

firepower 시스템에서 관리자 사용자의 비밀번호 재설정

목차

[소개](#)

[배경 정보](#)

[Firepower 위협 방어: 관리자 비밀번호 재설정](#)

[ASA Firepower 서비스 모듈: 관리자 비밀번호 재설정](#)

[ASA 5512-X~ASA 5555-X 및 ASA 5506-X~ASA 5516-X\(소프트웨어 ASA Firepower 모듈\) 및 ISA 3000 디바이스에서 관리자 비밀번호를 재설정합니다](#)

[ASA 5585-X Series 디바이스\(하드웨어 ASA Firepower 모듈\)에서 관리자 비밀번호 재설정](#)

[FMC 및 NGIPSv에 대한 CLI 또는 셸 관리자 비밀번호 변경](#)

[FMC의 웹 인터페이스 관리자 비밀번호 또는 7000 및 8000 Series 디바이스의 웹 인터페이스 관리자 및 CLI 관리자 비밀번호를 변경합니다](#)

[FMC 또는 NGIPSv에 대해 손실된 CLI 또는 셸 관리자 비밀번호를 재설정하거나 7000 및 8000 Series 디바이스에 대해 손실된 웹 인터페이스 또는 CLI 비밀번호를 재설정합니다](#)

[옵션 1. 안전하게 디바이스를 재부팅하고 부팅 시 단일 사용자 모드로 전환하여 비밀번호를 재설정합니다](#)

[옵션 2. 외부 인증을 사용하여 CLI에 액세스하여 Firepower Management Center의 비밀번호 재설정](#)

[firepower Management Center에 대해 손실된 웹 인터페이스 관리자 비밀번호 재설정](#)

kWh


소개

이 문서에서는 Firepower 시스템에서 관리자 계정의 비밀번호를 재설정하는 지침 단계에 대해 설명합니다.

배경 정보

FMC(Firepower 관리 센터)는 CLI(Command Line Interface)/셸 액세스 및 웹 인터페이스 액세스(사용 가능한 경우)를 위해 서로 다른 관리자 계정(별도의 비밀번호 사용)을 제공합니다. firepower 및 ASA(Adaptive Security Appliance) Firepower 서비스 어플라이언스와 같은 관리되는 디바이스의 관리자 계정은 CLI 액세스, 셸 액세스 및 웹 인터페이스 액세스(사용 가능한 경우)에 대해 동일합니다.

이러한 지침은 Firepower Management Center를 인용합니다.

 참고: Firepower Management Center CLI에 대한 참조는 버전 6.3 이상에만 적용됩니다. 7000 및 8000 Series 디바이스는 버전 6.4를 통해 지원됩니다.

Firepower 위협 방어: 관리자 비밀번호 재설정

Firepower 9300 및 4100 플랫폼에서 FTD(Firepower Threat Defense) 논리적 디바이스의 손실된 관리자 비밀번호를 재설정하려면 FXOS [Chassis Manager 설명서](#)를 통해 [FTD용 비밀번호 변경 또는 복구의 지침](#)을 수행합니다.

firepower 1000/2100/3100에서 실행되는 FTD 디바이스의 경우 디바이스를 다시 이미지해야 합니다. 이러한 플랫폼에서 [이미지로 다시 설치 절차에 대한 Firepower 위협 방어를 실행하는 Firepower 1000/2100 Series](#)에 대한 [Cisco FXOS 문제 해결](#) 가이드를 참조하십시오.


ASA 5500-X 및 ISA(Integrated Security Appliance) 3000 모델에서 실행되는 FTD 디바이스의 경우 디바이스를 리이미징해야 합니다. 지침은 [Cisco ASA 및 Firepower Threat Defense 디바이스 재이미징 가이드](#)를 참조하십시오.

가상 FTD 디바이스의 경우 디바이스를 새 구축으로 교체해야 합니다.

물리적 디바이스의 이미지로 다시 설치할 경우 컨피그레이션이 지워지고 관리자 비밀번호가 다음으로 재설정됩니다. Admin123.

AWS(Amazon Web Services)에서 Firepower 7.0 이상을 사용하는 FTDv를 제외하고, 새 FTDv 구축에는 컨피그레이션이 없으며 관리자 비밀번호는 다음과 같습니다. Admin123. AWS에서 Firepower 7.0 이상을 사용하는 FTDv의 경우, 새 구축에는 컨피그레이션이 없으며 기본 비밀번호는 없습니다. 구축 시간에 관리자 비밀번호를 제공합니다.

