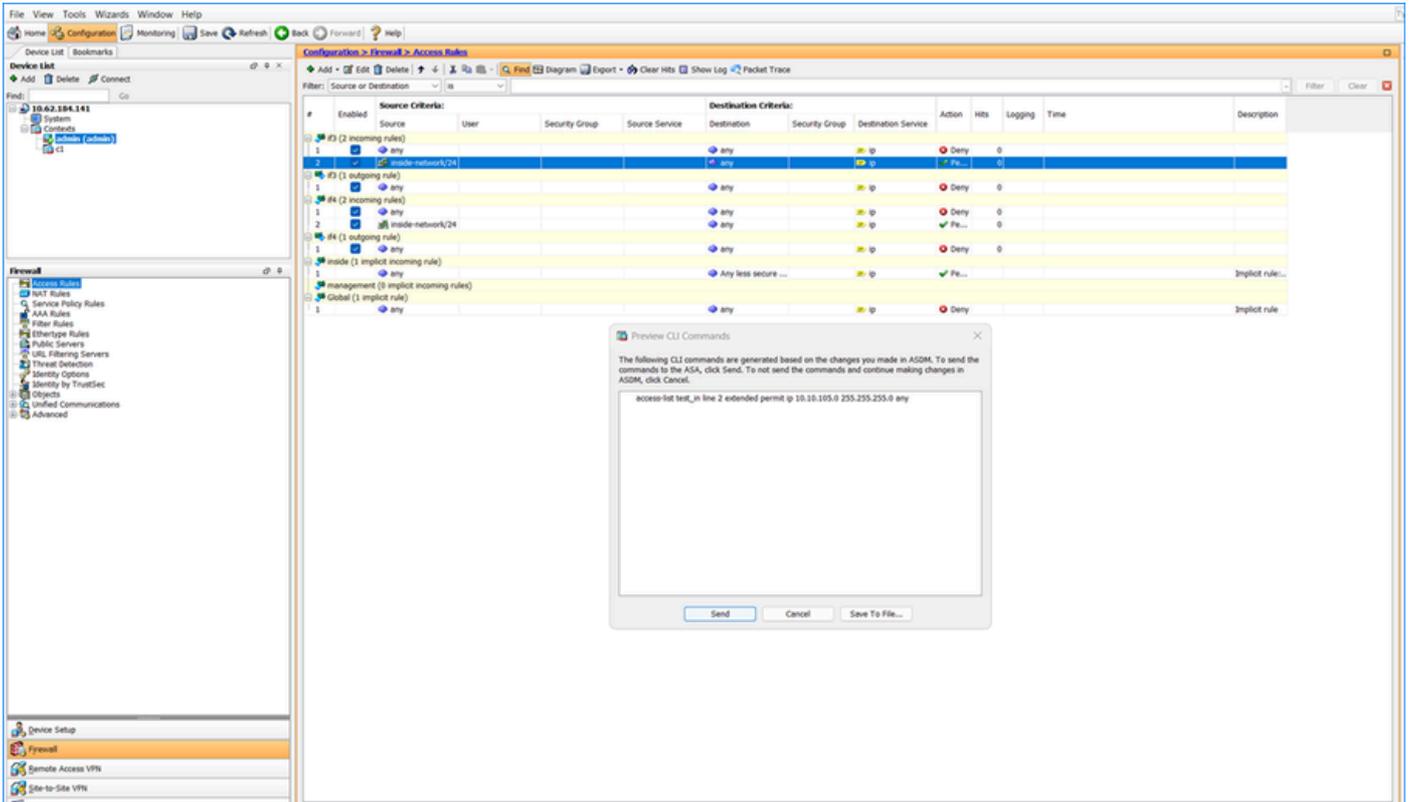
```
no hpm topN enable
```



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 7. ASDM은 다른 인터페이스에 대한 추가 액세스 제어 목록 규칙을 표시할 수 없습니다

ASDM은 인터페이스 레벨 액세스 제어 목록이 수정된 경우 여러 인터페이스에 대한 추가 액세스 제어 목록 규칙을 표시할 수 있습니다. 이 예에서는 인터페이스 if3 ACL에 수신 규칙#2가 추가되었습니다. ASDM에서는 #2 if4 인터페이스에 대한 컨피그레이션도 보여주지만, 이 규칙은 사용자가 구성하지 않았습니다. 명령 미리 보기에는 보류 중인 단일 변경 내용이 올바르게 표시됩니다. 이는 사용자 인터페이스 표시 문제입니다.



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwm71434 "ASDM에서 중복 인터페이스 액세스 목록 항목을 표시할 수 있습니다"를 참조하십시오.

문제 8. 실시간 로그 뷰어에서 실시간 로그를 사용할 수 없습니다.

실시간 로그 뷰어에 로그가 표시되지 않음

문제 해결 - 권장 조치

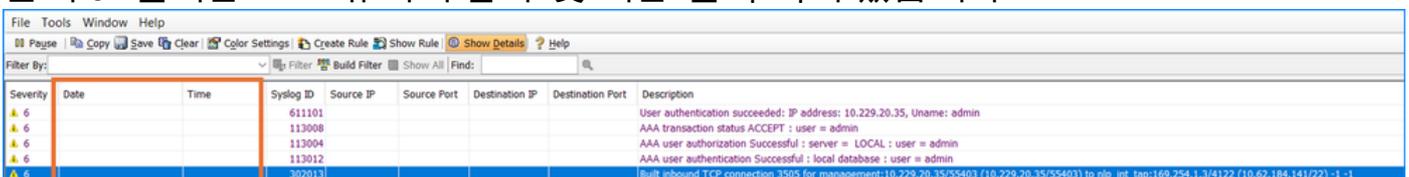
1. 로깅이 구성되었는지 확인합니다. ASDM [Book 1](#)을 [참조하십시오](#). [Cisco ASA Series General Operations ASDM 컨피그레이션 가이드, 7.22, 장: 로깅](#).
2. 소프트웨어 Cisco 버그 ID CSCvf82966 "[ASDM](#) - Logging: Unable to View Real-Time logs(실시간 로그를 볼 수 없음)".

참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

참조

- [ASDM 책 1: Cisco ASA Series General Operations ASDM 컨피그레이션 가이드, 7.22, 장: 로깅.](#)

문제 9. 실시간 로그 뷰어의 날짜 및 시간 열이 비어 있습니다.



The screenshot shows the ASDM log viewer interface. The table below has columns for Severity, Date, Time, Syslog ID, Source IP, Source Port, Destination IP, Destination Port, and Description. The Date and Time columns are empty for all rows, which is the issue being reported.

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6			611101					User authentication succeeded: IP address: 10.229.20.35, Username: admin
6			113008					AAA transaction status ACCEPT : user = admin
6			113004					AAA user authentication Successful : server = LOCAL : user = admin
6			113012					AAA user authentication Successful : local database : user = admin
6			302013					Built inbound TCP connection 3505 for management:10.229.20.35/55403 (10.229.20.35/55403) to rlp_int:169.254.1.3/4122 (10.62.184.141/22)-1-1

문제 해결 - 권장 조치

1. RFC5424 로깅 타임스탬프 형식이 사용되는지 확인:

```
<#root>
```

```
#
```

```
show run logging
```

```
logging enable
```

```
logging timestamp rfc5424
```

2. RFC5424 로깅 타임스탬프 형식을 사용하는 경우 소프트웨어 Cisco 버그 ID [CSCvs52212](#) "ASDM ENH: 이벤트 로그 뷰어가 rfc5424 타임스탬프 형식의 ASA syslog를 표시하는 기능" 해결 방법은 RFC5424 형식을 사용하지 않는 것입니다.

```
<#root>
```

```
firewall(config)#
```

```
no logging timestamp rfc5424
```

```
firewall(config)#
```

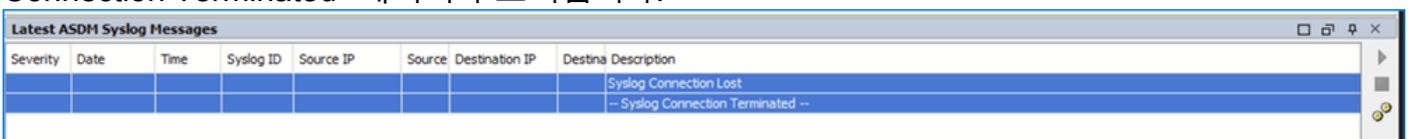
```
logging timestamp
```

3. 또한 소프트웨어 결함 Cisco 버그 ID [CSCwh70323](#) "일부 syslog 메시지가 syslog 서버로 전송 되기 위해 Timestamp entry missing"을 참조하십시오.

참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 10. 다중 컨텍스트 ASA에서 다른 컨텍스트로 전환한 후 ASDM에 로그인하지 못할 수 있습니다

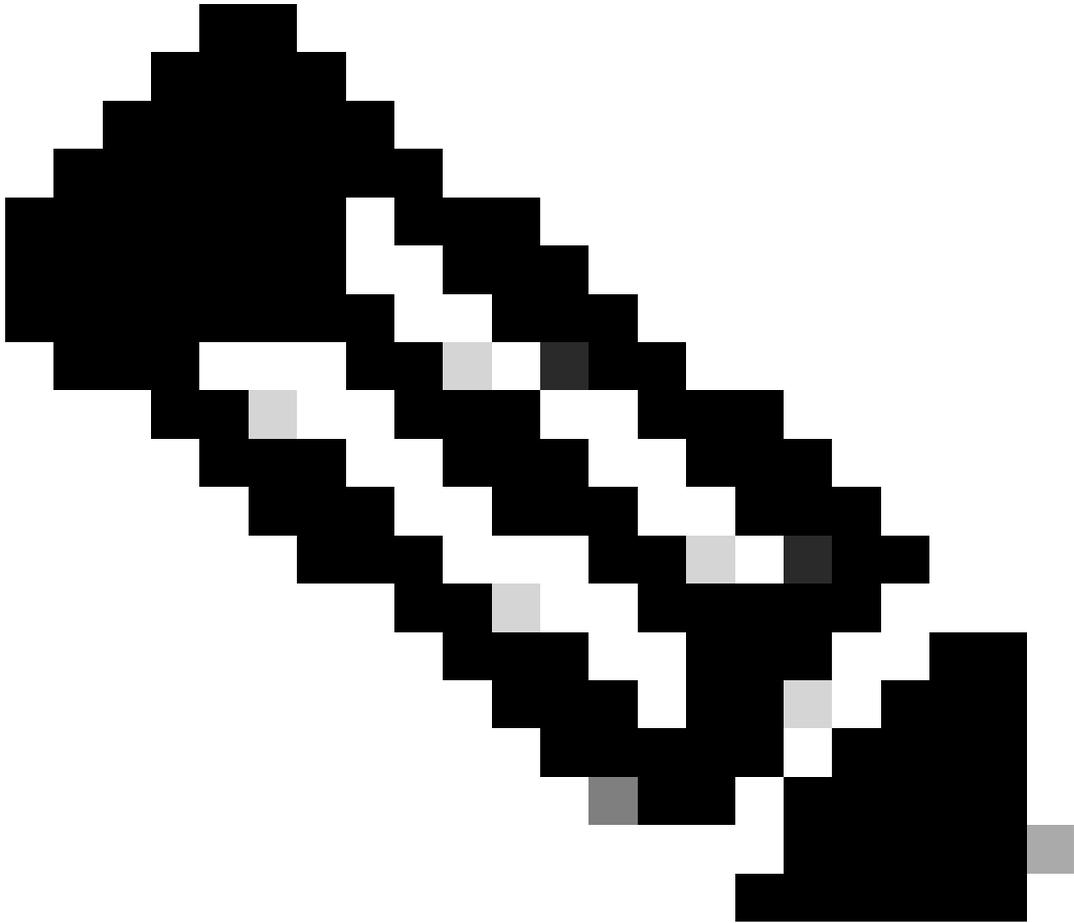
홈 페이지의 Latest ASDM Syslog Messages 탭에는 "Syslog Connection Lost" 및 "Syslog Connection Terminated" 메시지가 표시됩니다.



Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
								Syslog Connection Lost
								-- Syslog Connection Terminated --

문제 해결 - 권장 조치

로깅이 구성되었는지 확인합니다. 소프트웨어 Cisco 버그 ID CSCvz15404 "ASA: 다중 컨텍스트 모드: ASDM 로깅은 다른 컨텍스트로 전환되면 중지됩니다."



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 11. 다른 컨텍스트 간에 전환할 때 ASDM 세션이 갑자기 종료됨

"The maximum number of management sessions for protocol http or user already exists(프로토콜 http 또는 사용자에 대한 최대 관리 세션 수가 이미 존재합니다)"라는 오류 메시지와 함께 다른 컨텍스트 간에 전환할 때 ASDM 세션이 갑자기 종료되었습니다. 나중에 다시 시도하십시오." 이러한 로그는 syslog 메시지에 표시됩니다.

%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

문제 해결 - 권장 조치

1. 현재 ASDM 리소스 사용량이 Limit에 도달했는지 확인합니다. 이 경우 Denied 카운터가 증가합니다.

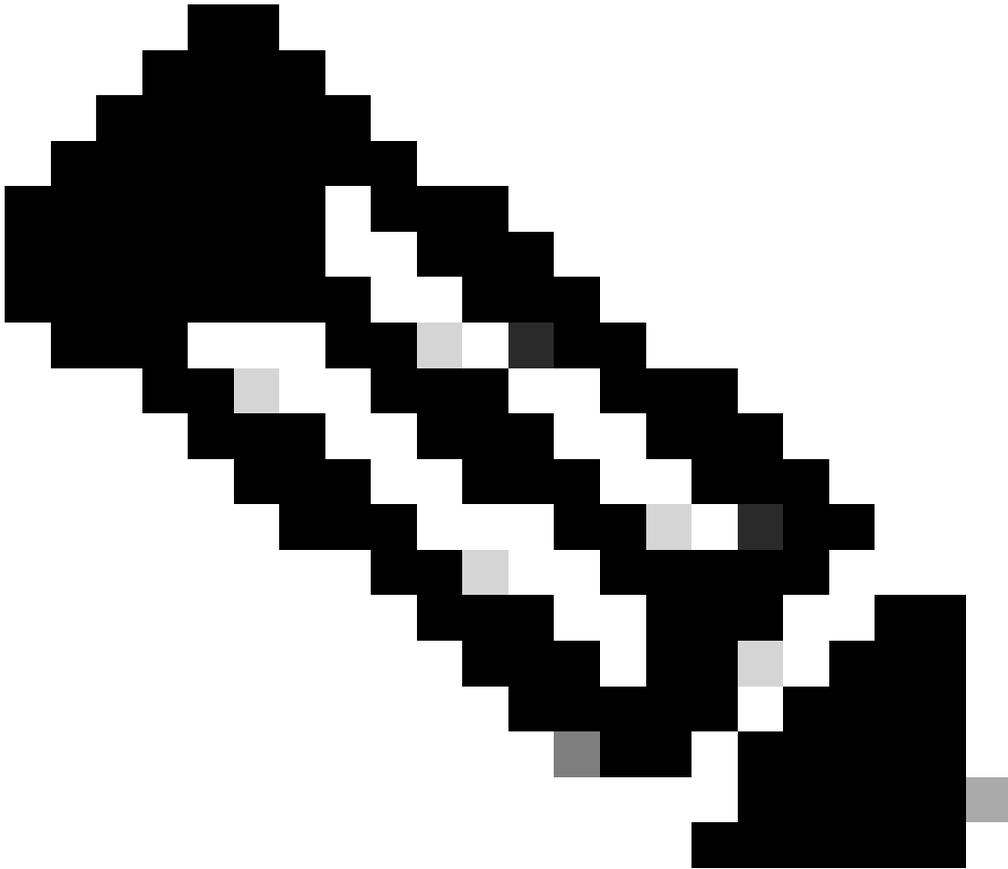
```
<#root>
```

```
firewall #
```

```
show resource usage resource ASDM
```

Resource	Current	Peak	Limit	Denied Context
ASDM				
5				
	5			
5				
10				
admin				

2. 소프트웨어 Cisco 버그 ID CSCvs72378 "[ASDM](#) session being snotween terminated when switching within different contexts"를 참조하십시오.



참고: 이 결함은 최근 ASA 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

3. 소프트웨어 버전에 Cisco 버그 ID CSCvs72378에 대한 수정 사항이 있고 현재 리소스가 한계에 도달한 경우 기존 ASDM 세션 중 일부의 연결을 끊습니다. ASDM을 닫거나 ASDM을 실행하는 호스트의 IP 주소에 대한 HTTPS 연결을 지울 수 있습니다. 이 예에서는 ASDM의 HTTP 서버가 기본 HTTPS 포트 443에서 실행된다고 가정합니다.

```
<#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
```

```
#
```

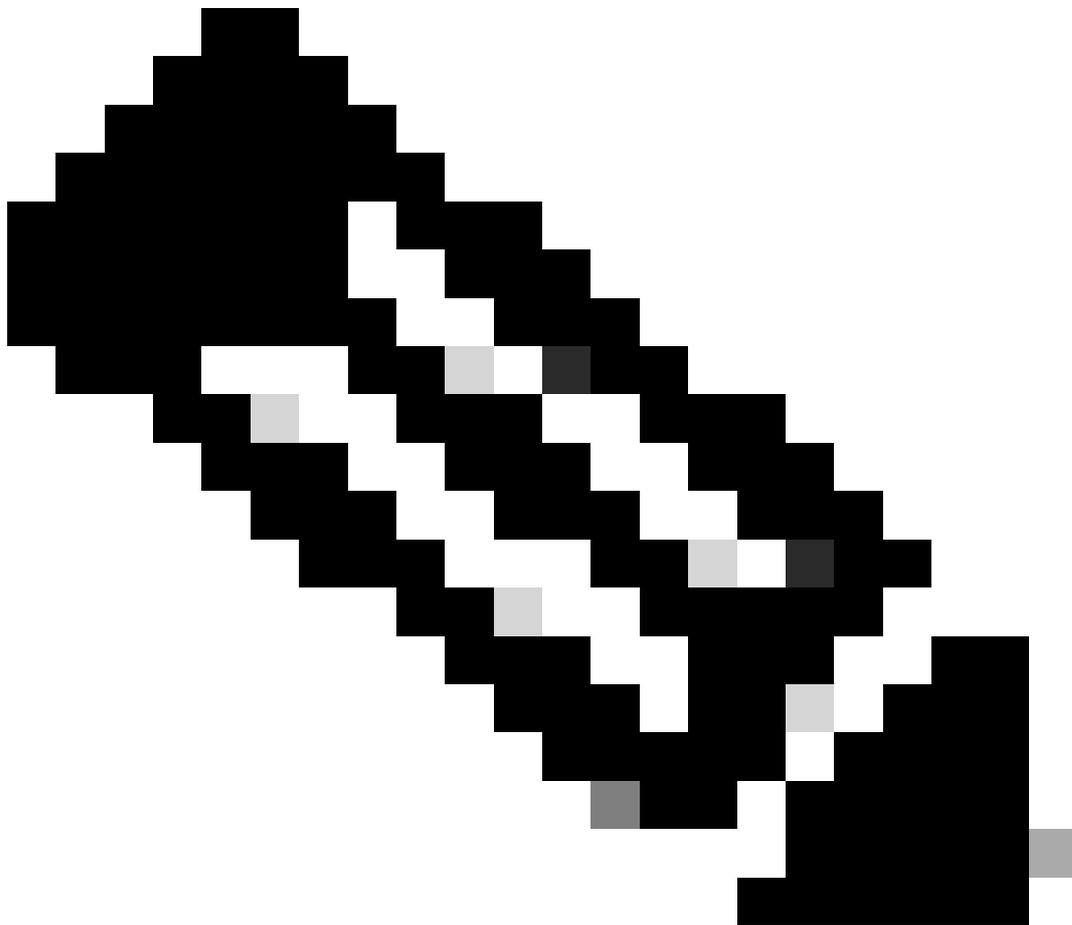
```
clear conn all protocol tcp port 443 address 192.0.2.35
```

문제 12. ASDM이 임의로 종료/종료됩니다. "ASDM이 연결을 끊을 ASA 디바이스에서 메시지를 받았습니다. 이제 ASDM이 종료됩니다."

다중 컨텍스트 ASA에서 ASDM은 "ASDM이 연결을 끊을 ASA 디바이스에서 메시지를 받았습니다. ASDM이 종료됩니다."

