

ASDM에서 ASA 연결 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제 해결 방법론](#)

[ASA 컨피그레이션](#)

[플래시의 ASDM 이미지](#)

[사용 중인 ASDM 이미지](#)

[HTTP 서버 제한](#)

[기타 가능한 컨피그레이션 문제](#)

[네트워크 연결](#)

[애플리케이션 소프트웨어](#)

[HTTPS로 명령 실행](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ASA with Cisco ASDM에 액세스/구성할 때 발생하는 문제를 검토하는 데 필요한 트러블슈팅 방법론에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 나열된 시나리오, 증상 및 단계는 ASA(Adaptive Security Appliance)에서 초기 컨피그레이션을 설정한 후 문제 해결을 위해 작성되었습니다. 초기 컨피그레이션에 대해서는 Cisco ASA Series General Operations ASDM(Adaptive Security Device Manager) 컨피그레이션 가이드, 7.1의 Configuring ASDM [Access for Appliances](#) 섹션을 참조하십시오.

이 문서에서는 트러블슈팅을 위해 ASA CLI를 사용하며, 이를 위해서는 ASA에 대한 SSH(Secure Shell)/텔넷/콘솔 액세스가 필요합니다.

사용되는 구성 요소

이 문서의 정보는 ASA 및 ASDM을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ASDM은 그래픽 관리 인터페이스를 통해 보안 어플라이언스에 대한 보안 관리 및 모니터링 서비스를 제공합니다.

문제 해결 방법론

이 트러블슈팅 문서에는 세 가지 주요 장애 포인트가 있습니다. 이 주문에서 일반적인 트러블슈팅 프로세스를 준수하는 경우 이 문서를 통해 ASDM 사용/액세스와 관련된 정확한 문제를 확인할 수 있습니다.

- ASA 컨피그레이션
- 네트워크 연결
- 애플리케이션 소프트웨어

ASA 컨피그레이션

ASDM에 성공적으로 액세스하기 위해 ASA에 필요한 세 가지 필수 컨피그레이션이 있습니다.

- 플래시의 ASDM 이미지
- 사용 중인 ASDM 이미지
- HTTP 서버 제한

플래시의 ASDM 이미지

필요한 버전의 ASDM이 플래시에 업로드되었는지 확인합니다. 현재 실행 중인 버전의 ASDM이나 ASA로의 기타 일반적인 파일 전송 방법(예: TFTP)으로 업로드할 수 있습니다.

ASA 플래시 메모리에 있는 파일을 나열하는 데 도움이 되도록 ASA CLI에 show flash를 입력합니다. ASDM 파일이 있는지 확인합니다.

```
<#root>
```

```
ciscoasa#
```

```
show flash
```

```
--#--  --length--  -----date/time-----  path
249  76267      Feb 28 2013 19:58:18  startup-config.cfg
250  4096        May 12 2013 20:26:12  sdesktop
251  15243264    May 08 2013 21:59:10  asa823-k8.bin
252  25196544    Mar 11 2013 22:43:40  asa845-k8.bin
253  17738924    Mar 28 2013 00:12:12  asdm-702.bin      ---- ASDM Image
```

플래시에 있는 이미지가 유효하고 손상되지 않았는지 추가로 확인하려면 verify 명령을 사용하여 소프트웨어 패키지에 저장된 MD5 해시와 존재하는 실제 파일의 MD5 해시를 비교할 수 있습니다.

```
<#root>
```

```
ciscoasa#
```

```
verify flash:/asdm-702.bin
```

```
Verifying file integrity of disk0:/asdm-702.bin  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
Done!  
Embedded Hash MD5: e441a5723505b8753624243c03a40980  
Computed Hash MD5: e441a5723505b8753624243c03a40980  
CCO Hash MD5: c305760ec1b7f19d910c4ea5fa7d1cf1  
Signature Verified  
Verified disk0:/asdm-702.bin
```

이 단계는 이미지가 ASA에 있는지 여부와 이미지의 무결성을 확인하는 데 도움이 될 수 있습니다.