- firepower 장치 관리자로 관리되는 FTD 장치를 다시 이미지화하는 경우:
 - 최근 외부 저장 백업이 있는 경우 이미지로 다시 설치한 후 백업된 컨피그레이션을 복원할 수 있습니다. 자세한 내용은 사용 중인 버전의 [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#)를 참조하십시오.
 - 백업이 없는 경우 인터페이스, 라우팅 정책, DHCP 및 DDNS(Dynamic Domain Name System) 설정을 포함하는 디바이스 컨피그레이션을 수동으로 다시 생성해야 합니다.
- firepower Management Center로 관리되는 FTD 디바이스를 이미지로 다시 설치할 경우, FMC 및 버전 6.3 이상을 실행하는 디바이스를 이미지로 다시 설치하기 전에 FMC 웹 인터페이스를 사용하여 디바이스 컨피그레이션을 백업하고 이미지로 다시 설치한 후에 백업을 복원할 수 있습니다. 자세한 내용은 해당 버전의 [Firepower Management Center 컨피그레이션 가이드](#)를 참조하십시오.

 참고: 버전 6.0.1-6.2.3을 실행하는 경우 FTD 컨피그레이션을 백업할 수 없습니다. 버전 6.3.0 - 6.6.0을 실행하는 경우 FTD 컨테이너 인스턴스에 대해서는 FMC 웹 인터페이스에서 백업 및 복원이 지원되지 않습니다. 리이미징한 후 Firepower Management Center에서 공유 정책을 적용할 수 있지만 인터페이스, 라우팅 정책, DHCP 및 DDNS 설정과 같은 디바이스별 설정을 수동으로 구성해야 합니다.

ASA Firepower 서비스 모듈: 관리자 비밀번호 재설정

ASA 일반 작업 CLI의 session 명령을 사용하여 ASA Firepower 모듈 CLI의 관리자 비밀번호를 재설정할 수 있습니다. ASA CLI의 비밀번호가 손실된 경우 ASA 버전에 대한 CLI [Book 1: Cisco ASA](#)

[Series 일반 작업 CLI 컨피그레이션 가이드](#)에 설명된 대로 비밀번호를 복구할 수 있습니다.

ASA 5512-X~ASA 5555-X 및 ASA 5506-X~ASA 5516-X(소프트웨어 ASA Firepower 모듈) 및 ISA 3000 디바이스에서 관리자 비밀번호를 재설정합니다

ASA Firepower 소프트웨어 모듈 또는 ISA 3000 디바이스의 관리자 사용자를 기본 비밀번호로 재설정하려면 ASA 프롬프트에서 다음 명령을 입력합니다.

```
session sfr do password-reset
```

자세한 내용은 사용 중인 ASA 버전의 [Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI 컨피그레이션](#) 가이드를 참조하십시오.

ASA 5585-X Series 디바이스(하드웨어 ASA Firepower 모듈)에서 관리자 비밀번호 재설정

ASA Firepower 하드웨어 모듈의 admin 사용자를 기본 비밀번호로 재설정하려면 ASA 프롬프트에서 다음 명령을 입력합니다.

```
session 1 do password-reset
```

자세한 내용은 사용 중인 ASA 버전의 [Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI 컨피그레이션](#) 가이드를 참조하십시오.

FMC 및 NGIPSv에 대한 CLI 또는 셸 관리자 비밀번호 변경

다음 지침에 따라 이러한 관리자 계정에 대해 알려진 비밀번호를 재설정합니다.

- Firepower Management Center: CLI 또는 셸에 액세스하는 데 사용되는 관리자 비밀번호입니다.
- NGIPSv(Next Generation Information Preservation System virtual: CLI 액세스에 사용되는 관리자 비밀번호.

