FTD에서 로컬 관리자에 대한 최대 로그인 시도 실패 구성

문제

- Cisco FTD(Secure Firewall Threat Defense)에서 로컬 관리자 계정에 대해 실패한 최대 로그인 시도 횟수를 구성하는 것이 목적입니다.
- 이 요청에는 GUI(그래픽 사용자 인터페이스) 및 CLI(Command Line Interface)를 통해 이 제한을 설정하는 지침이 포함됩니다.
- 관리 계정이 무차별 대입 로그인 시도로부터 보호되는지 확인합니다.

환경

- 제품: Cisco Secure Firewall
- 소프트웨어 버전: 모두
- 실패한 로그인 시도 제한을 설정하는 데 필요한 구성 지원

해결

Secure Firewall을 관리하는 방식에 따라 두 가지 경우가 있습니다.

기본 동작

기본적으로 보안 방화벽의 로컬 관리자 계정에 대한 maxfailedlogins는 구성할 수 없습니다.

```
> configure user maxfailedlogins admin 5
Unable to modify admin account.
```

FMC에서 관리하는 방화벽

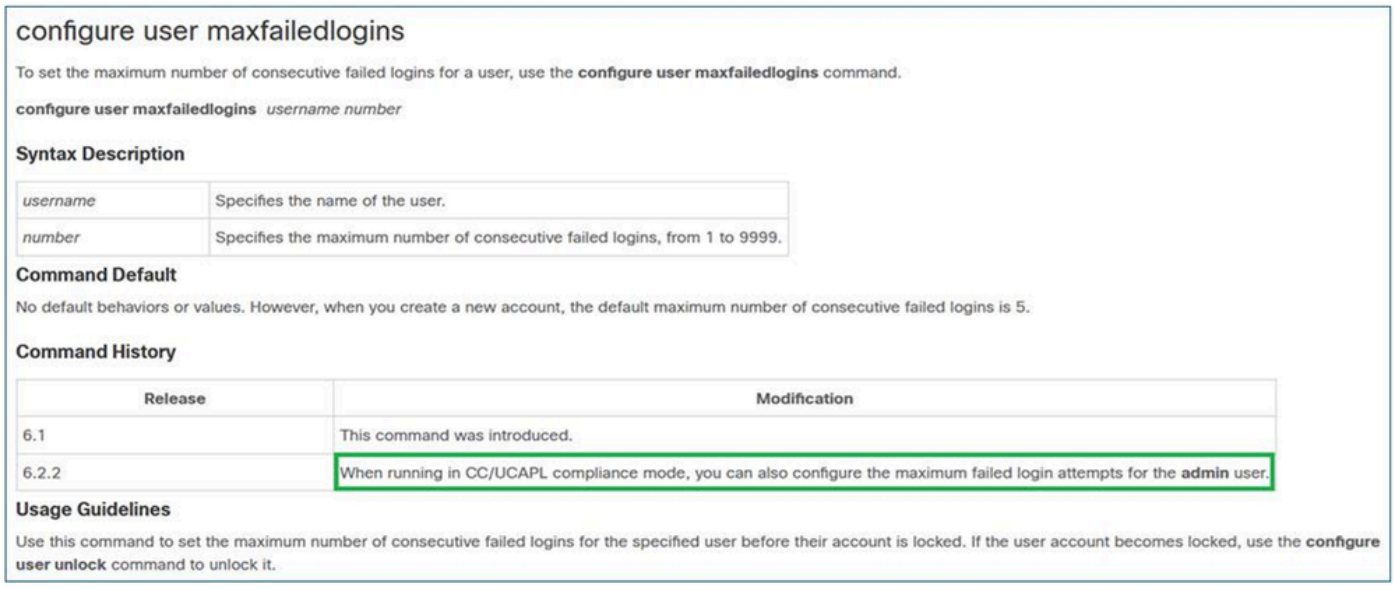
기본적으로 Cisco FMC에서 관리하는 로컬 관리자 계정에 대한 maxfailedlogins는 구성할 수 없습니다.

```
> configure user maxfailedlogins admin 5
Unable to modify admin account.
```

솔루션

이 제한을 극복하려면 방화벽에서 규정 준수 모드를 활성화해야 합니다. 이 내용은 Cisco FTD 명령 참조에 설명되어 있습니다.

https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firep



configure user maxfailedlogins

To set the maximum number of consecutive failed logins for a user, use the **configure user maxfailedlogins** command.

configure user maxfailedlogins *username number*

Syntax Description

username	Specifies the name of the user.
number	Specifies the maximum number of consecutive failed logins, from 1 to 9999.