사용 중인 ASDM 이미지

이 프로세스는 ASA의 ASDM 컨피그레이션에 정의되어 있습니다. 사용되는 현재 이미지의 샘플 컨피그레이션 정의는 다음과 같습니다.

```
asdm 이미지 disk0:/asdm-702.bin
```

추가로 확인하려면 show asdm image 명령을 사용할 수도 있습니다.

```
<#root>
```

```
ciscoasa# s
```

```
how asdm image
```

```
Device Manager image file, disk0:/asdm-702.bin
```

HTTP 서버 제한

이 단계는 ASDM 컨피그레이션에서 필수적입니다. 어떤 네트워크에서 ASA에 액세스할 수 있는지 정의되기 때문입니다. 샘플 컨피그레이션은 다음과 같습니다.

```
http server enable  
http 192.168.1.0 255.255.255.0 inside  
  
http 10.0.0.1 255.0.0.0 outside
```

이전 컨피그레이션에 필요한 네트워크가 정의되어 있는지 확인합니다. 이러한 정의가 없으면

ASDM Launcher가 연결되는 동안 시간이 초과되며 다음 오류가 발생합니다.



ASDM 시작 페이지(<https://<ASA IP address>/admin>)에서는 요청이 시간 초과되고 아무 페이지도 표시되지 않습니다.

HTTP 서버가 ASDM 연결에 비표준 포트(예: 8443)를 사용하는지 추가로 확인합니다. 이는 컨피그레이션에서 강조 표시됩니다.

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

비표준 포트를 사용하는 경우 ASDM 시작 관리자에서 ASA에 연결할 때 포트를 다음과 같이 지정해야 합니다.

Device IP Address / Name: 10.106.36.132:8443

Username: cisco

Password: [REDACTED]

이는 ASDM 시작 페이지(<https://10.106.36.132:8443/admin>)에 액세스하는 경우에도 적용됩니다.

기타 가능한 컨피그레이션 문제

이전 단계를 완료한 후 모든 것이 클라이언트 측에서 작동하는 경우 ASDM을 열 수 있습니다. 그러나 여전히 문제가 발생하면 다른 시스템에서 ASDM을 엽니다. 성공하면 애플리케이션 레벨에서 문제가 발생할 수 있으며 ASA 컨피그레이션도 괜찮습니다. 그러나 여전히 시작되지 않으면 다음 단계를 완료하여 ASA 측 컨피그레이션을 추가로 확인합니다.

1. ASA에서 SSL(Secure Sockets Layer) 컨피그레이션을 확인합니다. ASDM은 ASA와 통신하는 동안 SSL을 사용합니다. ASDM이 시작되는 방식에 따라, 최신 OS 소프트웨어는 SSL 세션을 협상할 때 더 약한 암호를 사용하도록 허용할 수 없습니다. ASA에서 어떤 암호가 허용되는지 확인하고, `show run all ssl` 명령을 사용하여 특정 SSL 버전이 컨피그레이션에 지정된 경우 다음을 수행합니다.

```
<#root>
```

```
ciscoasa#
```

```
show run all ssl
```

```
ssl server-version any <--- Check SSL Version restriction configured on the ASA
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1 <--- Check SSL ciphers
permitted on the ASA
```

ASDM이 실행되는 동안 SSL 암호 협상 오류가 발생하면 ASA 로그에 다음과 같이 표시됩니다.

```
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason:
no shared cipher
%ASA-6-302014: Teardown TCP connection 3 for mgmt:10.103.236.189/52501 to
identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
```


특정 설정이 표시되면 기본값으로 되돌립니다. 컨피그레이션에서 ASA에서 3DES 및 AES 암호

호를 사용하려면 ASA에서 VPN-3DES-AES 라이선스를 활성화해야 합니다. 이는 CLI의 show version 명령으로 확인할 수 있습니다. 출력은 다음과 같이 표시됩니다.

```
<#root>
ciscoasa#
show version

Hardware:   ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 32MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
<snip>
Failover           : Active/Active
VPN-DES            : Enabled
VPN-3DES-AES      : Enabled
<snip>
```

VPN-3DES-AES 라이선스는 [Cisco 라이선싱 웹 사이트](#)에서 비용 없이 얻을 수 [있습니다](#). Security Products(보안 제품)를 클릭한 다음 Cisco ASA 3DES/AES License(Cisco ASA 3DES/AES 라이선스)를 선택합니다.