절차:

1. SSH 또는 콘솔을 통해 어플라이언스 관리자 계정에 로그인합니다.

- firepower 관리 센터의 경우:
 - firepower Management Center에서 Firepower 버전 6.2 이하를 실행하는 경우 로그인하면 Linux 셸에 직접 액세스할 수 있습니다.
 - firepower Management Center에서 Firepower 버전 6.3 또는 6.4를 실행하고 Firepower Management Center CLI가 활성화되지 않은 경우 로그인하면 Linux 셸에 직접 액세스할 수 있습니다.
 - firepower Management Center에서 Firepower 버전 6.3 또는 6.4를 실행하고 Firepower Management CLI가 활성화된 경우 로그인하여 Firepower Management Center CLI에 액세스할 수 있습니다. expert 명령을 입력하여 Linux 셸에 액세스합니다.
 - firepower Management Center에서 Firepower 버전 6.5 이상을 실행하는 경우 로

그인하여 Firepower Management Center CLI에 액세스할 수 있습니다. expert 명령을 입력하여 Linux 셸에 액세스합니다.

- 관리되는 디바이스의 경우 로그인하면 디바이스 CLI에 액세스할 수 있습니다. expert 명령을 입력하여 Linux 셸에 액세스합니다.
2. 셸 프롬프트에서 다음 명령을 입력합니다. `sudo passwd admin`.
 3. 프롬프트가 표시되면 현재 관리자 비밀번호를 입력하여 권한을 루트 액세스로 높입니다.
 4. 프롬프트에 대한 응답으로 새 관리자 비밀번호를 두 번 입력합니다.



참고: 시스템에 BAD PASSWORD 메시지는 정보 제공용입니다. 이 메시지가 나타나는 경우에도 사용자가 입력한 비밀번호가 적용됩니다. 그러나 보안상의 이유로 더 복잡한 비밀번호를 사용하는 것이 좋습니다.

5. 유형 `exit` 셸을 종료합니다.
6. 관리되는 디바이스 또는 CLI가 활성화된 Firepower 관리 센터에서 `exit` 를 눌러 CLI를 종료합니다.

FMC의 웹 인터페이스 관리자 비밀번호 또는 7000 및 8000 Series 디바이스의 웹 인터페이스 관리자 및 CLI 관리자 비밀번호를 변경합니다

다음 지침에 따라 이러한 관리자 계정에 대해 알려진 비밀번호를 재설정합니다.

- Firepower 관리 센터: 웹 인터페이스에 액세스하는 데 사용되는 관리자 비밀번호입니다.
- 7000 및 8000 Series 디바이스: 웹 인터페이스 및 CLI에 액세스하는 데 사용되는 관리자 비밀번호입니다.

절차:


1. 관리자 액세스 권한이 있는 사용자로 어플라이언스의 웹 인터페이스에 로그인합니다.
2. 선택 `System > Users` 다음을 클릭합니다. `Edit admin` 사용자의 아이콘입니다.
3. 에 대한 값을 입력합니다. `Password` 및 `Confirm Password` 필드.
값은 동일해야 하며 사용자에게 대해 설정된 비밀번호 옵션을 준수해야 합니다.
4. 클릭 `Save`.

FMC 또는 NGIPSv에 대해 손실된 CLI 또는 셸 관리자 비밀번호를 재설정하거나 7000 및 8000 Series 디바이스에 대해 손실된 웹 인터페이스 또는 CLI 비밀번호를 재설정합니다.

다음 지침에 따라 이러한 관리자 계정에 대해 손실된 비밀번호를 재설정합니다.

- Firepower Management Center: CLI 또는 셸에 액세스하는 데 사용되는 관리자 비밀번호입니다.
- 7000 및 8000 Series 디바이스: 웹 인터페이스 및 CLI에 액세스하는 데 사용되는 관리자 비밀번호입니다.

- NGIPSV: CLI 액세스에 사용되는 관리자 비밀번호.

 참고: 이러한 관리자 계정에 대해 손실된 비밀번호를 재설정하려면 어플라이언스와의 콘솔 또는 SSH 연결을 설정해야 합니다(외부 사용자가 구성된 Firepower Management Center의 경우 SSH 연결을 사용할 수 있음). 또한 관리자 자격 증명이 손실된 어플라이언스를 재부팅해야 합니다. 사용 가능한 디바이스 액세스 유형에 따라 다양한 방법으로 리부팅을 시작할 수 있습니다.