문제 해결 - 권장 조치

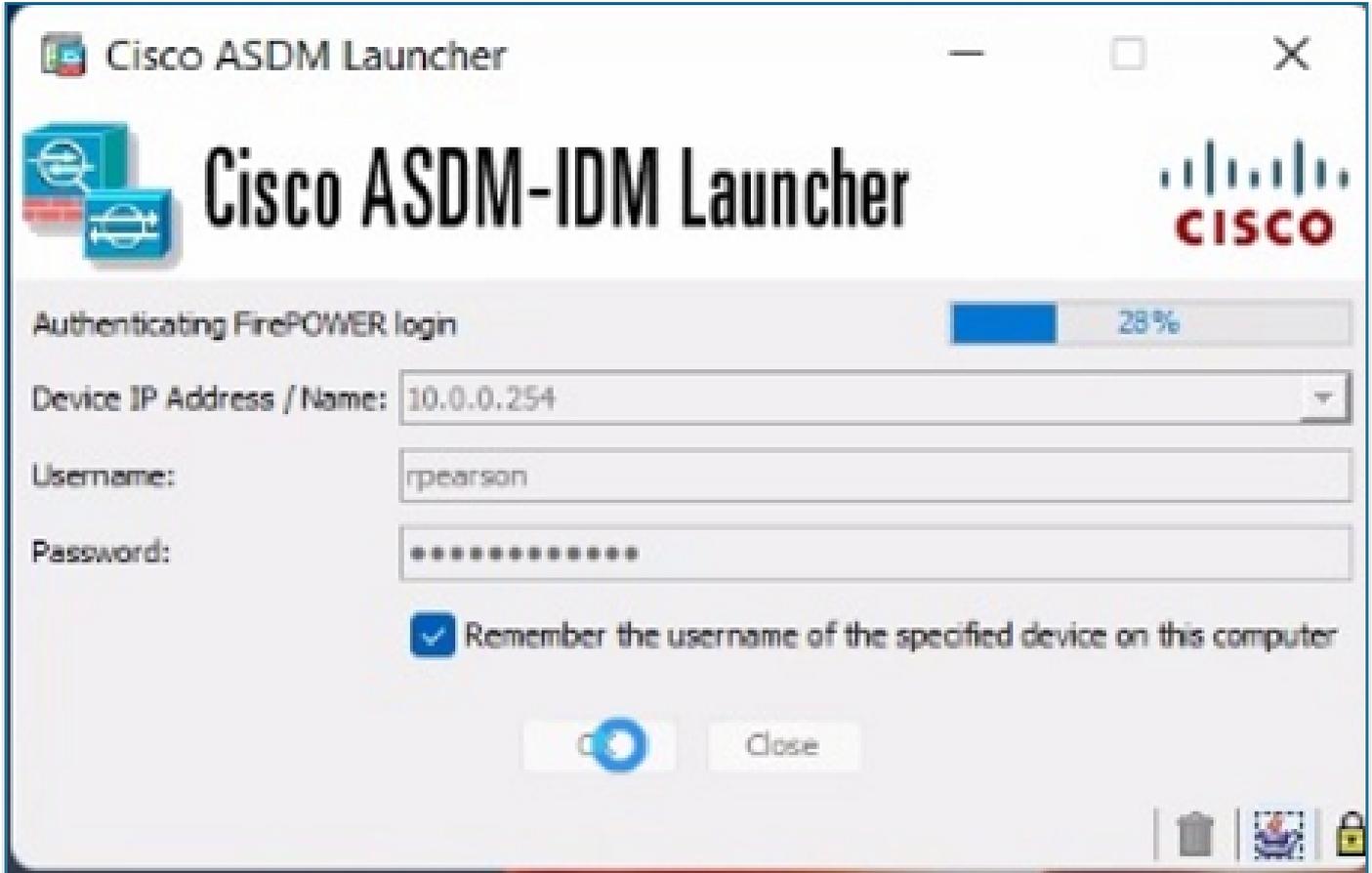
소프트웨어 결함 Cisco 버그 ID [CSCwh04395](#) "ASDM 애플리케이션이 다중 컨텍스트 설정에 대한 알림 메시지로 임의 종료/종료"를 참조하십시오.



참고: 이 결함은 최근 ASA 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 13. "인증 Firepower 로그인" 메시지와 함께 ASDM 로드가 중단됩니다.

ASDM 로드가 "Authentication Domain login(인증 Firepower 로그인)" 메시지와 함께 중단됩니다.



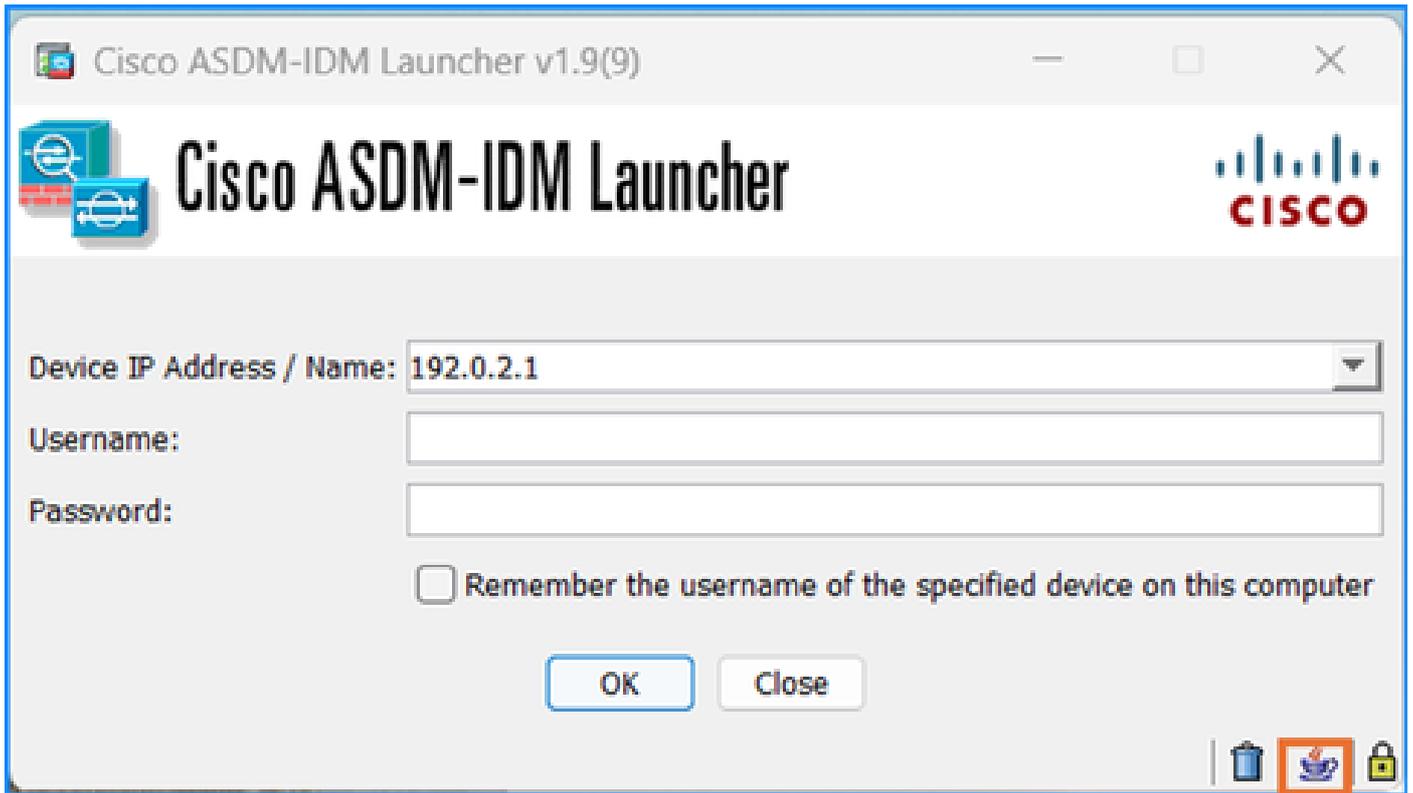
Java 콘솔 로그에는 "Firepower에 연결하지 못했습니다. 이 메시지 없이 계속합니다." 메시지가 표시됩니다.

<#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: cp1@18c4cb7
93 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup - CLI-PASSTHROUGH-DEBUG Inside d
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cp1@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 again
Env.isAsdmInHeadlessMode()----->false
java.lang.InterruptedExcepcion
    at java.lang.Object.wait(Native Method)
```

이 증상을 확인하려면 Java 콘솔 로그를 활성화합니다.



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwe15164 "ASA: ASDM은 CLI를 통해 "절전 모드 해제"될 때까지 SFR 탭을 표시할 수 없습니다." 해결 단계:

1. ASDM 관리자를 닫습니다.
2. SFR에 대한 SSH 액세스 권한을 얻고 사용자를 root로 전환합니다(sudo su).
3. 위 단계를 수행한 후 ASDM을 다시 실행하면 Firepower(SFR) 탭을 로드할 수 있습니다.

참고: 이 결함은 최근 Firepower 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 14. ASDM에 Firepower 모듈 관리/구성이 표시되지 않습니다

firepower 모듈 컨피그레이션은 ASDM에서 사용할 수 없습니다.

문제 해결 - 권장 조치

1. ASA, ASDM, Firepower 모듈 및 운영 체제 버전이 호환되는지 확인합니다. [Cisco Secure Firewall ASA 릴리스 노트](#), [Cisco Secure Firewall ASDM 릴리스 노트](#), [Cisco Secure Firewall ASA 호환성을](#) 참조하십시오.

 - ASA 9.14/ASDM 7.14/Firepower 6.6은 ASA 5525-X, 5545-X 및 5555-X의 ASA Firepower 모듈에 대한 최종 버전입니다.

- ASA 9.12/ASDM 7.12/Firepower 6.4.0은 ASA 5515-X 및 5585-X의 ASA Firepower 모듈에 대한 최종 버전입니다.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3은 ASA 5506-X Series 및 5512-X의 ASA Firepower 모듈에 대한 최종 버전입니다.
- 달리 명시되지 않는 한 ASDM 버전은 모든 이전 ASA 버전과 역호환됩니다. 예를 들어 ASDM 7.13(1)은 ASA 9.10(1)에서 ASA 5516-X를 관리할 수 있습니다.
- ASDM은 ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ 및 9.16(3.19)+의 Firepower 모듈 관리에 지원되지 않습니다. 이 릴리스로 모듈을 관리하려면 FMC를 사용해야 합니다. 이러한 ASA 릴리스에는 ASDM 7.18(1.152) 이상이 필요하지만 ASA Firepower 모듈에 대한 ASDM 지원이 7.16으로 종료되었습니다.
- ASDM 7.13(1) 및 ASDM 7.14(1)는 ASA 5512-X, 5515-X, 5585-X 및 ASASM을 지원하지 않습니다. asdm 지원을 복원하려면 ASDM 7.13(1.101) 또는 7.14(1.48)로 업그레이드해야 합니다.

2. 버전이 호환 가능한 경우 모듈이 작동 및 실행 중인지 확인합니다.