 참고: 8.6/9.x 코드와 함께 제공되는 새 ASA 5500-X 플랫폼에서 SSL 암호 설정은 기본적으로 des-sha1로 설정되므로 ASDM 세션이 작동하지 않습니다. 자세한 내용은 [ASA 5500-x: ASDM 및 기타 SSL 기능은 기본 제공](#) 문서인 ASDM을 참조하십시오.

- ASA에서 WebVPN이 활성화되어 있는지 확인합니다. 활성화된 경우 ASDM 웹 시작 페이지에 액세스할 때 이 URL(<https://10.106.36.132/admin>)을 사용하여 액세스해야 합니다.
- 포트 443에 대해 ASA에서 NAT(Network Address Translation) 컨피그레이션을 확인합니다. 그러면 ASA에서 ASDM에 대한 요청을 처리하지 않고 NAT가 구성된 네트워크/인터페이스로 전송합니다.
- 모든 것이 확인되었지만 ASDM이 계속 시간 초과되는 경우 ASA CLI에서 show asp table socket 명령을 사용하여 ASDM에 대해 정의된 포트에서 수신 대기하도록 ASA가 설정되었는지 확인합니다. 출력은 ASA가 ASDM 포트에서 수신 대기함을 보여줍니다.

Protocol	Socket	Local Address	Foreign Address	State
SSL	0001b91f	10.106.36.132:443	0.0.0.0:*	LISTEN

이 출력이 표시되지 않으면 ASA 소프트웨어에서 소켓을 재설정하기 위해 ASA에서 HTTP 서버 컨피그레이션을 제거하고 다시 적용합니다.

- ASDM에 로그인/인증할 때 문제가 발생하면 HTTP에 대한 인증 옵션이 올바르게 설정되었는지 확인합니다. 어떤 인증 명령도 설정되지 않은 경우 ASA enable 비밀번호를 사용하여 ASDM에 로그인할 수 있습니다. 사용자 이름/비밀번호 기반 인증을 활성화하려는 경우 ASA의 사용자 이름/비밀번호 데이터베이스에서 ASA에 대한 ASDM/HTTP 세션을 인증하려면 이 컨피그레이션을 입력해야 합니다.

```
<#root>
```

```
aaa authentication http console LOCAL
```

이전 명령을 활성화할 때 사용자 이름/비밀번호를 생성해야 합니다.

```
username <username> password <password> priv <Priv level>
```

이러한 단계가 도움이 되지 않을 경우 추가 조사를 위해 ASA에서 이러한 디버그 옵션을 사용할 수 있습니다.

```
debug http 255  
debug asdm history 255
```

네트워크 연결

이전 섹션을 완료했지만 여전히 ASDM에 액세스할 수 없는 경우, 다음 단계는 ASDM에 액세스하려는 머신에서 ASA에 대한 네트워크 연결을 확인하는 것입니다. ASA가 클라이언트 머신에서 요청을 수신하는지 확인하기 위한 몇 가지 기본 문제 해결 단계가 있습니다.

1. ICMP(Internet Control Message Protocol)로 테스트합니다.

ASDM에 액세스하려는 ASA 인터페이스를 ping합니다. ICMP가 네트워크를 통과하도록 허용되고 ASA 인터페이스 레벨에 제한이 없는 경우 ping에 성공할 수 있습니다. ping이 실패하면 ASA와 클라이언트 머신 간에 통신 문제가 있기 때문일 수 있습니다. 그러나 이러한 유형의 통신 문제가 있다고 판단하는 결정적인 단계는 아닙니다.

2. 패킷 캡처를 확인합니다.

ASDM에 액세스하려는 인터페이스에 패킷 캡처를 배치합니다. 캡처는 인터페이스 IP 주소로 향하는 TCP 패킷이 목적지 포트 번호 443(기본값)을 사용하여 도착함을 표시할 수 있습니다.