- Firepower Management Center의 경우 관리자 액세스 권한이 있는 웹 인터페이스 사용자의 로그인 자격 증명 또는 CLI/셸 액세스 권한이 있는 외부 인증 사용자의 로그인 자격 증명이 필요합니다.
 - 7000 또는 8000 Series 디바이스의 경우 관리자 액세스 권한이 있는 웹 인터페이스 사용자, 구성 액세스 권한이 있는 CLI 사용자 또는 관리 Firepower Management Center에서 관리자 액세스 권한이 있는 사용자 중 하나에 대한 로그인 자격 증명が必要です.
 - NGIPSV의 경우, 구성 액세스 권한이 있는 CLI 사용자 또는 관리 Firepower 관리 센터에서 관리자 액세스 권한이 있는 사용자의 로그인 자격 증명が必要です.
 - Firepower Management Center, 7000 및 8000 Series 디바이스, NGIPSV 디바이스의 경우 콘솔 연결(물리적 또는 원격)이 있는 경우 로그인 자격 증명 없이 이 작업을 수행할 수 있습니다.
- 이러한 방법 중 하나로 디바이스에 액세스할 수 없는 경우, 이러한 지침에 따라 관리자 비밀번호를 재설정할 수 없습니다. Cisco TAC에 문의하십시오.

옵션 1. 안전하게 디바이스를 재부팅하고 부팅 시 단일 사용자 모드로 전환하여 비밀번호를 재설정합니다

1. 관리자 비밀번호가 손실된 디바이스의 어플라이언스 콘솔에 대한 연결을 엽니다.
 - 7000 Series 장치, 8000 Series 장치 및 Firepower Management Center의 경우 키보드/모니터 또는 직렬 연결을 사용합니다.
 - 가상 어플라이언스의 경우 가상 플랫폼에서 제공하는 콘솔을 사용합니다. 자세한 내용은 [Cisco Firepower Management Center 가상 시작 설명서](#) 또는 [Cisco Firepower NGIPSV Quick Start Guide for VMware](#)를 참조하십시오.
 - 또는 Firepower Management Center, 7000 및 8000 Series, 가상 어플라이언스의 경우, 원격 KVM(KeyboardVideo/Mouse)을 사용하여 어플라이언스와 콘솔 연결을 설정한 경우 해당 인터페이스에 액세스할 수 있습니다.
2. 관리자 비밀번호가 손실된 디바이스를 재부팅합니다. 다음 중에서 선택할 수 있습니다.
 - Firepower 관리 센터의 경우:
 - a. 관리자 액세스 권한이 있는 사용자로 Firepower Management Center의 웹 인터페이스에 로그인합니다.
 - b. 해당 버전의 Firepower Management Center 컨피그레이션 가이드에 설명된 대로 [Firepower Management Center](#)를 재부팅합니다.
 - 7000 또는 8000 Series 디바이스 또는 NGIPSV의 경우, 관리 Firepower Management Center에서 관리자 액세스 권한이 있는 웹 인터페이스 사용자에게 대한 자격 증명에 있는 경우:
 - a. 관리자 액세스 권한이 있는 사용자로 관리 Firepower Management Center의 웹 인터페이스에 로그인합니다.
 - b. 사용 중인 버전의 [Firepower Management Center](#) 컨피그레이션 가이드에 설명된 대로 관

리되는 [디바이스](#)를 종료하고 재시작합니다.


· 7000 또는 8000 Series 디바이스의 경우 관리자 액세스 권한이 있는 웹 인터페이스 사용자에게 대한 자격 증명이 있는 경우:


- a. 디바이스의 웹 인터페이스에 관리자 액세스 권한이 있는 사용자로 로그인합니다.
- b. 사용 중인 버전의 [Firepower Management Center 컨피그레이션 가이드](#)에 설명된 대로 디바이스를 재부팅합니다.

· 7000 또는 8000 Series 디바이스 또는 NGIPSv의 경우, 컨피그레이션 액세스 권한이 있는 CLI 사용자에게 대한 자격 증명이 있는 경우:


- a. CLI 컨피그레이션 액세스 권한이 있는 사용자 이름을 통해 셸로 어플라이언스에 로그인합니다.
- b. 프롬프트에서 system reboot 명령을 입력합니다.

· Firepower Management Center, 7000 및 8000 Series, 그리고 콘솔이 있는 가상 어플라이언스의 경우 CTRL-ALT-DEL. (원격 KVM을 사용하는 경우 KVM 인터페이스는 CTRL-ALT-DEL KVM 자체에 대한 간섭 없이 장치에 연결할 수 있습니다.)