```
<#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
```

모듈이 다운된 경우 sw-module module reset 명령을 사용하여 모듈을 재설정한 다음 모듈 소프트웨어를 다시 로드할 수 있습니다.

참조

- [Cisco Secure Firewall ASA 릴리스 정보](#)
- [Cisco Secure Firewall ASDM 릴리스 정보](#)
- [Cisco Secure Firewall ASA 호환성](#)

문제 15. ASDM에서 보안 클라이언트 프로파일에 액세스할 수 없습니다.

Java 콘솔 로그에 "java.lang.ArrayIndexOutOfBoundsException이 표시됩니다. 3" 오류 메시지:

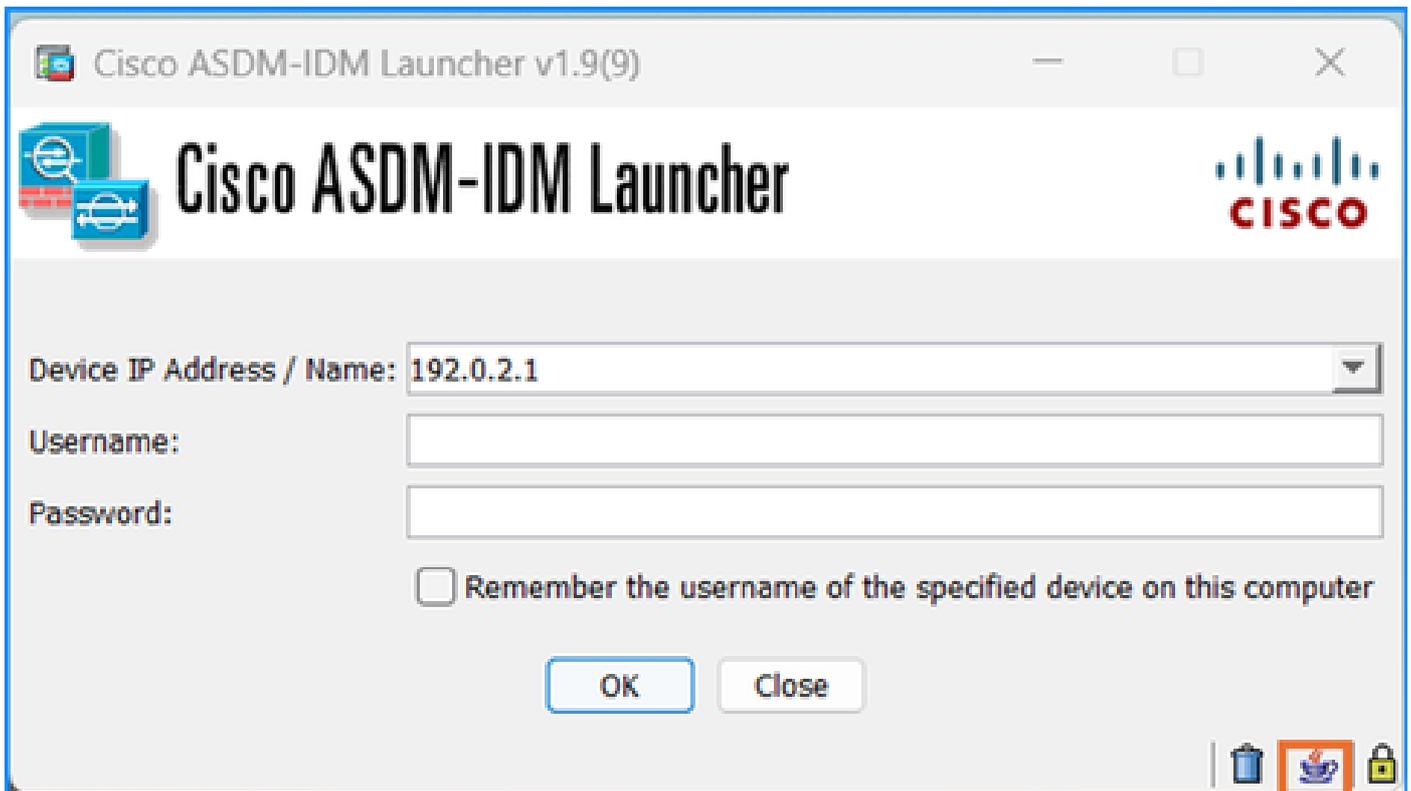
<#root>

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

java.lang.ArrayIndexOutOfBoundsException: 3

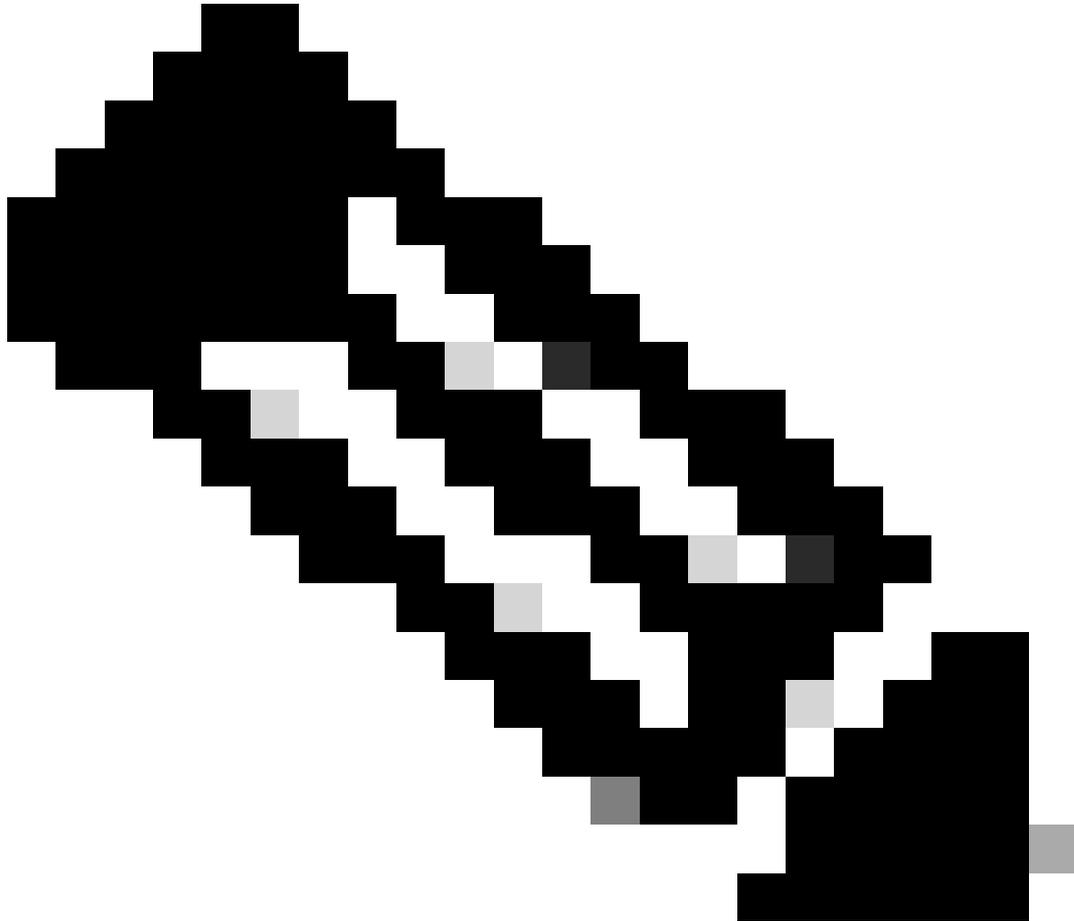
```
at doz.a(doz.java:1256)
at doz.a(doz.java:935)
at doz.l(doz.java:1100)
```

이 증상을 확인하려면 Java 콘솔 로그를 활성화합니다.



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwi56155 "Unable to access Secure Client Profile on ASDM"을 참조하십시오.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

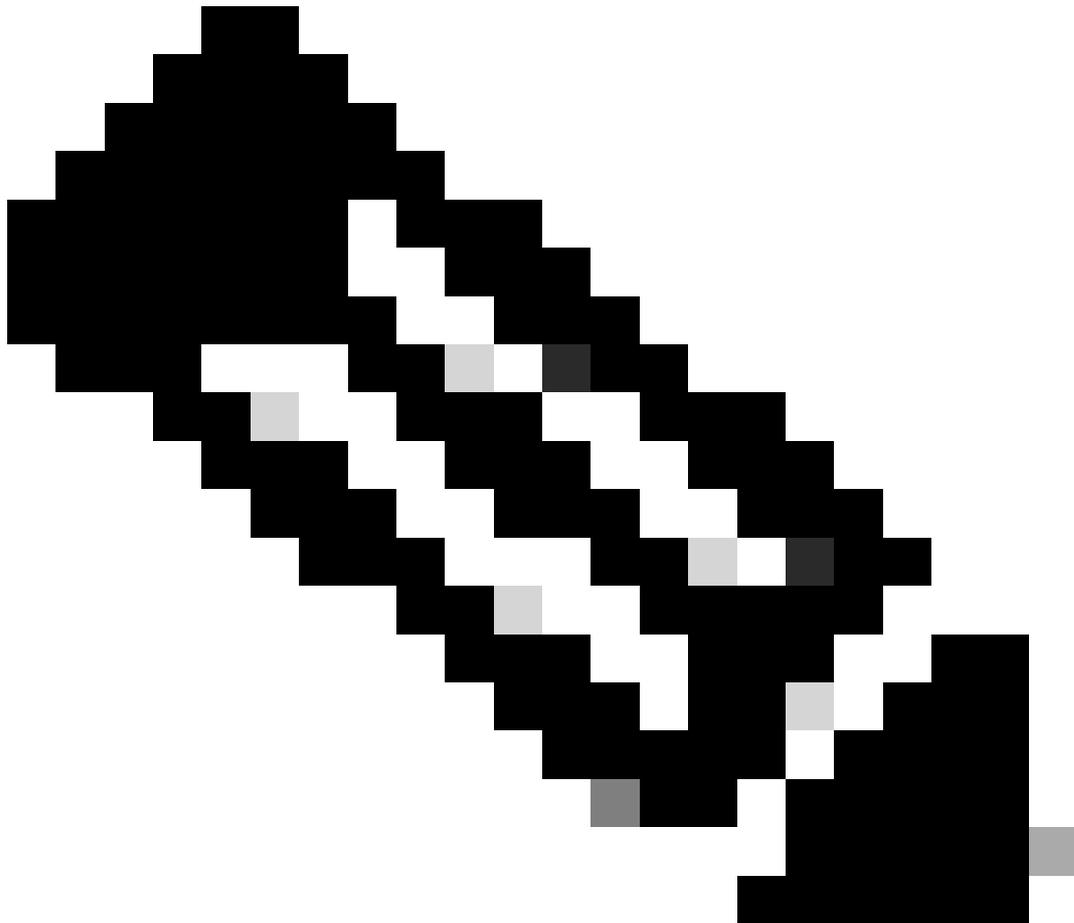
문제 16. ASDM에서 보안 클라이언트 프로파일 XML 프로파일을 편집할 수 없습니다

버전 4.8 이전의 디스크에 AnyConnect 이미지가 있는 경우 ASDM Configuration(ASDM 컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스)의 Secure Client Profile(보안 클라이언트 프로파일) XML 프로파일을 ASA 디바이스에서 편집할 수 없습니다.

오류 메시지 "장치의 보안 클라이언트 이미지에 프로파일 편집기 플러그인이 없습니다. Please go to Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Client Software(보안 클라이언트 소프트웨어)로 이동하여 Secure Client Image version 2.5 이상을 설치한 후 다시 시도하십시오)"가 표시됩니다.

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwk64399 "ASDM- Unable to edit Secure Client Profile"을 참조하십시오. 해결 방법은 우선 순위가 낮은 다른 AnyConnect 이미지를 설정하는 것입니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 17. 컨피그레이션 변경 후 Secure Client 이미지가 없습니다.

ASDM Configuration(ASDM 컨피그레이션) > Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Client Profile(보안 클라이언트 프로파일)을 변경한 후 Configuration(컨피그레이션) > Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Client Software(보안 클라이언트 소프트웨어)의 이미지가 누락되었습니다.

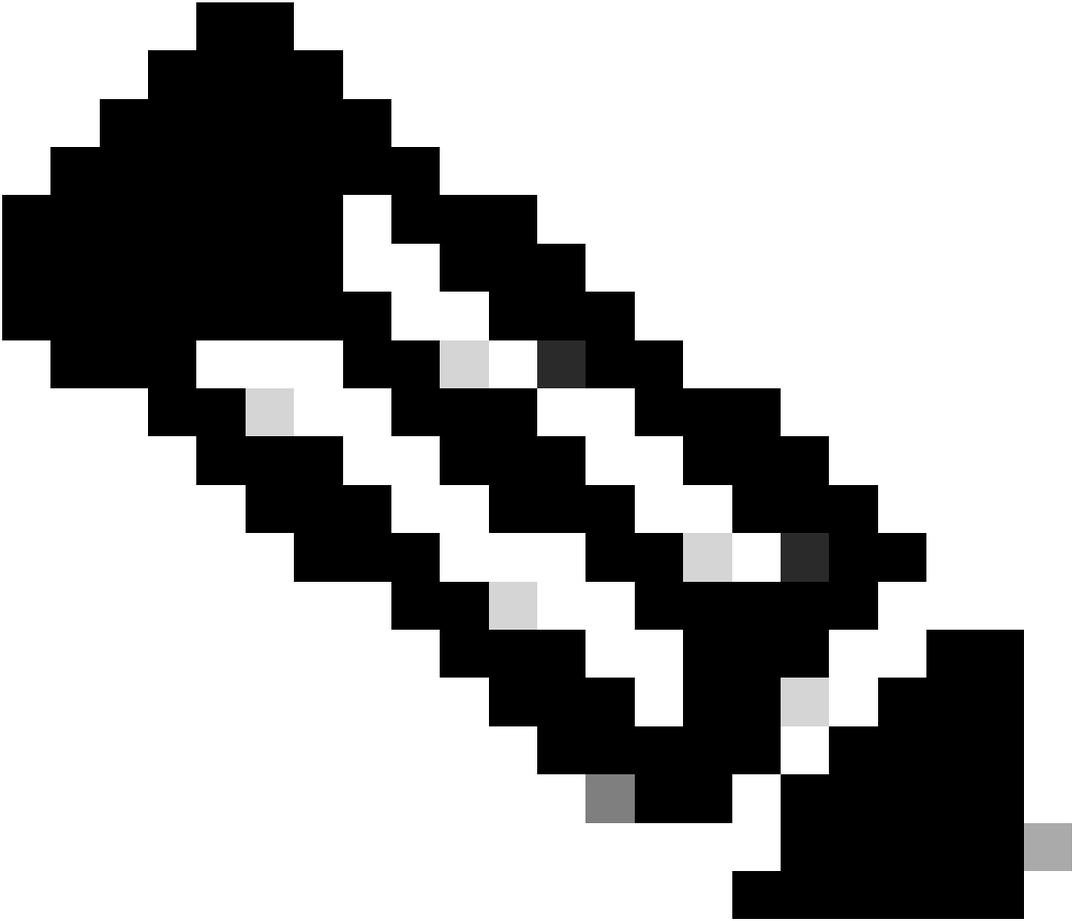
문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwf23826 "Secure Client Software is not displayed after modify the Secure Client Profile Editor in ASDM"을 참조하십시오. 해결 방법:

- ASDM에서 Refresh(새로 고침) 아이콘을 클릭합니다

또는

- ASDM을 닫고 다시 엽니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 18. 비효율적인 http server session-timeout 및 http server idle-timeout 명령

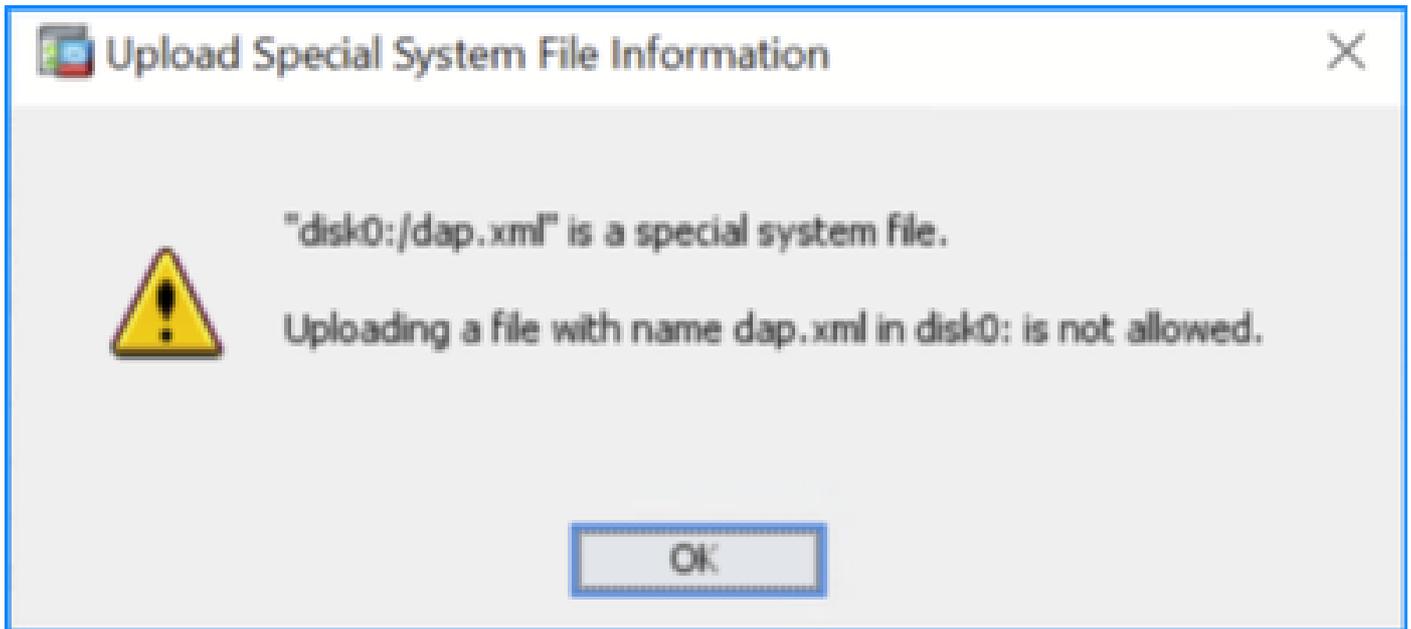
http server session-timeout 및 http server idle-timeout 명령은 다중 컨텍스트 모드 ASA에 영향을 주지 않습니다.

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCtx41707 "Support for http server timeout command in multi-context mode"를 참조하십시오. 명령은 구성할 수 있지만 값이 영향을 미치지 않습니다.

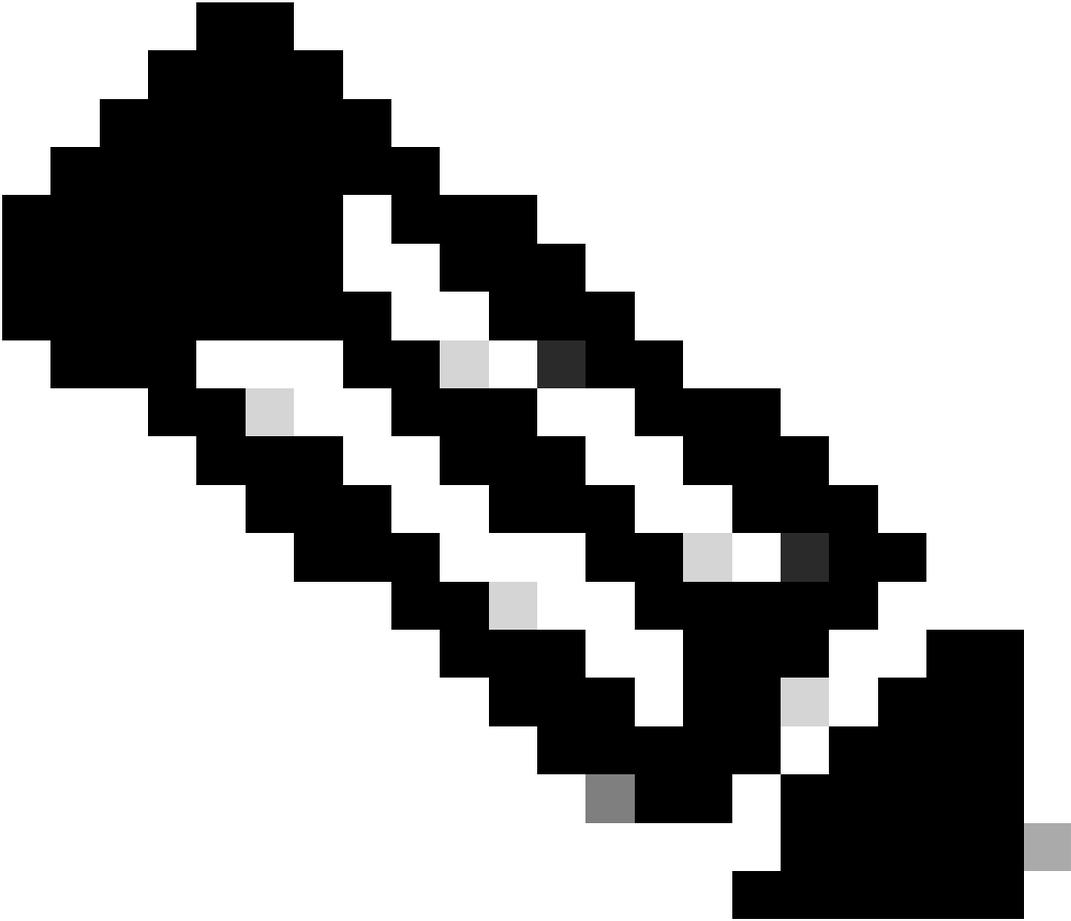
문제 19. ASDM에서 Dap.xml 복사 실패

ASDM의 File Management(파일 관리) 창을 통해 dap.xml을 ASA로 복사하지 못하면 "disk0:/dap.xml is a special system file(디스크0:는 특수 시스템 파일입니다.)"이라는 오류 메시지가 표시됩니다. disk0에 dap.xml 이름을 가진 파일 업로드: 허용되지 않음:



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCvt62162 "Cannot copy dap.xml using File Management in ASDM 7.13.1"을 참조하십시오. 해결 방법은 FTP 또는 TFTP와 같은 프로토콜을 사용하여 ASA에 파일을 직접 복사하는 것입니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 20. ASDM에 IKE 정책 및 IPSEC 제안서가 표시되지 않음