캡처를 구성하려면 다음 명령을 사용합니다.

```
<#root>
```

```
capture asdm_test interface
```

```
match tcp host
```

```
eq 443 host
```

```
For example, cap asdm_test interface mgmt match tcp host 10.106.36.132  
eq 443 host 10.106.36.13
```

이는 ASDM에 연결하는 ASA 인터페이스의 포트 443에 대해 오는 모든 TCP 트래픽을 캡처합니다. 이때 ASDM을 통해 연결하거나 ASDM 웹 시작 페이지를 엽니다. 그런 다음 show capture asdm_test 명령을 사용하여 캡처된 패킷의 결과를 봅니다.

```
<#root>
```

```
ciscoasa#
```

```
show capture asdm_test
```

```
Three packets captured
```

```
1: 21:38:11.658855 10.106.36.13.54604 > 10.106.36.132.443:  
S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>  
  
2: 21:38:14.659252 10.106.36.13.54604 > 10.106.36.132.443:  
S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>  
  
3: 21:38:20.662166 10.106.36.13.54604 > 10.106.36.132.443:  
S 807913260:807913260(0) win 8192 <mss 1260,nop,nop,sackOK>
```

이 캡처는 클라이언트 머신에서 ASA로의 동기화(SYN) 요청을 표시하지만 ASA는 응답을 보내지 않습니다. 이전 캡처와 유사한 캡처가 표시되는 경우 패킷이 ASA에 도달하지만 ASA가 이러한 요청에 응답하지 않으므로 문제가 ASA 자체로 격리됩니다. 추가 트러블슈팅을 하려면 이 문서의 첫 번째 섹션을 참조하십시오.

그러나 이전과 유사한 출력이 표시되지 않고 패킷이 캡처되지 않으면 ASA와 ASDM 클라이언트 시스템 간에 연결 문제가 있음을 의미합니다. TCP 포트 443 트래픽을 차단할 수 있는 중간 디바이스가 없는지, 그리고 트래픽이 ASA에 도달하지 못하게 할 수 있는 브라우저 설정(예: 프록시 설정)이 없는지 확인합니다.

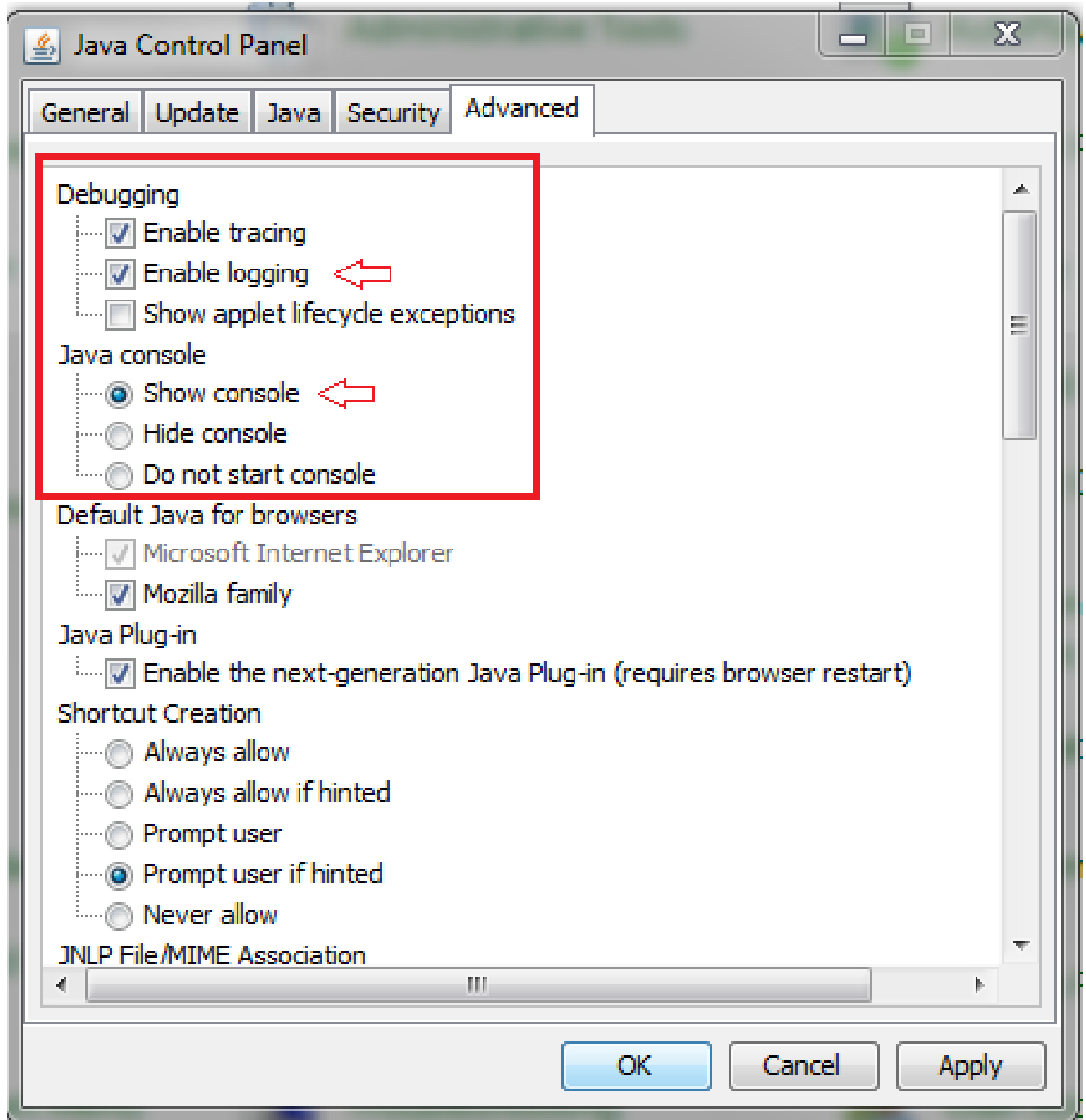
일반적으로 패킷 캡처는 ASA에 대한 경로가 분명한지, 그리고 네트워크 연결 문제를 배제하기 위해 추가 진단이 필요하지 않은지 확인할 수 있는 좋은 방법입니다.