 참고: Firepower Management Center 또는 관리되는 디바이스를 재부팅하면 어플라이언스에서 로그아웃되며, 완료하는 데 최대 1시간이 걸릴 수 있는 데이터베이스 검사가 실행됩니다.

 주의: 전원 버튼을 사용하여 어플라이언스를 종료하거나 전원 케이블을 뽑지 마십시오. 시스템 데이터베이스가 손상될 수 있습니다. 웹 인터페이스를 사용하여 어플라이언스를 완전히 종료합니다.

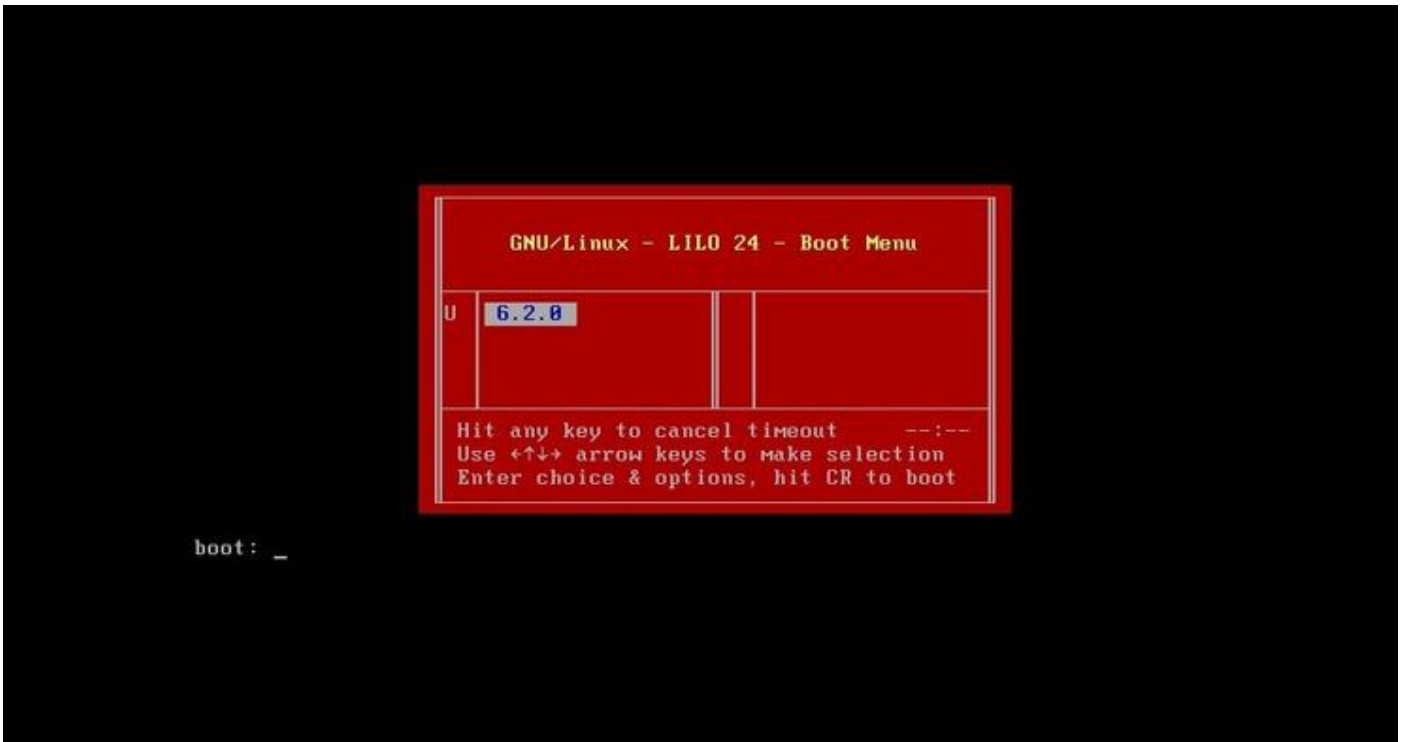
3. 어플라이언스 콘솔 화면에서 재부팅 프로세스를 관찰하고 재부팅되는 어플라이언스 유형에 따라 계속 진행합니다.

 주: 시스템이 데이터베이스 검사를 진행 중인 경우 다음 메시지를 볼 수 있습니다. The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish.