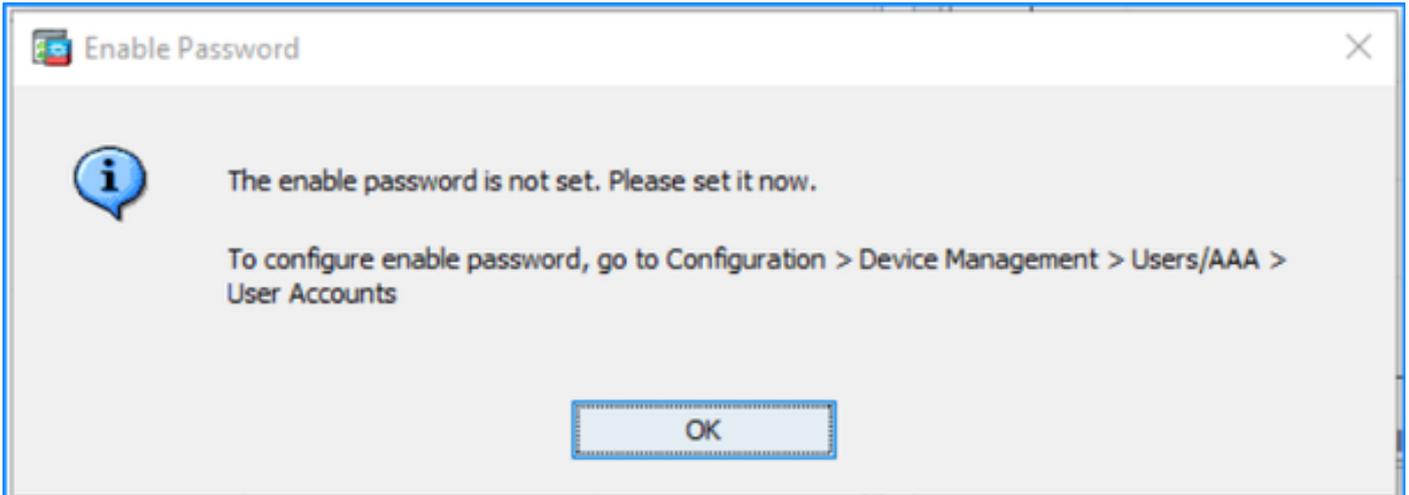
ASDM은 Configurations(컨피그레이션) > Site-to-Site VPN(사이트 대 사이트 VPN) 창에 IKE 정책 및 IPSEC 제안을 표시하지 않습니다.

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwm42701 "ASDM display blank in IKE policies and IPSEC proposals(IKE 정책 및 IPSEC 제안 탭에 ASDM 표시 비어 있음)"를 참조하십시오.

문제 21. ASDM에 "The enable password is not set. 지금 설정하십시오."

ASDM에 "The enable password is not set. 지금 설정하십시오." 명령줄에서 enable 비밀번호를 변경한 후



문제 해결 - 권장 조치

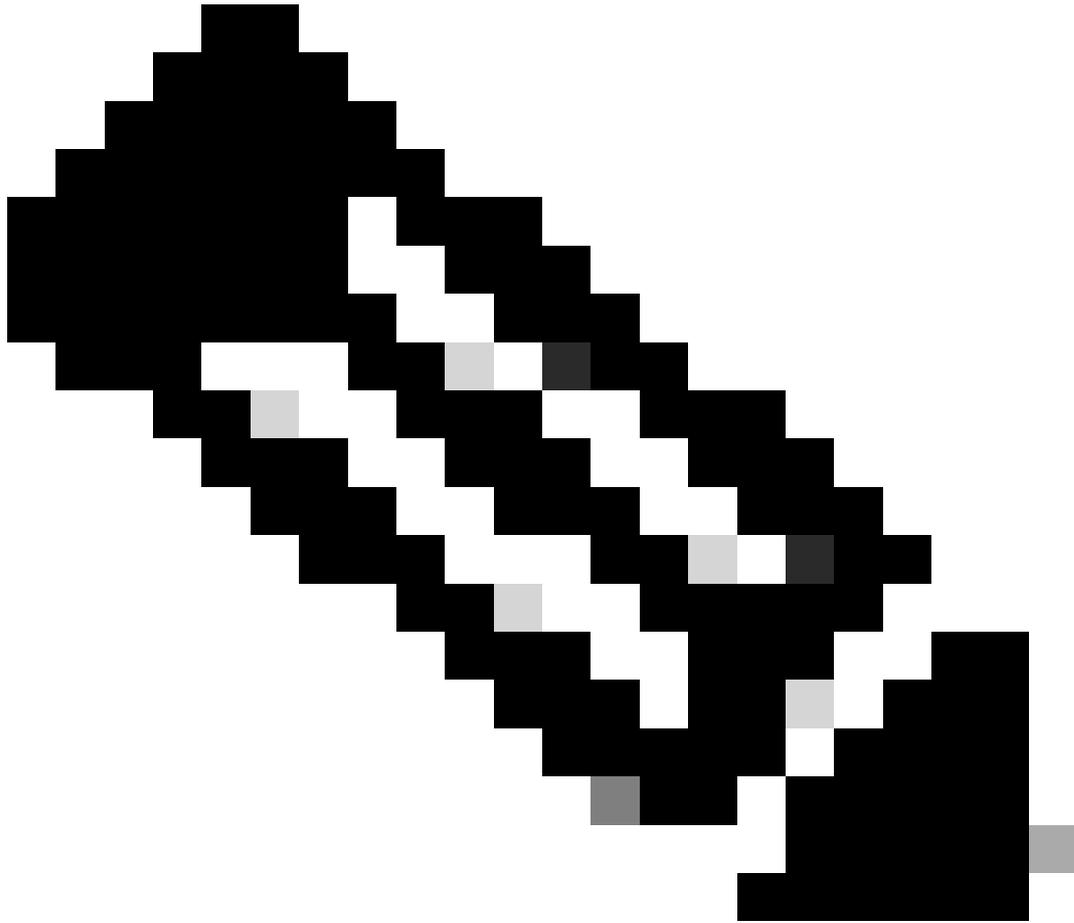
소프트웨어 Cisco 버그 ID CSCvq42317 "CLI에서 설정한 후 enable 비밀번호를 변경하라는 ASDM 프롬프트"를 참조하십시오.

문제 22. ASDM UI를 새로 고치면 ASDN 객체가 사라집니다.

객체 그룹과 객체 호스트를 기존 객체 그룹에 추가할 때 ASDM을 새로 고치면 객체 그룹이 ASDM 목록에서 사라집니다. 개체 이름은 이 결함이 일치하도록 숫자로 시작해야 합니다.

문제 해결 - 권장 조치

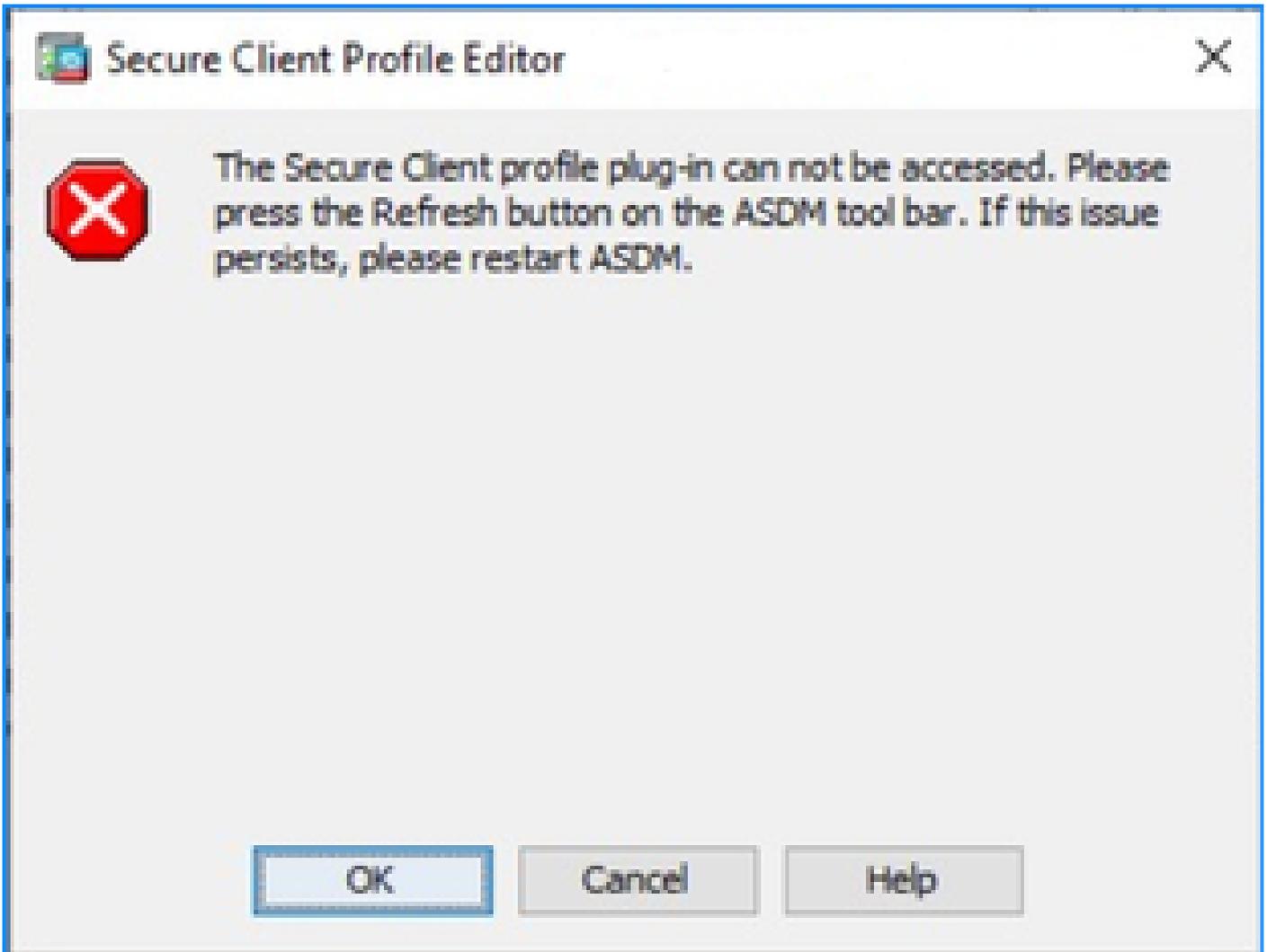
소프트웨어 Cisco 버그 ID CSCwf71723 "ASDM losing configured objects/object groups"를 참조하십시오.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

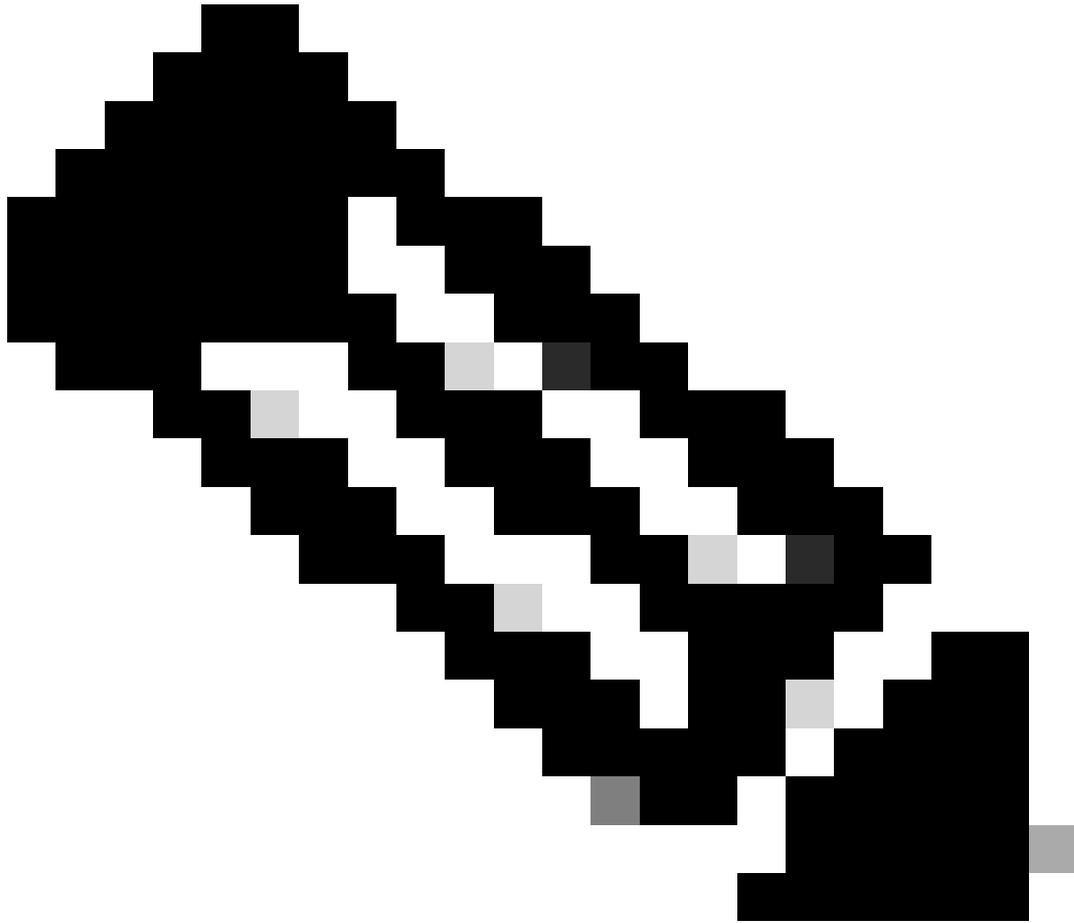
문제 23. 4.5 이전 버전의 AnyConnect 클라이언트 프로파일을 편집할 수 없습니다.

버전 4.5 이전의 AnyConnect 프로파일에 대해서는 AnyConnect 클라이언트 프로파일을 편집할 수 없습니다. 오류 메시지는 "The Secure Client profile plug-in can not access. ASDM 도구 모음에서 Refresh(새로 고침) 버튼을 누르십시오. 이 문제가 지속되면 ASDM을 다시 시작하십시오.":



문제 해결 - 권장 조치

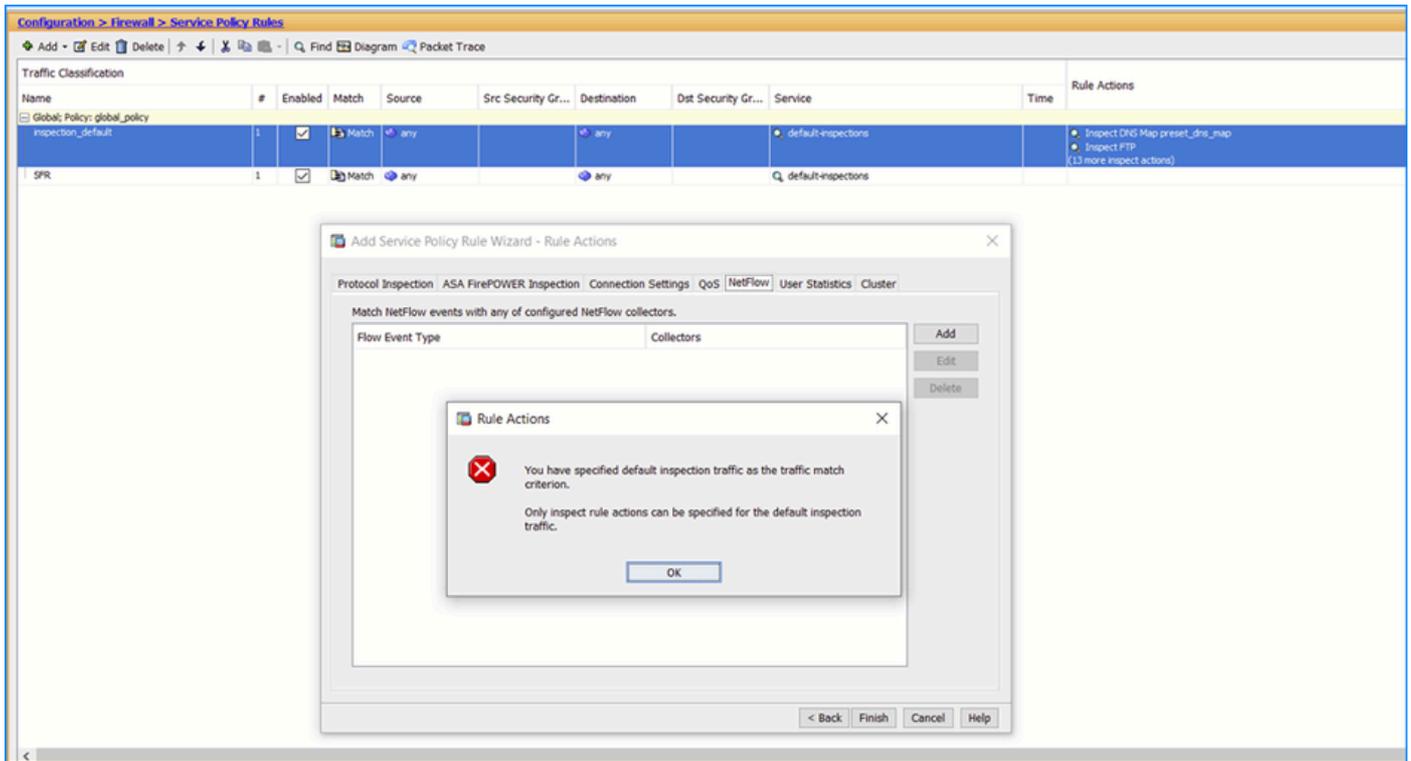
소프트웨어 Cisco 버그 ID CSCwf16947 "ASDM - Unable to load Anyconnect Profile Editor"를 참조하십시오.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

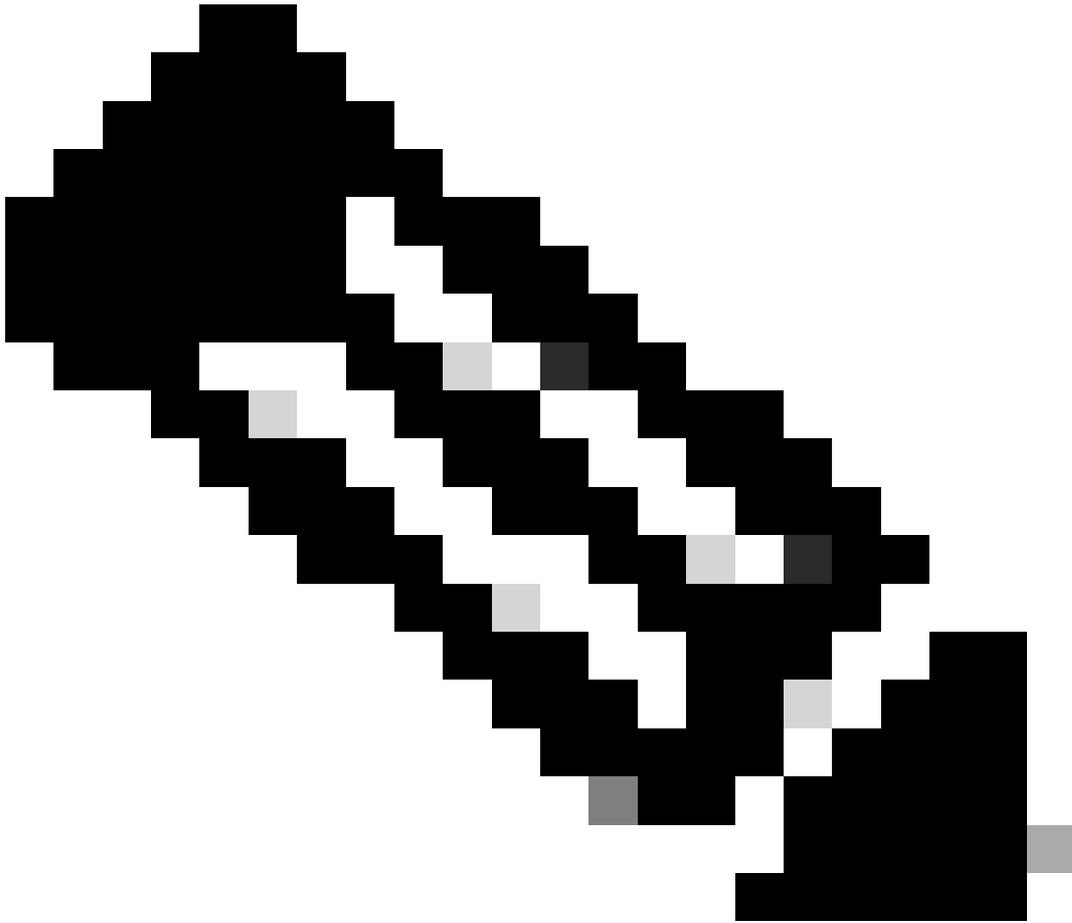
문제 24. Edit Service Policy(서비스 정책 수정) > Rule Actions(규칙 작업) > ASA Firepower Inspection(ASA 검사) 탭으로 이동할 수 없습니다.

ASDM 버전 7.8.2에서는 사용자가 Edit Service Policy(서비스 정책 수정) > Rule Actions(규칙 작업) > ASA Monitoring Inspection(ASA Firepower 검사) 탭으로 이동할 수 없으며 오류가 표시됩니다. "기본 검사 트래픽을 트래픽 일치 기준으로 지정했습니다. 기본 검사 트래픽에 대해서는 검사 규칙 작업만 지정할 수 있습니다." 이는 리디렉션을 위해 ACL을 선택한 경우에도 발생합니다.



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCvg15782 "ASDM - 버전 7.8(2)로 업그레이드한 후 수정 SFR 트래픽 리디렉션이 볼 수 없음"을 참조하십시오. 해결 방법은 CLI를 사용하여 정책 맵 컨피그레이션을 수정하는 것입니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

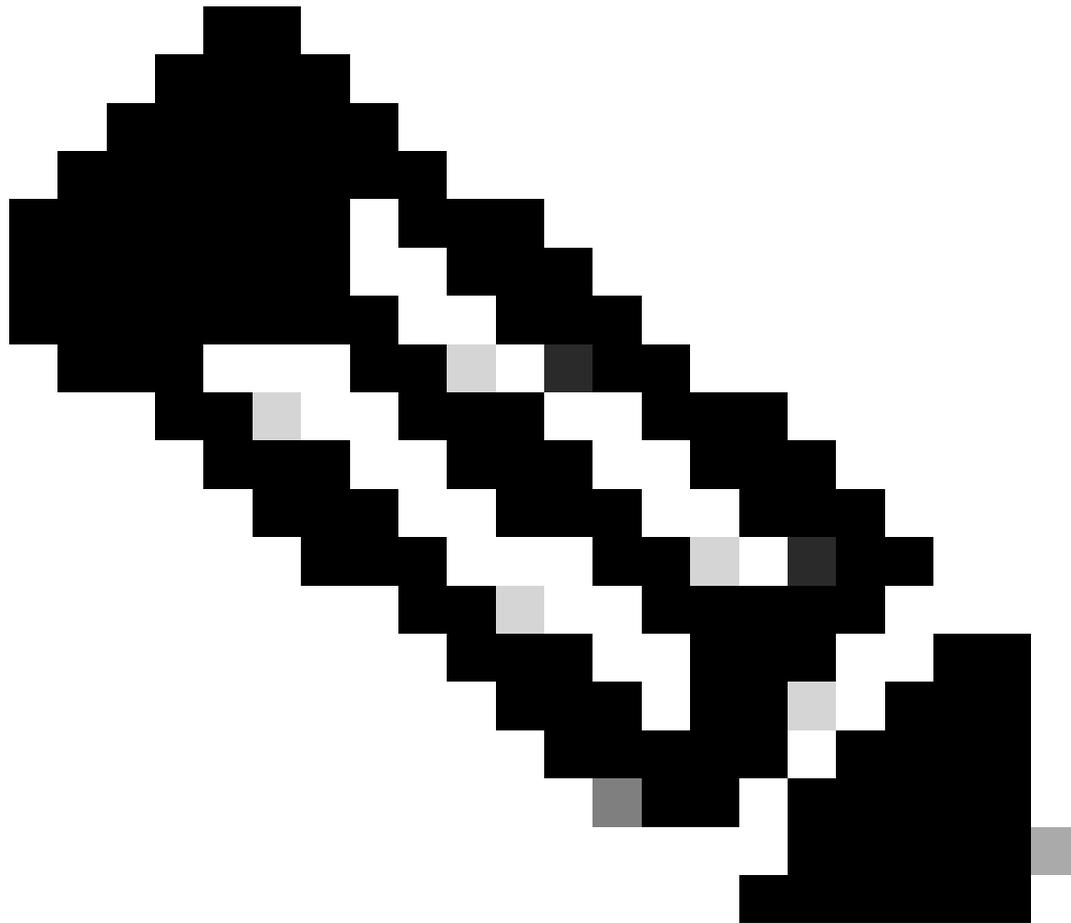
문제 25. ASDM의 AnyConnect 이미지 버전 5.1 및 AnyConnect 프로파일 편집기

Secure Client 소프트웨어 버전 5.1에서는 다음과 같은 증상이 나타납니다.

1. Win/Mac/Linux 패키지를 로드할 때 그룹 정책 모듈 이름이 나열되지 않습니다
2. ASDM에서 AnyConnect 프로파일 편집기를 열지 못했습니다.

문제 해결 - 권장 조치

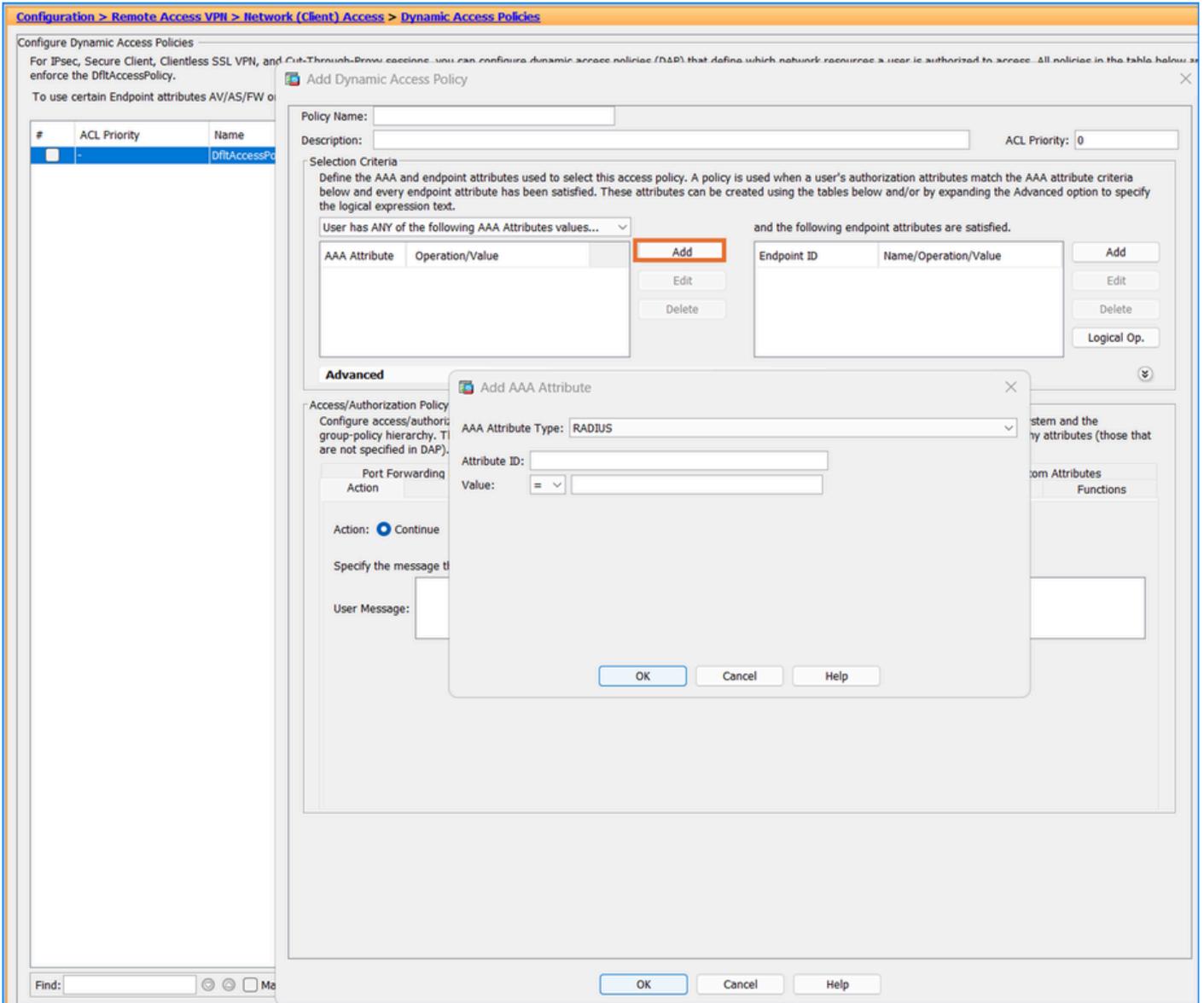
소프트웨어 Cisco 버그 ID CSCwh74417 "[ASDM](#): CSC Image 5.1"을 사용하는 경우 AnyConnect 프로파일 편집기 및 그룹 정책을 로드할 수 없습니다. 해결 방법은 Secure Client의 하위 버전을 사용하는 것입니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

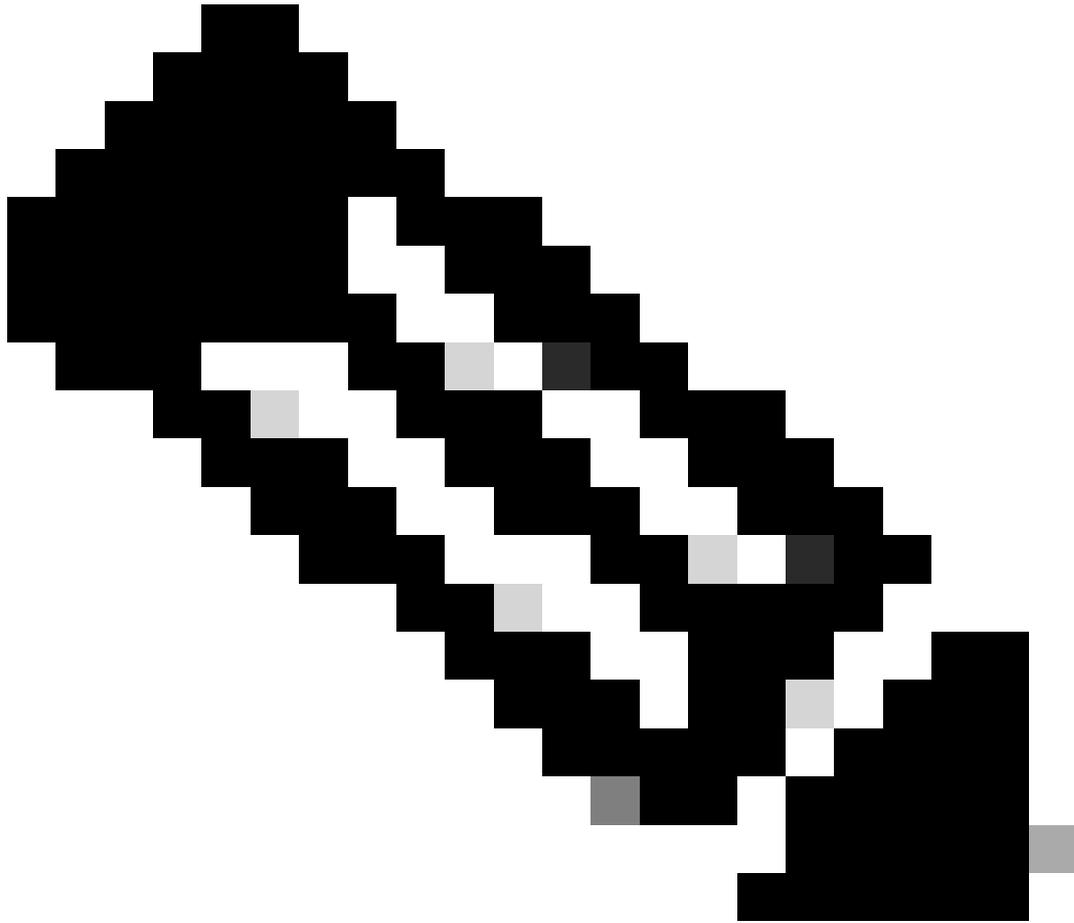
문제 26. AAA 특성 유형(Radius/LDAP)은 ASDM에 표시되지 않습니다.

AAA 특성 유형(Radius/LDAP)은 ASDM > Configuration(구성) > Remote Access VPN(원격 액세스 VPN)> Network (Client) Access(네트워크(클라이언트) 액세스)> Dynamic Access Policies(동적 액세스 정책)>Add(추가) > On AAA attribute(AAA 특성) 필드 > Add(추가) > Select Radius or LDAP(Radius 또는 LDAP 선택)에서 표시되지 않습니다.