애플리케이션 소프트웨어

이 섹션에서는 클라이언트 머신에 설치된 ASDM 시작 관리자 소프트웨어가 시작/로드에 실패하는 경우 문제를 해결하는 방법에 대해 설명합니다. ASDM Launcher는 클라이언트 시스템에 상주하며 ASDM 이미지를 검색하기 위해 ASA에 연결되는 구성 요소입니다. 검색된 ASDM 이미지는 일반적으로 캐시에 저장되며, ASDM 이미지 업데이트와 같이 ASA 측에서 변경 사항이 발견될 때까지 캐시에서 가져옵니다.

클라이언트 머신에서 문제를 배제하려면 다음 기본 문제 해결 단계를 완료하십시오.

1. 다른 시스템에서 ASDM 시작 페이지를 엽니다. 클라이언트 머신이 시작되면 문제가 해당 클라이언트 머신에 있음을 의미합니다. 장애가 발생하면 처음부터 문제 해결 가이드를 사용하여 관련 구성 요소를 순서대로 격리합니다.
2. 웹 실행을 통해 ASDM을 열고 바로 소프트웨어를 실행합니다. 성공하면 ASDM Launcher 설치에 문제가 있을 수 있습니다. 클라이언트 시스템에서 ASDM 시작 프로그램을 제거하고 ASA 웹 시작 프로그램 자체에서 다시 설치합니다.
3. 사용자의 홈 디렉토리에서 ASDM의 캐시 디렉토리를 지웁니다. 전체 캐시 디렉토리를 삭제하면 캐시가 지워집니다. ASDM이 성공적으로 시작되면 ASDM File 메뉴 내에서 캐시를 지울 수도 있습니다.
4. 올바른 Java 버전이 설치되어 있는지 확인합니다. [Cisco ASDM Release Notes](#)에는 테스트된 Java 버전에 대한 요구 사항이 나열되어 있습니다.
5. Java 캐시를 지웁니다. Java 제어판에서 General(일반) > Temporary Internet File(임시 인터넷 파일)을 선택합니다. 그런 다음 View를 클릭하여 Java Cache Viewer를 실행합니다. ASDM을 참조하거나 ASDM과 관련된 모든 항목을 삭제합니다.
6. 이 단계가 실패할 경우 추가 조사를 위해 클라이언트 머신에서 디버깅 정보를 수집합니다. URL <https://<ASA의 IP 주소>?debug=5>를 사용하여 ASDM에 대한 디버깅을 활성화합니다(예: <https://10.0.0.1?debug=5>).
Java 버전 6(버전 1.6이라고도 함)에서는 Java Control Panel(Java 제어판) > Advanced(고급)에서 Java 디버깅 메시지가 활성화됩니다. 그런 다음 Debugging(디버깅) 아래의 확인란을 선택합니다. Java 콘솔 아래에서 Do not start console을 선택하지 마십시오. ASDM을 시작하기 전에 Java 디버깅을 활성화해야 합니다.