· Firepower Management Center 모델 750, 1500, 2000, 3500, 4000 또는 Firepower 7000, 8000 Series 디바이스 또는 NGIPSv의 경우 재부팅 프로세스를 중단합니다.

a. 어플라이언스가 부팅되기 시작하면 키보드의 아무 키나 눌러 LILO Boot Menu(LILO 부팅 메뉴)에서 카운트다운을 취소합니다.

b. LILO Boot Menu(LILO 부팅 메뉴)에 표시되는 버전 번호를 확인합니다. 이 예에서 버전 번호는 6.2.0입니다.



c. boot: 프롬프트에서 version single 명령을 입력합니다. 여기서 version 은 버전 번호(예: 6.2.0 single)입니다. 시스템에 UCAPL(United Capabilities Approved Products List) 규정 준수가 활성화된 경우 비밀번호를 입력하라는 메시지가 표시됩니다. 비밀번호를 입력합니다 Sourcefire.

· Firepower Management Center 모델 1000, 1600, 2500, 2600, 4500 또는 4600:
부팅 메뉴가 나타나면 Option 4, Cisco Firepower Management Console Password Restore Mode.

4. 새 관리자 비밀번호를 할당합니다. 디바이스에 적합한 지침을 사용합니다.

· Firepower Management Center 또는 NGIPSv에 대한 새 CLI 및 셸 관리자 비밀번호:

a. 시스템에서 파운드 기호(#)로 끝나는 OS 프롬프트를 표시하는 경우 다음 명령을 입력합니다

```
passwd admin
```

b. 새 관리자 비밀번호를 입력하라는 프롬프트가 표시되면 입력합니다(두 번).

참고: 시스템에 BAD PASSWORD 메시지는 정보 제공용입니다. 이 메시지가 나타나는 경우에도 사용자가 입력한 비밀번호가 적용됩니다. 그러나 보안상의 이유로 더 복잡한 비밀번호를 사용하는 것이 좋습니다.

· 7000 및 8000 Series 디바이스에 대한 새 웹 및 CLI 관리자 비밀번호:

파운드 기호(#)로 끝나는 OS 프롬프트에서 다음 명령을 입력합니다.

```
usertool.pl -p 'admin password'
```

여기서 비밀번호는 새 관리자 비밀번호입니다.

5. 로그인 시도가 너무 많이 실패하여 관리자 계정이 잠겼다면 계정을 잠금 해제해야 합니다. 디바

이스에 적합한 지침을 사용합니다.

- Firepower Management Center 또는 NGIPSv에서 CLI 및 셸 관리자 계정의 잠금을 해제하려면 OS 프롬프트에서 파운드 기호(#)로 끝나는 다음 명령을 입력합니다.

```
pam_tally --user admin --reset
```

- 7000 및 8000 Series 디바이스에서 웹 및 CLI 관리자 어카운트의 잠금을 모두 해제하려면 OS 프롬프트에서 파운드 기호(#)로 끝나는 다음 명령을 입력합니다.

```
usertool.pl -u admin
```

6. 파운드 기호(#)로 끝나는 OS 프롬프트에서 `reboot` 명령을 실행합니다.

7. 재부팅 프로세스를 완료할 수 있습니다.

옵션 2. 외부 인증을 사용하여 CLI에 액세스하여 Firepower Management Center의 비밀번호 재설정

관리자 액세스 권한이 있는 계정으로 FMC 웹 인터페이스에 계속 액세스할 수 있는 상황이면 `External Authentication` CLI에 액세스하는 기능입니다. 이 방법을 사용하면 FMC의 CLI에 로그인하고, Linux 셸에 액세스하며, 루트로 승격하고, CLI/셸 관리자 비밀번호를 수동으로 재설정할 수 있습니다. 이 옵션은 재부팅 또는 콘솔 액세스가 필요하지 않습니다. 이 옵션을 사용하려면 관리자 비밀번호를 재설정하려는 Firepower Management Center에서 외부 인증(SSH 액세스 포함)을 올바르게 구성해야 합니다. (사용 중인 버전에 대한 [지침은 Firepower Management Center](#) 컨피그레이션 가이드를 참조하십시오.) 구성이 완료되면 다음 단계를 수행합니다.