문제 해결 - 권장 조치

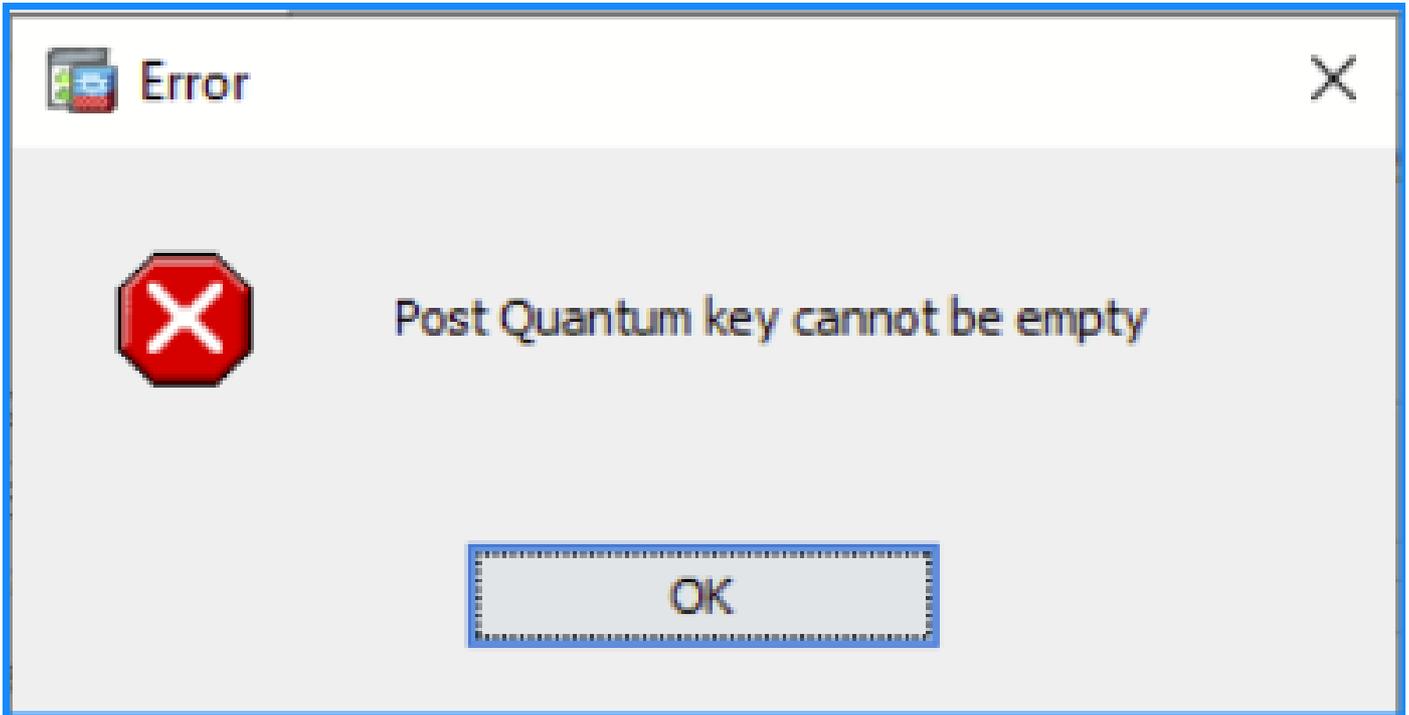
소프트웨어 Cisco 버그 ID CSCwa99370 "[ASDM](#): ASDM:DAP config missing AAA Attributes type (Radius/LDAP)" 및 Cisco 버그 ID [CSCwd16386](#) "ASDM:DAP config missing AAA Attributes type (Radius/LDAP)"



참고: 이러한 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

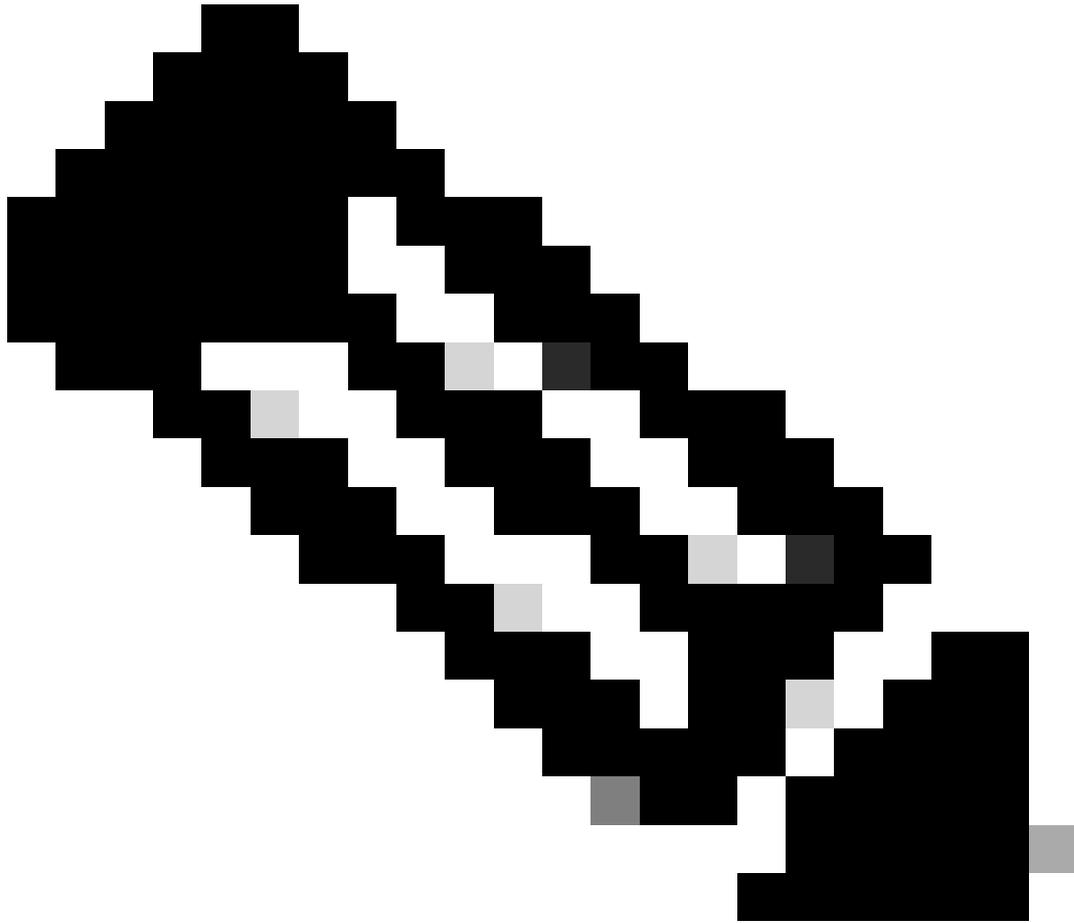
문제 27. 'Post Quantum key cannot be empty' 오류가 ASDM에 표시됩니다.

'Post Quantum key cannot be empty' 오류는 ASDM > Configuration(구성) > Remote Access VPN(원격 액세스 VPN)> Network (Client) Access(네트워크(클라이언트) 액세스) >IPsec (IKEv2) Connection Profiles(IKEv2) 연결 프로파일)의 Advanced(고급) 섹션을 편집할 때 표시됩니다.



문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwe58266 "ASDM IKEv2 configuration - Post Quantum Key cannot be empty error message"를 참조하십시오.



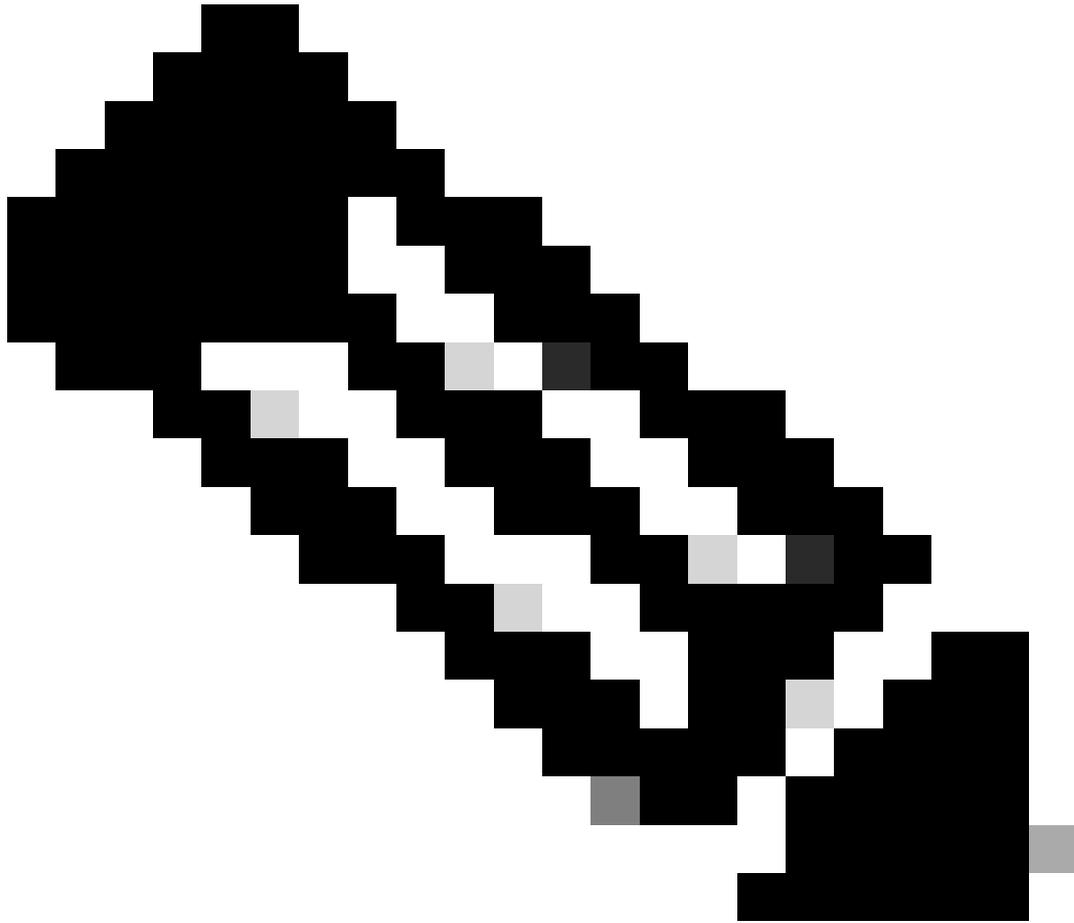
참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 28. ASDM은 "where used" 옵션을 사용할 때 어떤 결과도 표시하지 않습니다.

ASDM에서는 Configuration(컨피그레이션) > Firewall(방화벽) > Objects(개체) > Network Objects/Groups(네트워크 개체/그룹)로 이동하고 마우스 오른쪽 버튼으로 Object(개체)를 클릭하여 "where used(사용처)" 옵션을 사용할 때 결과를 표시하지 않습니다.

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID [CSCwd98702](#)의 ""ASDM에서 작동하지 않는"" 옵션을 참조하십시오.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 29. 네트워크 개체를 삭제할 때 "[Network Object]는 다음에 사용되므로 삭제할 수 없습니다."

ASDM은 Configuration(컨피그레이션) > Firewall(방화벽) > Objects(개체) > Network Objects/Groups(네트워크 개체/그룹)에서 네트워크 그룹에서 참조되는 네트워크 개체를 삭제할 때 "[Network Object] cannot be deleted in the following(다음에 사용되므로 [네트워크 개체]를 삭제할 수 없습니다)"라는 경고 메시지를 표시하지 않습니다¶

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID [CSCwe67056](#) "[네트워크 개체]는 다음 "경고 표시 안 함"에 사용되므로 삭제할 수 없습니다.

참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

문제 30. ASDM의 Network Objects/Group(네트워크 개체/그룹) 탭의 사용 편의성 문제

다음 증상 중 하나 이상이 관찰됩니다.

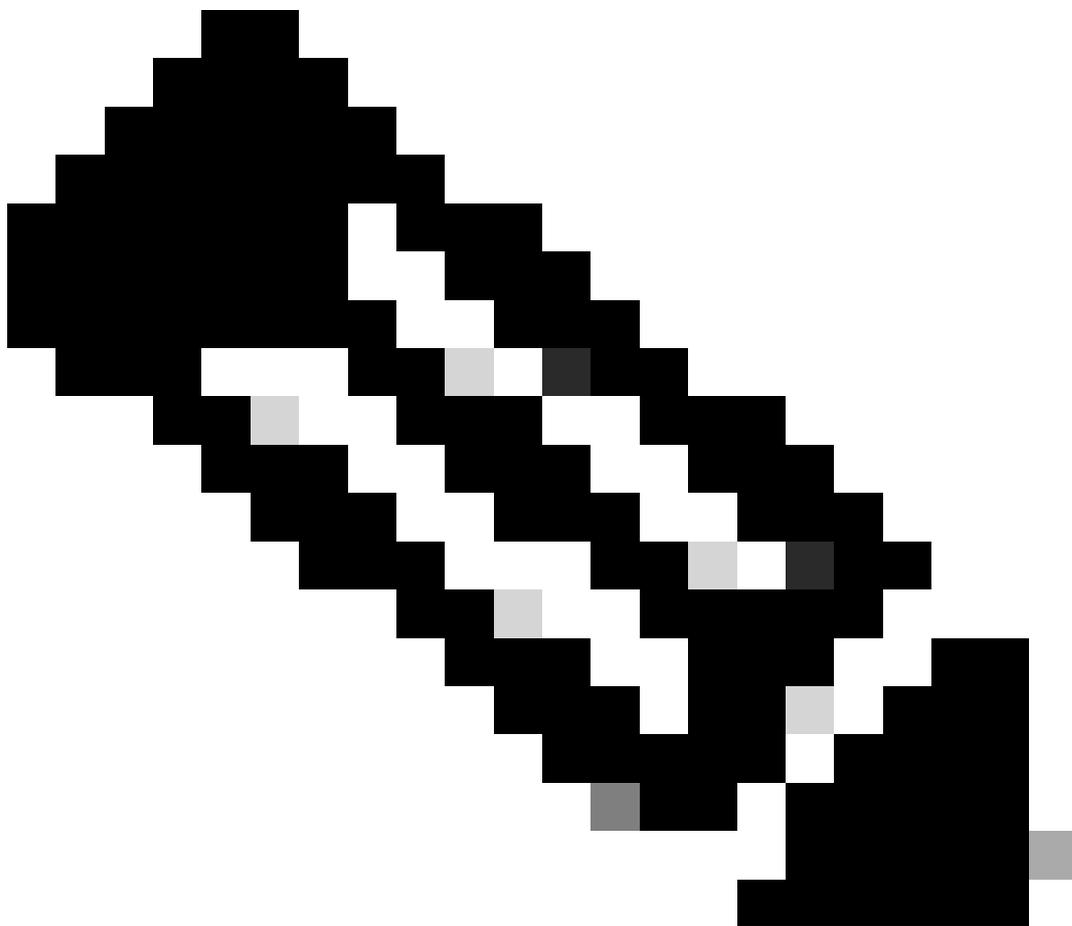
- "개체 그룹 추가/편집 창"의 "새 개체 구성원 만들기" 섹션에 있는 "이름" 텍스트 입력은 "선택 사항"으로 표시됩니다. 그러나 이름을 입력하지 않으면 객체를 만들고 추가할 수 있는 "Add>>" 버튼이 비활성화됩니다.
- 사용자가 "사용 위치..."를 클릭하면 열리는 "사용" 탭 컨텍스트 메뉴에는 객체를 직접 참조하는 엔티티(ACL, 경로 맵, 객체 그룹)만 나열됩니다. 또한 재귀적으로 두 번째, 세 번째 등을 나열해야 합니다. 주문 참조(객체가 포함된 객체 그룹을 사용하는 ACL은 객체의 "사용"으로 나열되어야 함)
- 컨텍스트 메뉴에서 사용할 수 있는 "삭제" 작업에는 이 동작도 표시됩니다. 객체를 직접 참조

하는 엔티티는 자동으로 삭제됩니다(객체가 삭제될 때 엔티티가 비어 있는 경우). 2차, 3차 등에서는 이렇게 작동하지 않습니다. 객체 및 첫 번째 순서 참조가 삭제되므로 순서 참조가 비어 있게 됩니다.

사용자는 ASDM에서 나머지 컨피그레이션에서 객체가 삭제되어 비어 있는 엔티티가 차단되는 것을 방지한다고 생각할 수 있습니다. 그러나 반드시 그렇지는 않습니다.

문제 해결 - 권장 조치

소프트웨어 Cisco 버그 ID CSCwe86257 "Usability of Network Objects/Group Tab in ASDM"을 참조하십시오.

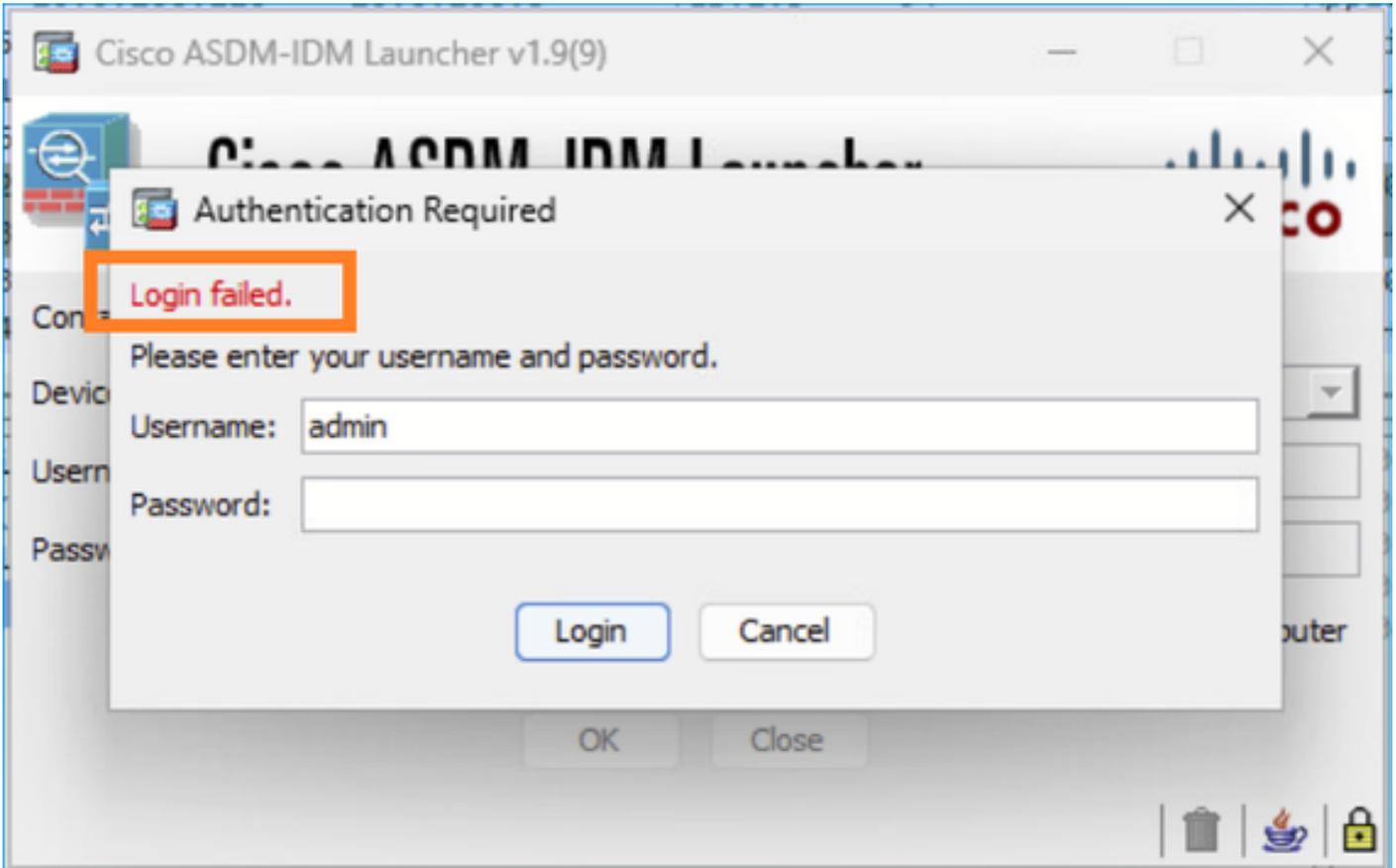


참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

ASDM 인증 문제 해결

문제 1. ASDM 로그인 실패

ASDM UI에 표시되는 오류는 다음과 같습니다.



문제 해결 - 권장 조치

이 오류는 동일한 인터페이스에서 HTTP 및 Webvpn Cisco Secure Client(AnyConnect)를 모두 활성화한 경우에 표시될 수 있습니다. 따라서 모든 조건이 충족되어야 합니다.

1. AnyConnect/Cisco Secure Client가 인터페이스에서 활성화됨
2. HTTP 서버는 AnyConnect/Cisco Secure Client와 동일한 인터페이스 및 포트에서 활성화됨

예:

```
<#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
```

문제 해결 팁: 'debug http 255'를 활성화하면 ASDM과 Webvpn 간의 충돌을 확인할 수 있습니다.

```
<#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
```

참고 사항으로, 로그인 실패에도 불구하고 ASA syslog는 인증이 성공했음을 보여줍니다.

```
<#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 = user2
```

```
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

해결 방법

해결 방법 1

ASA HTTP 서버의 TCP 포트를 변경합니다. 예를 들면 다음과 같습니다.

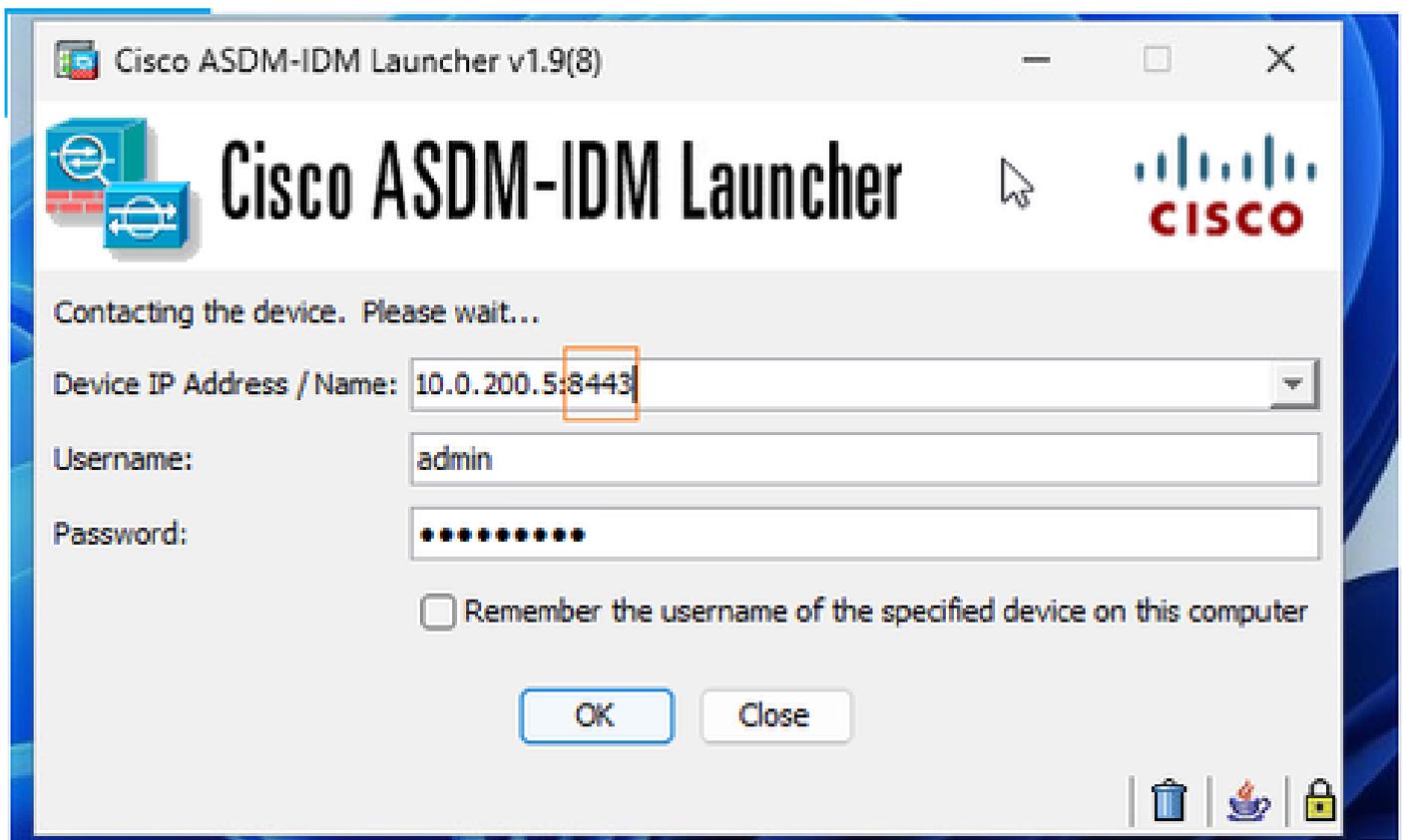
```
<#root>
```

```
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

```
http server enable 8443
```



해결 방법 2

AnyConnect/Cisco Secure Client의 TCP 포트를 변경합니다. 예를 들면 다음과 같습니다.

```
<#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
```

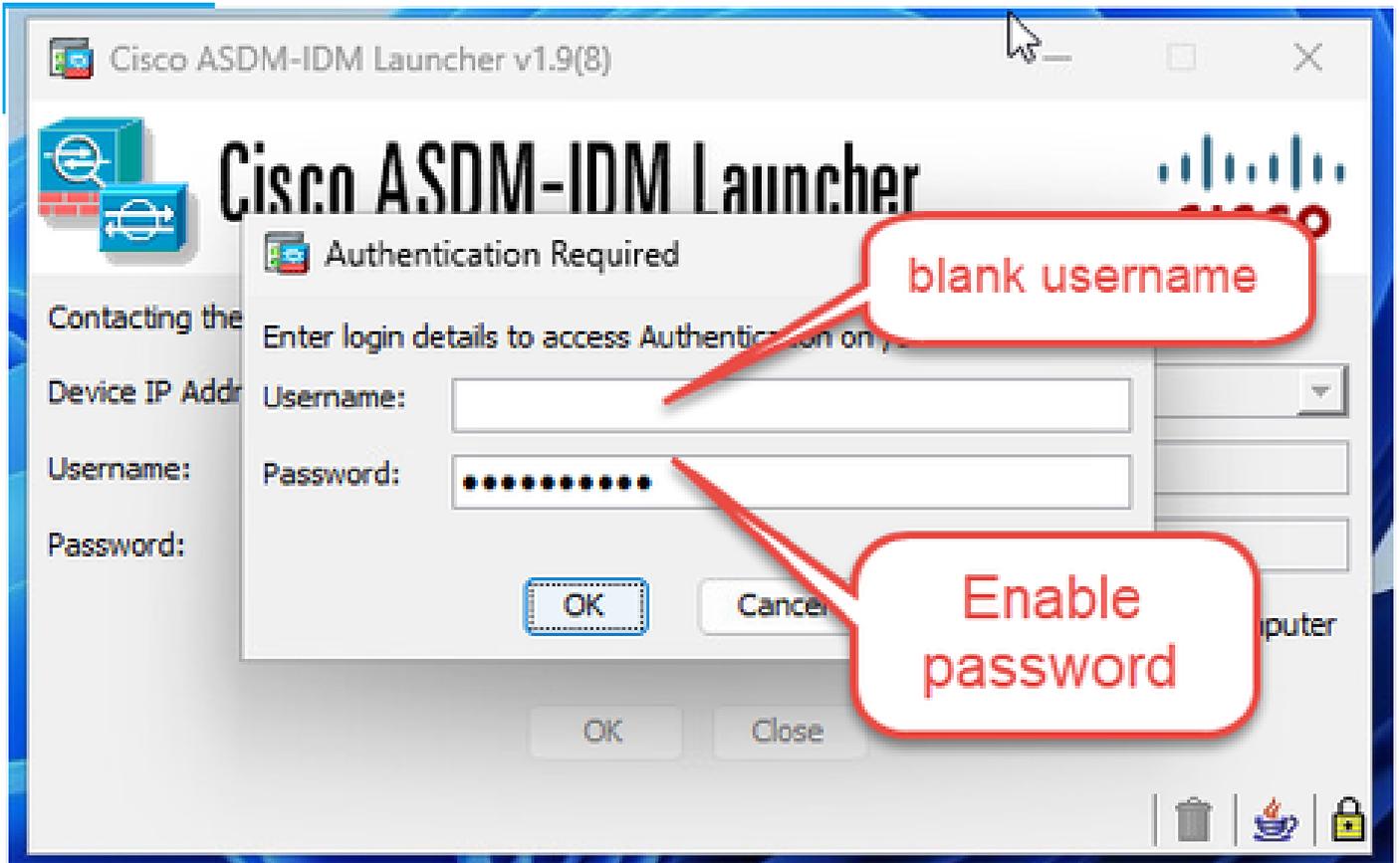
해결 방법 3

또 다른 해결 방법은 "aaa authentication http console" 컨피그레이션을 제거하는 것입니다.

```
<#root>
```

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

이 경우 enable 비밀번호를 사용하여 ASDM에 로그인할 수 있습니다.



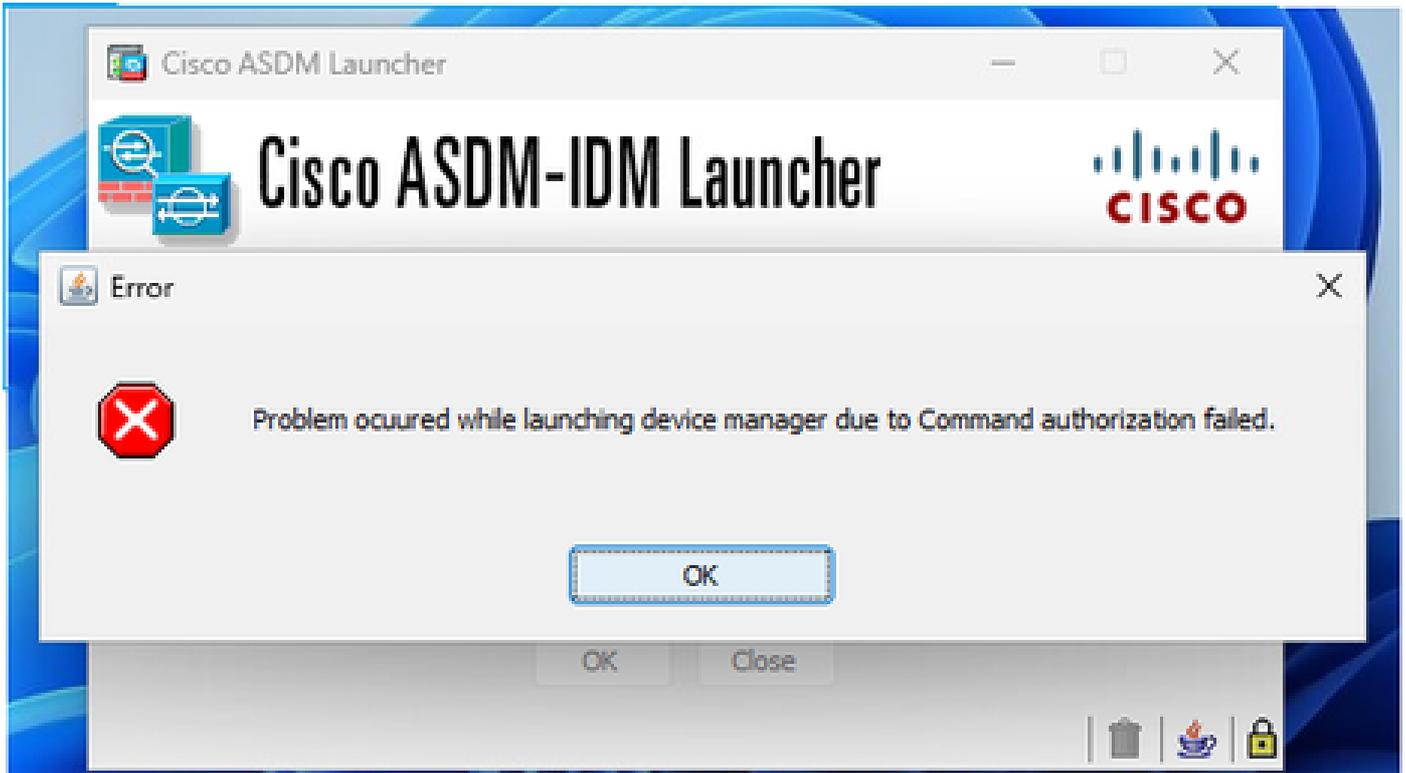
관련 결함

Cisco 버그 ID [CSCwb67583](#)

webvpn 및 ASDM이 동일한 인터페이스에서 활성화된 경우 경고 추가

문제 2. ASDM 명령 권한 부여에 실패했습니다.

ASDM UI에 표시되는 오류는 다음과 같습니다.



문제 해결 - 권장 단계

ASA에서 AAA 컨피그레이션을 확인하고 다음을 확인합니다.

- aaa 인증도 구성되었습니다.
- 원격 인증 서버를 사용하는 경우 이 서버에 연결할 수 있으며 명령을 인증합니다.

참조

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

문제 3. ASDM 읽기 전용 액세스 구성

ASDM 사용자에게 읽기 전용 액세스를 제공하려는 경우가 있습니다.

문제 해결 - 권장 단계

사용자 지정 권한 레벨(5)을 가진 새 사용자를 생성합니다. 예를 들면 다음과 같습니다.

```
<#root>
```

```
asa(config)#
```

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

이 명령은 "모니터링 전용" 수준인 권한 수준이 5인 사용자를 생성합니다. `[username]` 및 `[password]` 를 원하는 사용자 이름 및 비밀번호로 바꿉니다.

세부사항

로컬 명령 권한 부여에서는 16개의 권한 레벨(0~15) 중 하나에 명령을 할당할 수 있습니다. 기본적으로 각 명령은 권한 레벨 0 또는 15에 지정됩니다. 각 사용자를 특정 권한 레벨로 정의할 수 있으며 각 사용자는 지정된 권한 레벨 이하의 모든 명령을 입력할 수 있습니다. ASA는 로컬 데이터베이스, RADIUS 서버 또는 LDAP 서버(LDAP 특성을 RADIUS 특성에 매핑하는 경우)에 정의된 사용자 권한 레벨을 지원합니다.

절차

1단계	Configuration(컨피그레이션) > Device Management(디바이스 관리) > Users/AAA(사용자/AAA) > AAA Access(AAA 액세스) > Authorization(권한 부여)을 선택합니다.
2단계	Enable authorization for ASA command access(ASA 명령 액세스에 대한 권한 부여 활성화) > Enable(활성화) 확인란을 선택합니다.
3단계	Server Group 드롭다운 목록에서 LOCAL을 선택합니다.
4단계	<p>로컬 명령 권한 부여를 활성화할 때 개별 명령 또는 명령 그룹에 수동으로 권한 레벨을 할당하거나 미리 정의된 사용자 계정 권한을 활성화할 수 있습니다.</p> <ul style="list-style-type: none"> · Set ASDM Defined User Roles(ASDM에서 정의한 사용자 역할 설정)를 클릭하여 미리 정의된 사용자 계정 권한을 사용합니다. <p>ASDM Defined User Roles Setup 대화 상자가 나타납니다. 사전 정의된 사용자 계정 권한을 사용하려면 Yes를 클릭합니다. Admin(권한 레벨 15, 모든 CLI 명령에 대한 전체 액세스 권한) 읽기 전용(권한 레벨 5, 읽기 전용 액세스), 및 Monitor Only(권한 레벨 3, Monitoring 섹션에만 액세스).</p> <ul style="list-style-type: none"> · 명령 레벨을 수동으로 구성하려면 Configure Command Privileges를 클릭합니다. <p>Command Privileges Setup 대화 상자가 나타납니다. Command Mode 드롭다운 목록에서 All Modes를 선택하여 모든 명령을 보거나 컨피그레이션 모드를 선택하여 해당 모드에서 사용 가능한 명령을 볼 수 있습니다. 예를 들어, 컨텍스트를 선택하면 컨텍스트 컨피그레이션 모드에서 사용 가능한 모든 명령을 볼 수 있습니다. 컨피그레이션 모드뿐 아니라 사용자 EXEC 모드 또는 특권 EXEC 모드에서 명령을 입력할 수 있고 각 모드에서 서로 다른 작업을 수행하는 경우 이러한 모드에 대한 권한 레벨을 별도로 설정할 수 있습니다.</p> <p>Variant 열에는 show, clear 또는 cmd가 표시됩니다. 명령의 show, clear 또는 configure 형식에 대해서만 권한을 설정할 수 있습니다. 이 명령의 configure 형식은 일반적으로 컨피그레이션 변경을 발생시키는 형식으로, 수정되지 않은 명령(show 또는 clear 접두사 없음) 또는 no 형식으로 수행됩니다.</p>

	<p>명령의 레벨을 변경하려면 두 번 클릭하거나 Edit를 클릭합니다. 수준을 0~15로 설정할 수 있습니다. 기본 명령의 권한 수준만 구성할 수 있습니다. 예를 들어, 모든 aaa 명령의 수준을 구성할 수 있지만, aaa authentication 명령 및 aaa authorization 명령의 수준은 별도로 구성할 수 없습니다.</p> <p>나타나는 모든 명령의 레벨을 변경하려면 모두 선택, 편집을 클릭합니다.</p> <p>확인(OK)을 클릭하여 변경 사항을 승인합니다.</p>
5단계	<p>적용을 클릭합니다.</p> <p>권한 부여 설정이 할당되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.</p>

참조

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

문제 4. ASDM MFA(Multi-Factor Authentication)

문제 해결 - 권장 단계

이 문서 작성 시 ASDM은 MFA(또는 2FA)를 지원하지 않습니다. 이 제한에는 PingID 등의 솔루션이 포함된 MFA가 포함됩니다.

참조

Cisco 버그 ID [CSCvs85995](#)

ENH: MFA(Two Factor Authentication)를 사용하는 ASDM 액세스

문제 5. ASDM 외부 인증 컨피그레이션

문제 해결 - 권장 단계

LDAP, RADIUS, RSA SecurID 또는 TACACS+를 사용하여 ASDM에서 외부 인증을 구성할 수 있습니다.

참조

- <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

문제 6. ASDM 로컬 인증에 실패했습니다.

문제 해결 - 권장 단계

외부 인증 및 LOCAL 인증을 대안으로 사용하는 경우 로컬 인증은 외부 서버가 다운되었거나 작동하지 않는 경우에만 작동합니다. 이 시나리오에서만 LOCAL 인증이 인계되며 LOCAL 사용자와 연결할 수 있습니다.

외부 인증이 LOCAL 인증보다 우선하기 때문입니다.

예:

```
<#root>
```

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

참조

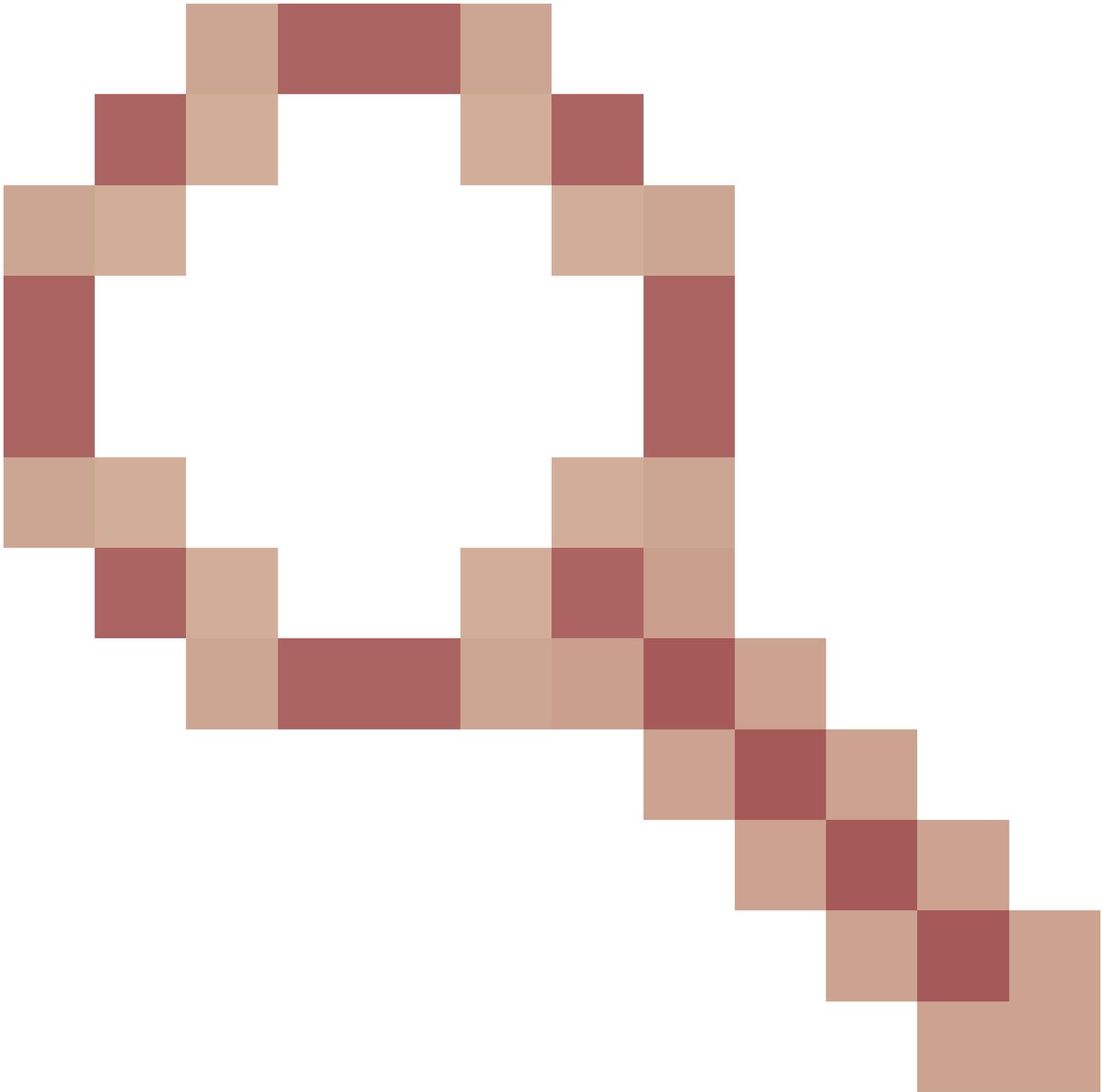
- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320>

문제 7. ASDM 일회용 비밀번호

문제 해결 - 권장 단계

- ASDM OTP(일회용 비밀번호) 인증 지원이 ASA 버전 8.x - 9.x에 추가되었고 단일 라우팅 모드에서만 지원됩니다.
- ASA 방화벽 투명 모드 및/또는 다중 컨텍스트 모드에 대한 ASDM OTP 인증은 이 범주에 들어가지 않습니다.

Cisco 버그 ID CSCtf를 [참조하십시오23419](#)



ENH: 다중 컨텍스트 및 투명 모드에서 ASDM OTP 인증 지원

문제 8. 연결 프로파일에 모든 방법이 표시되지 않음

이 경우 ASA CLI 컨피그레이션과 ASDM UI 간의 불일치가 문제가 됩니다.

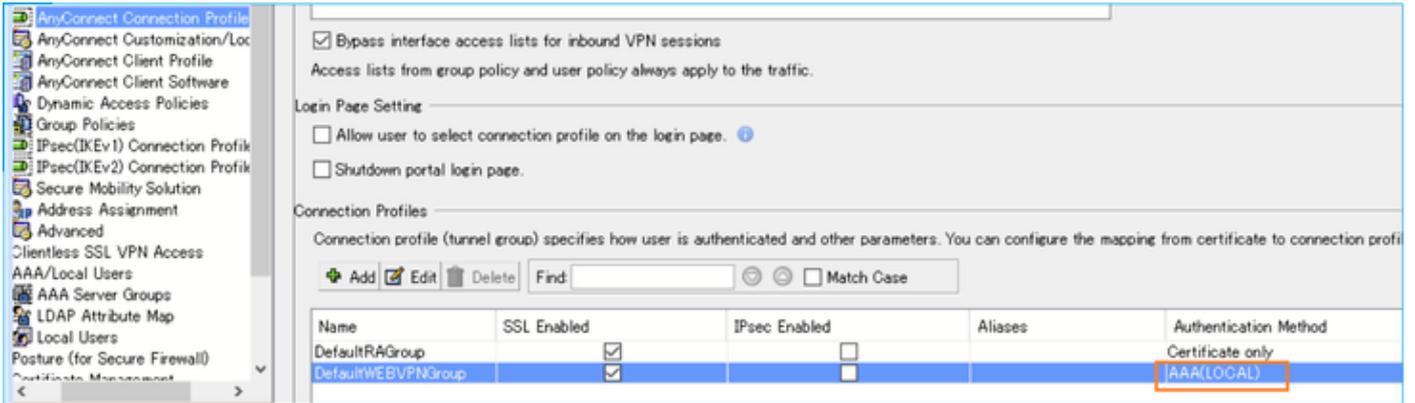
특히 CLI는 다음을 수행합니다.