Java 콘솔 출력은 사용자 홈 디렉토리의 .asdm/log 디렉토리에 기록됩니다. ASDM 로그는 동일한 디렉토리에서도 찾을 수 있습니다.

HTTPS로 명령 실행

이 절차를 통해 HTTP 채널에 대한 모든 레이어 7 문제를 확인할 수 있습니다. 이 정보는 ASDM 애플리케이션 자체에 액세스할 수 없고 디바이스를 관리하는 데 사용할 수 있는 CLI 액세스가 없는 경우에 유용합니다.

ASDM 웹 시작 페이지에 액세스하는 데 사용되는 URL을 사용하여 ASA에서 컨피그레이션 레벨 명령을 실행할 수도 있습니다. 이 URL은 ASA에 대한 기본 레벨에서 컨피그레이션을 변경하는 데 사용할 수 있으며, 여기에는 원격 디바이스 재로드가 포함됩니다. 명령을 입력하려면 다음 구문을 사

용합니다.

https://<ASA>/admin/exec/<command>의 IP 주소

명령에 공백이 있고 브라우저가 URL의 공백 문자를 구문 분석할 수 없는 경우 + 기호 또는 %20을 사용하여 공백을 나타낼 수 있습니다.

예를 들어 [https://10.106.36.137/admin/exec/show ver](https://10.106.36.137/admin/exec/show%20ver) 를 입력하면 브라우저에 show version 출력이 표시됩니다.



```
Cisco Adaptive Security Appliance Software Version 8.4(3)

Compiled on Fri 06-Jan-12 10:24 by builders
System image file is "disk0:/asa843-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 4 mins 41 secs

Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
Boot microcode : CN1000-MC-BOOT-2.00
SSL/IKE microcode : CNLite-MC-SSLM-PLUS-2.03
IPSec microcode : CNLite-MC-IPSECM-MAIN-2.06
Number of accelerators: 1

0: Int: Internal-Data0/0 : address is d0d0.fd0f.902d, irq 11
1: Ext: Ethernet0/0 : address is d0d0.fd0f.9025, irq 255
2: Ext: Ethernet0/1 : address is d0d0.fd0f.9026, irq 255
3: Ext: Ethernet0/2 : address is d0d0.fd0f.9027, irq 255
4: Ext: Ethernet0/3 : address is d0d0.fd0f.9028, irq 255
5: Ext: Ethernet0/4 : address is d0d0.fd0f.9029, irq 255
6: Ext: Ethernet0/5 : address is d0d0.fd0f.902a, irq 255
7: Ext: Ethernet0/6 : address is d0d0.fd0f.902b, irq 255
8: Ext: Ethernet0/7 : address is d0d0.fd0f.902c, irq 255
9: Int: Internal-Data0/1 : address is 0000.0003.0002, irq 255
10: Int: Not used : irq 255
11: Int: Not used : irq 255

Licensed features for this platform:
Maximum Physical Interfaces : 8 perpetual
VLANs : 3 DMZ Unrestricted
Dual ISPs : Enabled perpetual
VLAN Trunk Ports : 8 perpetual
```

이 명령 실행 방법을 사용하려면 HTTP 서버가 ASA에서 활성화되어 있어야 하며 필요한 HTTP 제한이 활성화되어 있어야 합니다. 그러나 ASA에 ASDM 이미지가 있을 필요는 없습니다.

관련 정보

- [어플라이언스에 대한 ASDM 액세스 구성](#)

- [ASA 5500-x: ASDM 및 기타 SSL 기능이 즉시 작동하지 않음](#)
- [Cisco ASDM 릴리스 정보](#)
- [ASA에서 3DES/AES 라이선스를 얻기 위한 Cisco License 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.