1. SSH 또는 콘솔을 사용하여 CLI/셸 액세스 권한이 있는 외부 인증 계정으로 Firepower Management Center에 로그인합니다.
 - FMC에서 버전 6.2 이하를 실행하는 경우 Linux 셸에 직접 액세스할 수 있습니다.
 - FMC에서 버전 6.3 또는 6.4를 실행하고 FMC CLI가 활성화되지 않은 경우 Linux 셸에 직접 액세스할 수 있습니다.
 - FMC에서 버전 6.3 또는 6.4를 실행하고 Firepower Management Center CLI가 활성화된 경우 Firepower Management Center CLI에 액세스할 수 있습니다. 다음을 입력합니다. `expert` 명령을 사용하여 Linux 셸에 액세스합니다.
 - FMC에서 버전 6.5 이상을 실행하는 경우 Firepower Management Center CLI에 액세스할 수 있습니다. 다음을 입력합니다. `expert` 명령을 사용하여 Linux 셸에 액세스합니다.
2. 달러 기호(\$)가 있는 셸 프롬프트에서 다음 명령을 입력하여 관리자 사용자의 CLI 비밀번호를 재설정합니다.

```
sudo passwd admin
```
3. 에서 `Password` 프롬프트에서 현재 로그인한 사용자 이름의 비밀번호를 입력합니다.
4. 새 관리자 비밀번호를 입력하라는 프롬프트가 표시되면 입력합니다(2회).



참고: 시스템에 BAD PASSWORD(잘못된 비밀번호) 메시지가 표시되는 경우 이 정보는 참조용입니다. 이 메시지가 나타나는 경우에도 사용자가 입력한 비밀번호가 적용됩니다. 그러나 보안상의 이유로 더 복잡한 비밀번호를 사용하는 것이 좋습니다.

5. 로그인 시도 실패가 너무 많아서 관리자 계정이 잠긴 경우 계정을 잠금 해제하고 `pam_tally` 명령

을 입력하고 프롬프트가 표시되면 비밀번호를 입력합니다.

```
sudo pam_tally --user --reset
```

6. 유형 `exit` 셸을 종료합니다.

7. CLI가 활성화된 Firepower 관리 센터에서 다음을 입력합니다 `exit` 를 눌러 CLI를 종료합니다.

firepower Management Center에 대해 손실된 웹 인터페이스 관리자 비밀번호 재설정

다음 지침에 따라 Firepower Management Center 웹 인터페이스에 액세스하는 데 사용되는 관리자 계정의 비밀번호를 변경합니다.

절차:

1. SSH 또는 콘솔을 사용하여 CLI 관리자 계정으로 어플라이언스에 로그인합니다.
2. Linux 셸에 액세스합니다.
 - FMC에서 버전 6.2 이하를 실행하는 경우 로그인하여 Linux 셸에 직접 액세스할 수 있습니다.
 - FMC에서 버전 6.3 또는 6.4를 실행하고 Firepower Management Center CLI가 활성화되지 않은 경우 로그인하여 Linux 셸에 직접 액세스할 수 있습니다.
 - FMC에서 버전 6.3 또는 6.4를 실행하고 Firepower Management Center CLI가 활성화된 경우 로그인하여 Firepower Management Center CLI에 액세스할 수 있습니다. 다음을 입력합니다. `expert` 명령을 사용하여 Linux 셸에 액세스합니다.
 - FMC에서 버전 6.5 이상을 실행하는 경우 로그인하면 Firepower Management Center CLI에 액세스할 수 있습니다. 다음을 입력합니다. `expert` 명령을 사용하여 Linux 셸에 액세스합니다.
3. 웹 인터페이스 admin 사용자의 비밀번호를 재설정하려면 셸 프롬프트에서 다음 명령을 입력합니다.

```
sudo usertool.pl -p 'admin password'
```

여기서 `password`는 웹 인터페이스 관리자 사용자의 새 비밀번호입니다.

4. 에서 `Password` 프롬프트에서 현재 로그인한 사용자 이름의 비밀번호를 입력합니다.
5. 너무 많은 로그인 시도 실패 때문에 웹 관리자 계정이 잠겼다면 계정을 잠금 해제해야 합니다. 실행 `usertool` 명령을 입력한 다음 프롬프트가 표시되면 CLI 관리자 비밀번호를 입력합니다.

```
sudo usertool.pl -u admin
```

6. 유형 `exit` 셸을 종료합니다.

7. CLI가 활성화된 Firepower 관리 센터에서 다음을 입력합니다 `exit` 를 눌러 CLI를 종료합니다.

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.