```
<#root>
```

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

```
authentication aaa certificate
```

ASDM UI에서는 인증서 방법을 언급하지 않지만



문제 해결 - 권장 단계

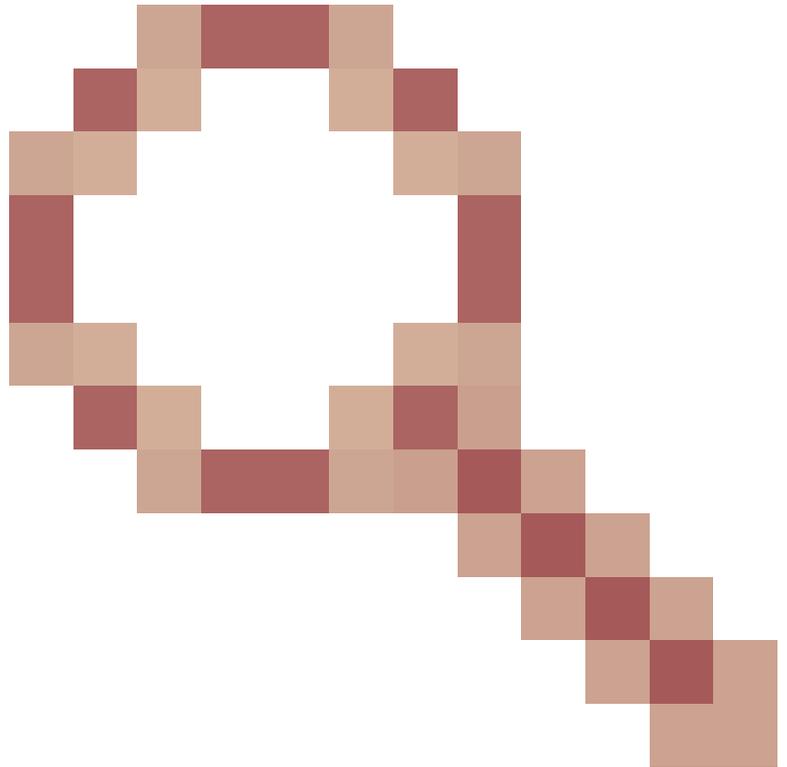
이것은 미용상의 문제입니다. ASDM에서 이 방법이 표시되지 않지만 인증서 인증이 사용됩니다.

문제 9. ASDM 세션이 시간 초과되지 않습니다.

ASDM GUI 세션 시간 초과는 고려되지 않습니다.

문제 해결 - 권장 단계

"aaa authentication http console LOCAL" 명령이 관리되는 ASA에 설정되지 않은 경우 이 오류가 발생합니다.



Cisco 버그 ID CSCwj를 [참조하십시오70826](#)

ENH: 경고를 추가합니다. 세션 시간 초과 설정, "aaa authentication http console LOCAL" 필요

해결 방법

관리되는 ASA에서 ""aaa authentication http console LOCAL"" 명령을 구성합니다.

문제 10. ASDM LDAP 인증에 실패했습니다.

문제 해결 - 권장 단계

1단계

다음과 같이 컨피그레이션이 제대로 되어 있는지 확인합니다.

<#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
```

2단계

LDAP 서버 상태를 확인합니다.

<#root>

```
asa#
show aaa-server
```

좋은 시나리오:

<#root>

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

잘못된 시나리오:

<#root>

Server status:

FAILED

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

3단계

LDAP 인증을 일시적으로 비활성화하여 LOCAL 인증이 제대로 작동하는지 확인합니다.

4단계

ASA에서 LDAP 디버그를 실행하고 사용자 인증을 시도합니다.

<#root>

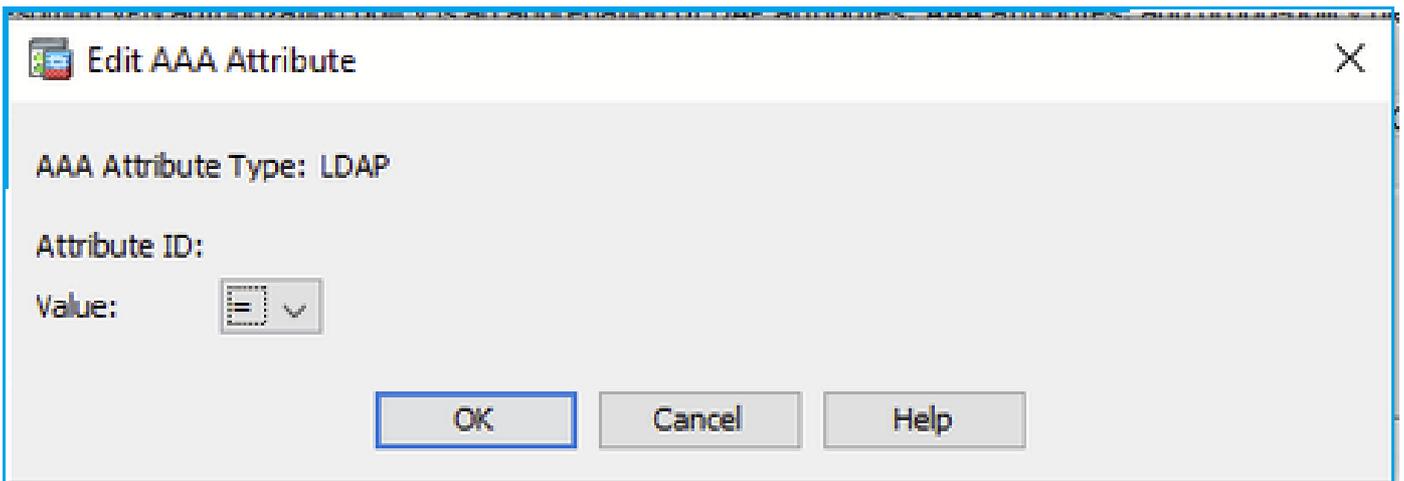
#

debug ldap 255

디버그에서는 "실패"와 같은 힌트가 포함된 줄을 찾습니다.

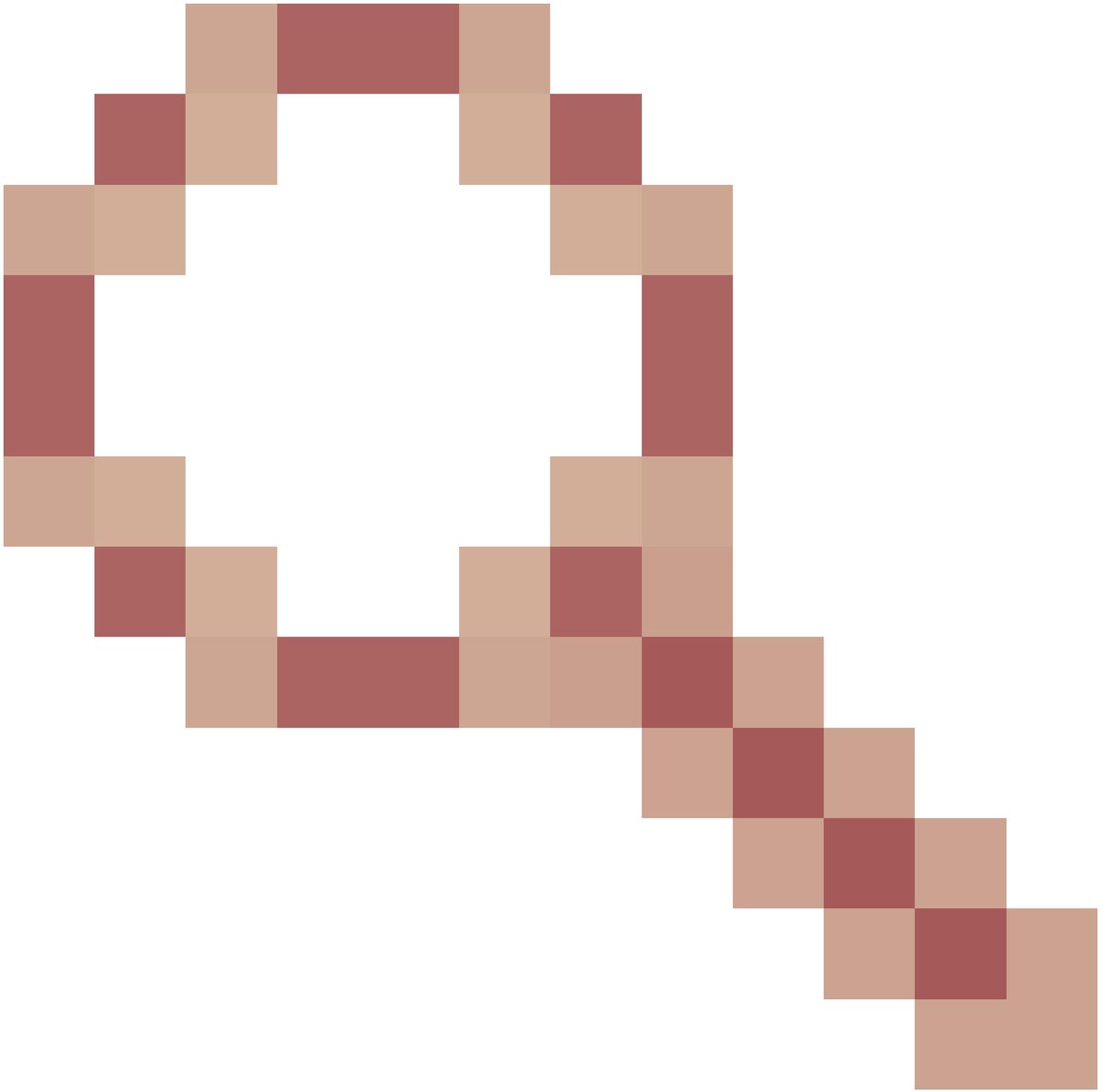
문제 11. ASDM Webvpn DAP 구성이 없습니다.

ASDM AAA Attributes(RADIUS/LDAP) 특성의 DAP 컨피그레이션에서 = 및 !=(드롭다운)만 볼 수 없습니다.

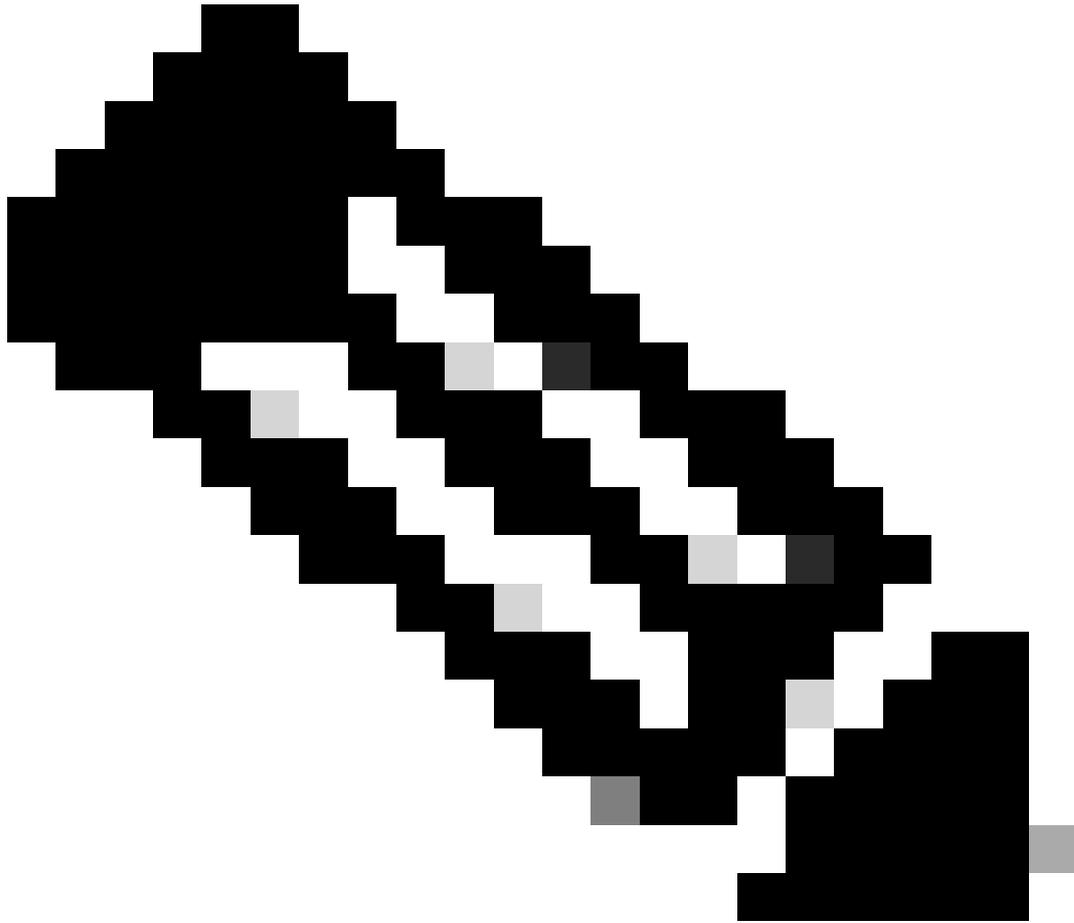


문제 해결 - 권장 단계

이는 Cisco 버그 ID CSCwa에서 추적한 소프트웨어 [결함입니다99370](#)



ASDM:DAP 구성에 AAA 특성 유형(Radius/LDAP)이 없습니다.

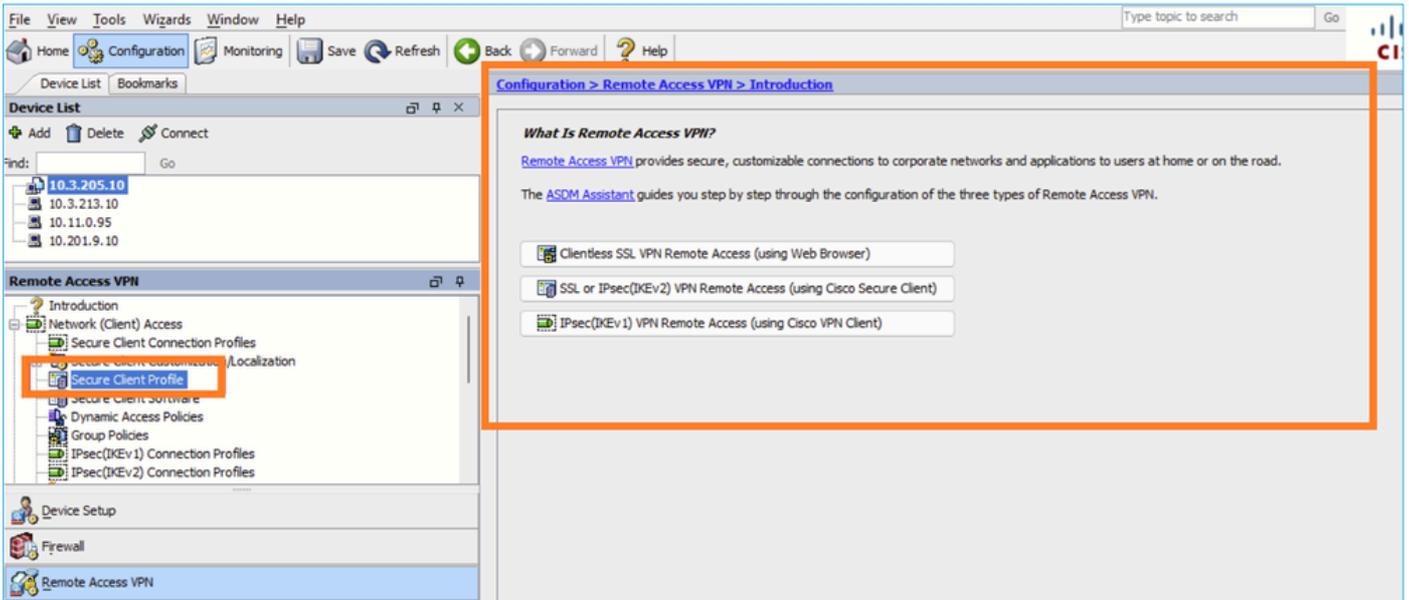


참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

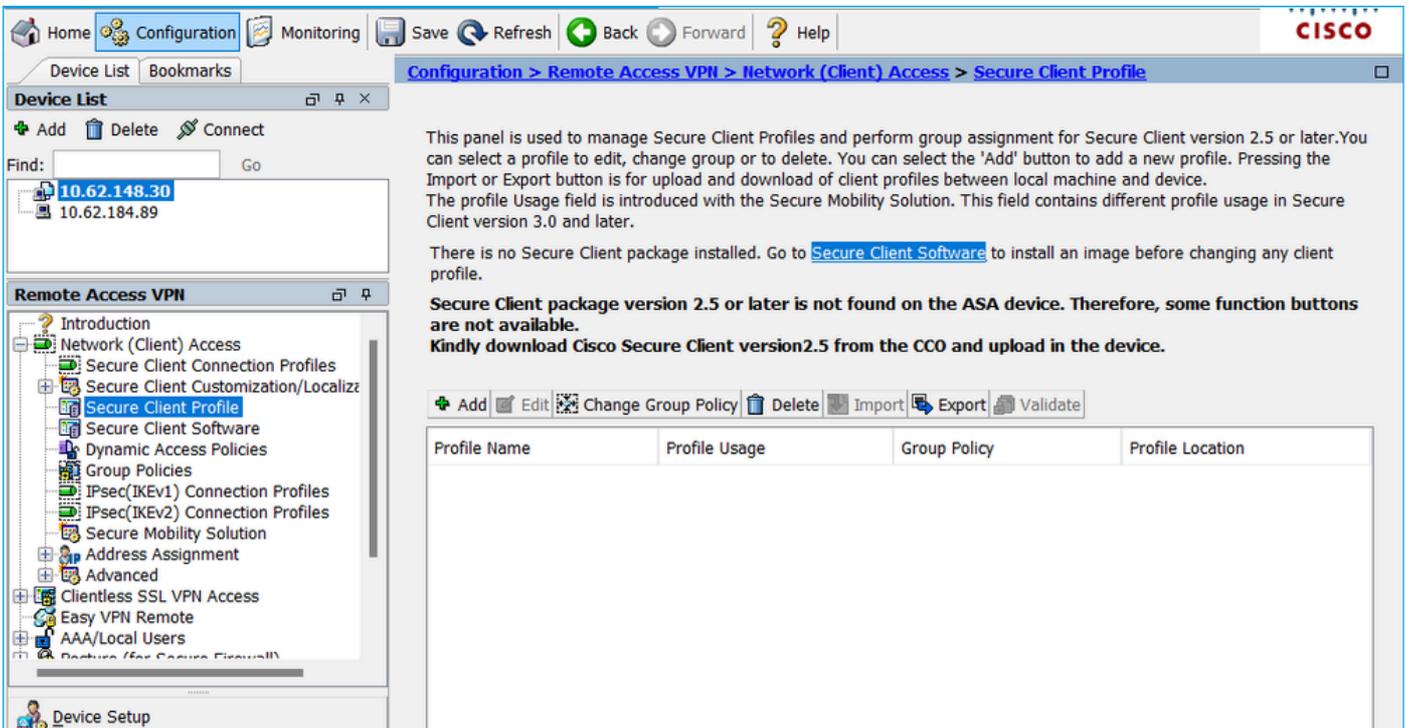
ASDM 기타 문제 해결

문제 1. ASDM에서 보안 클라이언트 프로파일에 액세스할 수 없습니다.

ASDM UI에는 다음 항목이 표시됩니다.



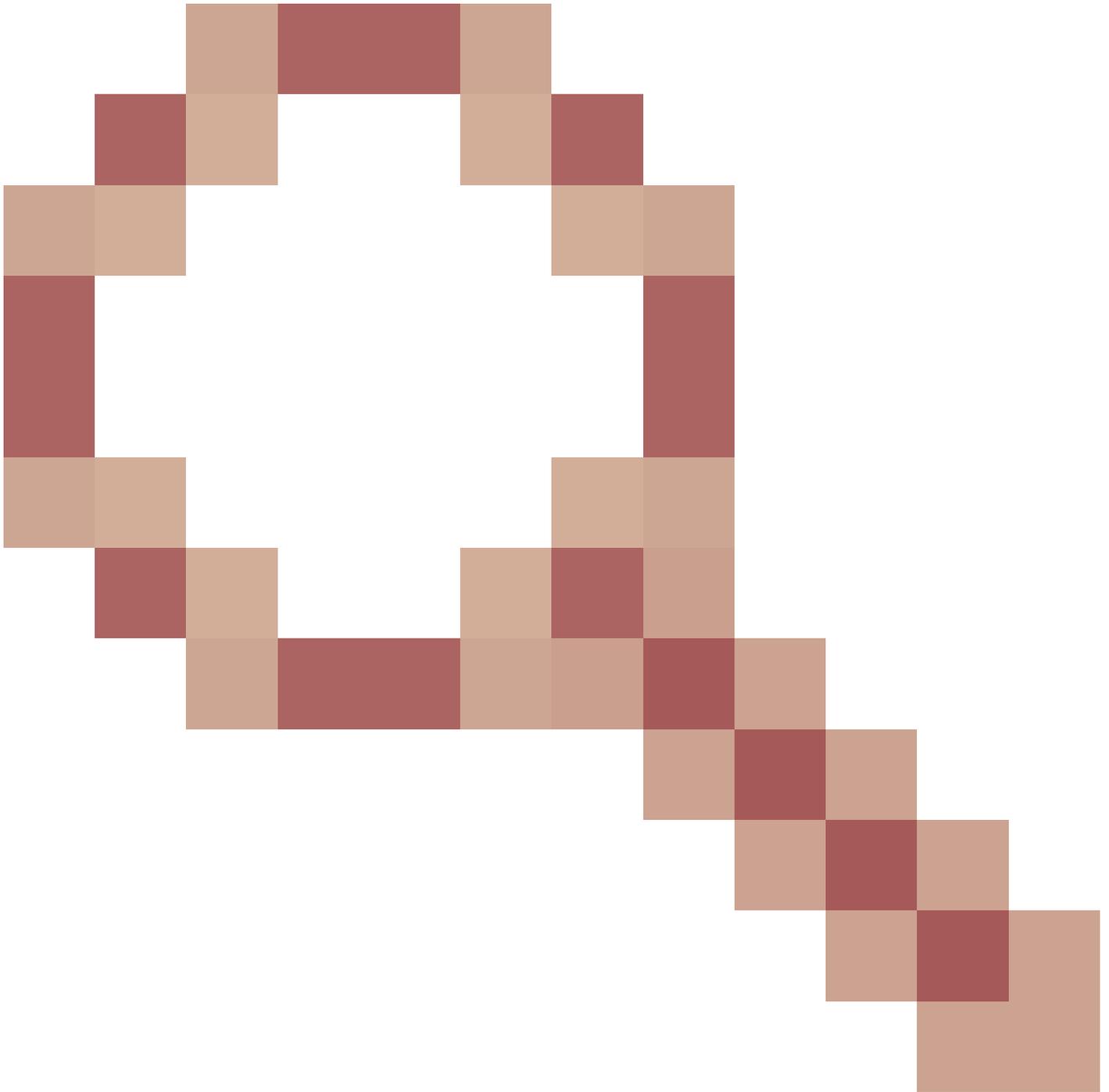
필요한 UI 출력은 다음과 같습니다.



문제 해결 - 권장 단계

이는 알려진 결함입니다.

Cisco 버그 ID [CSCwi56155](#)



ASDM에서 보안 클라이언트 프로파일에 액세스할 수 없음

해결 방법:

AnyConnect 다운그레이드

또는

ASDM을 버전 7.20.2로 업그레이드

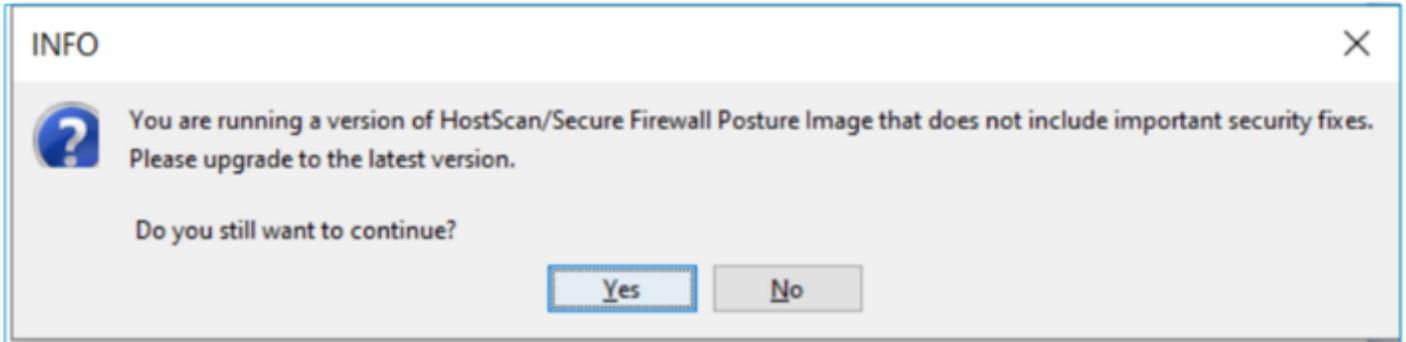
자세한 내용은 결함 노트를 참조하십시오. 또한, 당사는 결함을 구독할 수 있으므로 당사는 결함 업데이트에 대한 알림을 받을 수 있습니다.

문제 2. ASDM에서 hostscan 팝업을 표시합니다. 이미지에 중요한 보안 수정 사항이

포함되어 있지 않습니다.

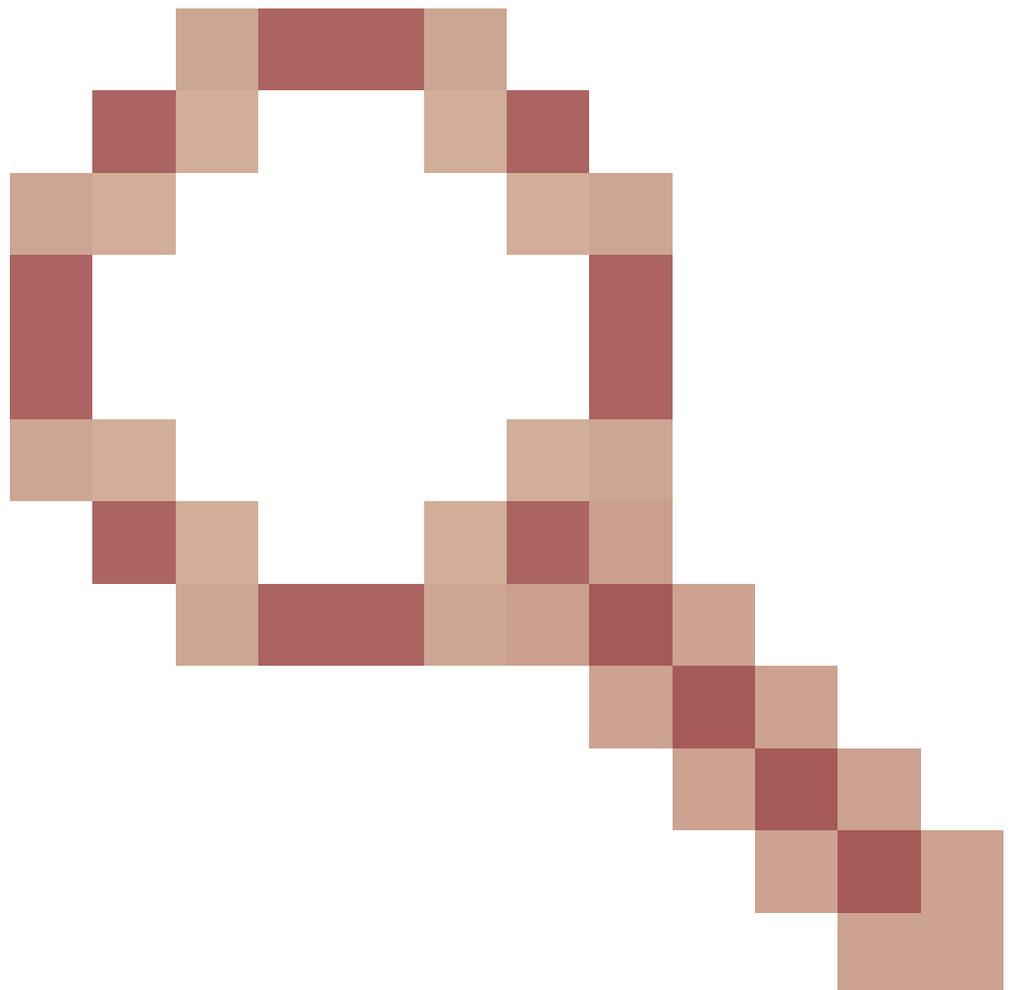
ASDM UI에는 다음이 표시됩니다.

"중요한 보안 수정 사항이 포함되지 않은 버전의 HostScan/SecureFirewall Posture 이미지를 실행하고 있습니다. 최신 버전으로 업그레이드하십시오. 계속하시겠습니까?"



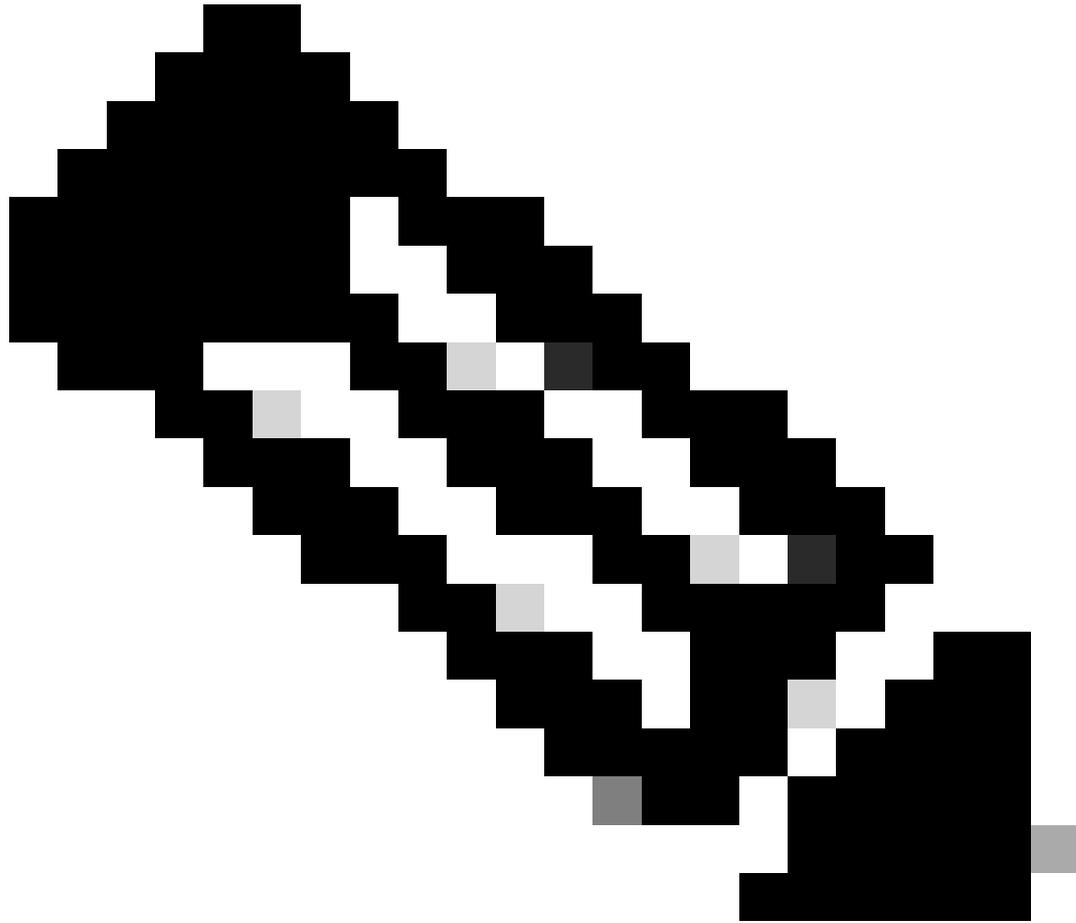
문제 해결 - 권장 단계

이는 알려진 결함입니다.



Cisco 버그 ID CSCwc[62461](#)

hostscan을 위해 ASDM 팝업에 로그인할 때 이미지에 중요한 보안 수정 사항이 포함되지 않습니다.



참고: 이 결함은 최근 ASDM 소프트웨어 릴리스에서 수정되었습니다. 자세한 내용은 결함 세부사항을 확인하십시오.

해결 방법:

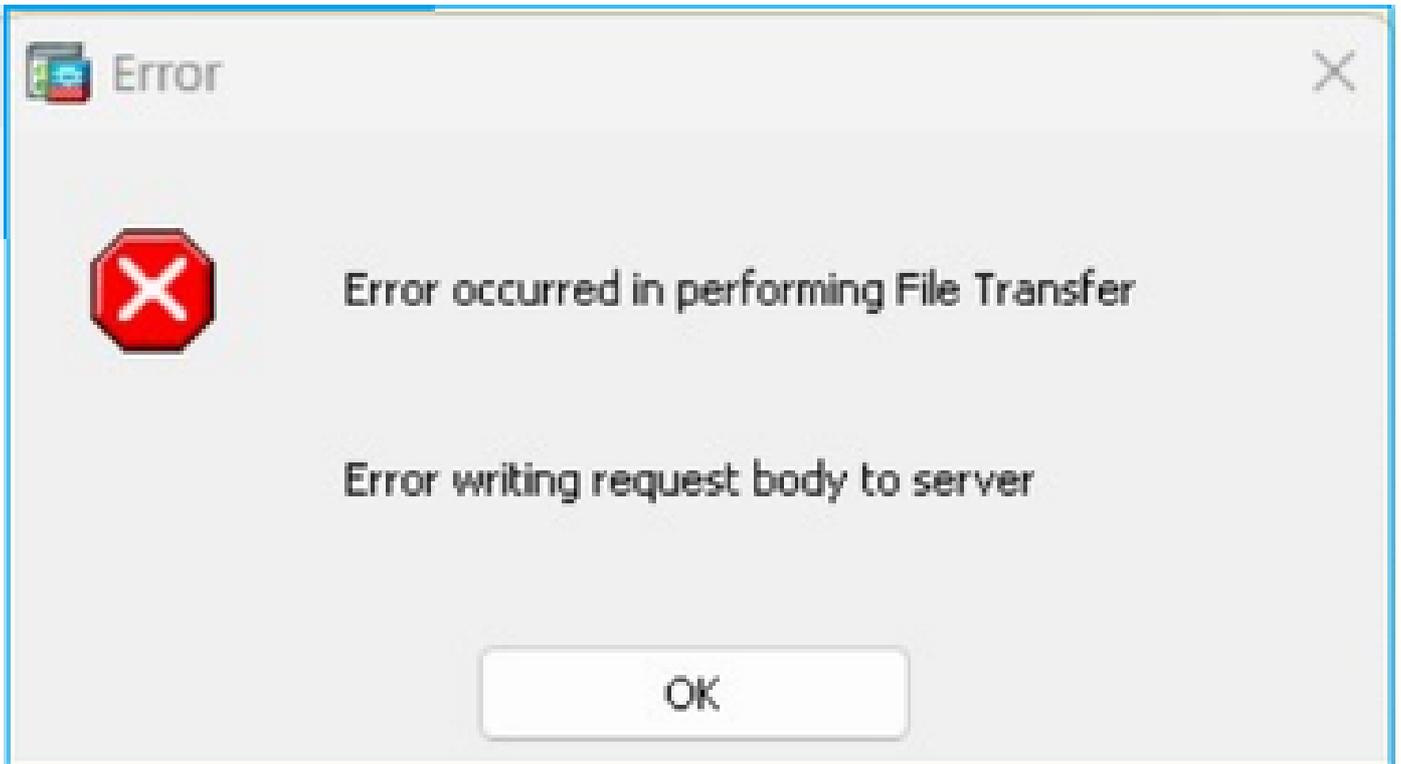
계속하려면 팝업 메시지 상자에서 '예'를 클릭하십시오.

문제 3. ASDM을 통해 이미지를 복사할 때 ASDM "서버에 요청 본문을 쓰는 중 오류"

ASDM UI에는 다음이 표시됩니다.

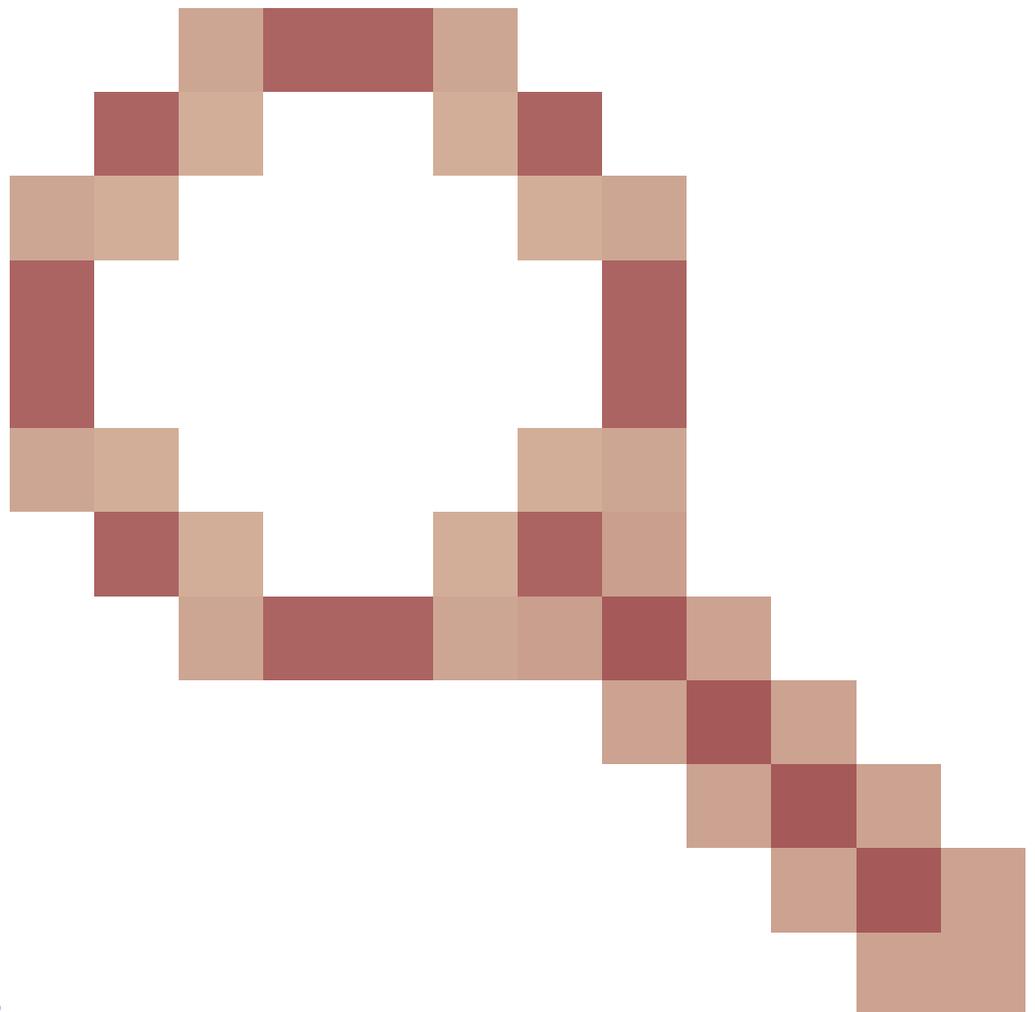
파일 전송을 수행하는 동안 오류가 발생했습니다.

서버에 요청 본문을 쓰는 동안 오류가 발생했습니다.



문제 해결 - 권장 조치

이는 알려진 결함으로 추적됩니다.



이미지를 복사할 때 ASDM "요청 본문을 서버에 쓰는 중 오류"

해결 방법

SCP/TFTP를 사용하여 파일을 전송합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.