Command Default

No default behaviors or values. However, when you create a new account, the default maximum number of consecutive failed logins is 5.

Command History

Release	Modification
6.1	This command was introduced.
6.2.2	When running in CC/UCAPL compliance mode, you can also configure the maximum failed login attempts for the **admin** user.

Usage Guidelines

Use this command to set the maximum number of consecutive failed logins for the specified user before their account is locked. If the user account becomes locked, use the **configure user unlock** command to unlock it.

inline_image_0.png

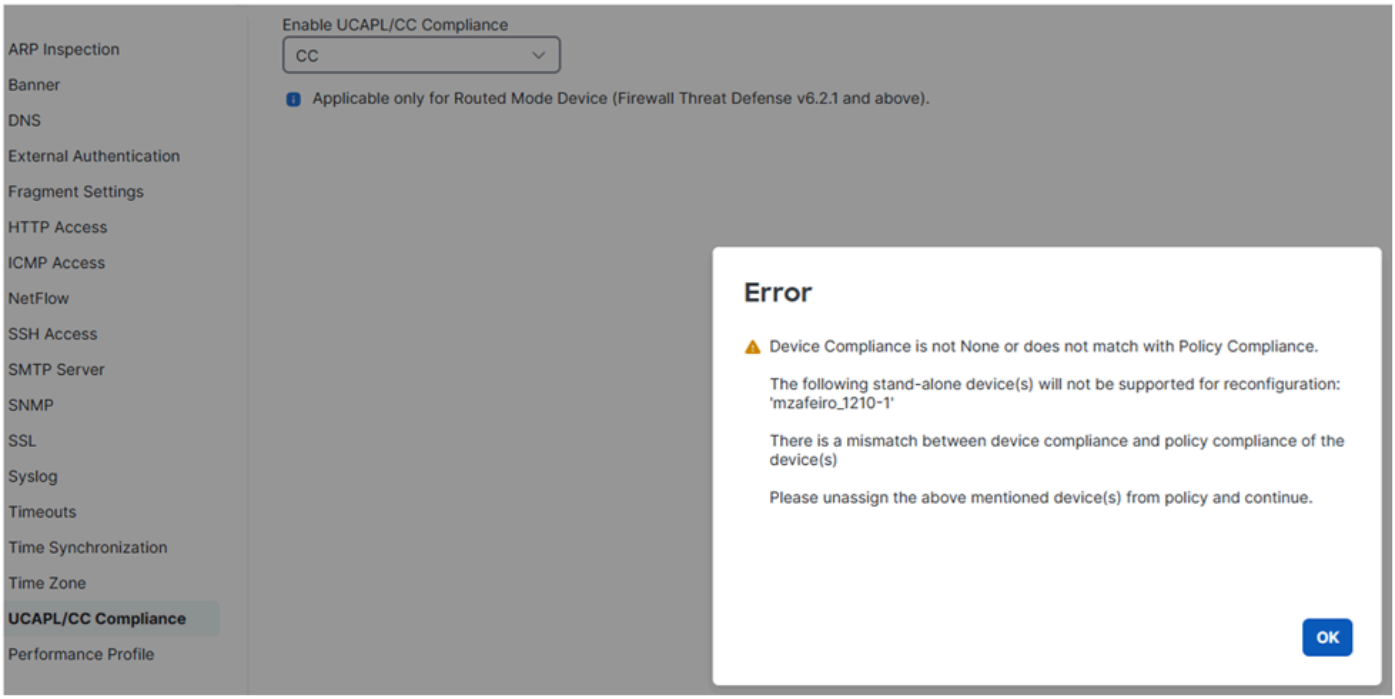
CC 및 UCAPL 규정 준수

보안 제품을 강화하기 위한 요구 사항을 지정하는 보안 컴플라이언스 표준입니다.

maxfailedlogins의 경우, 관련 정보는 Security Certifications Compliance에 있습니다.

중요 참고 사항

먼저, FTD에서 CC 또는 UCAPL 규정 준수를 활성화한 후에는 변경 사항을 되돌릴 수 없습니다. 되돌리려고 하면 다음과 같은 결과가 발생합니다.



inline_image_0.png

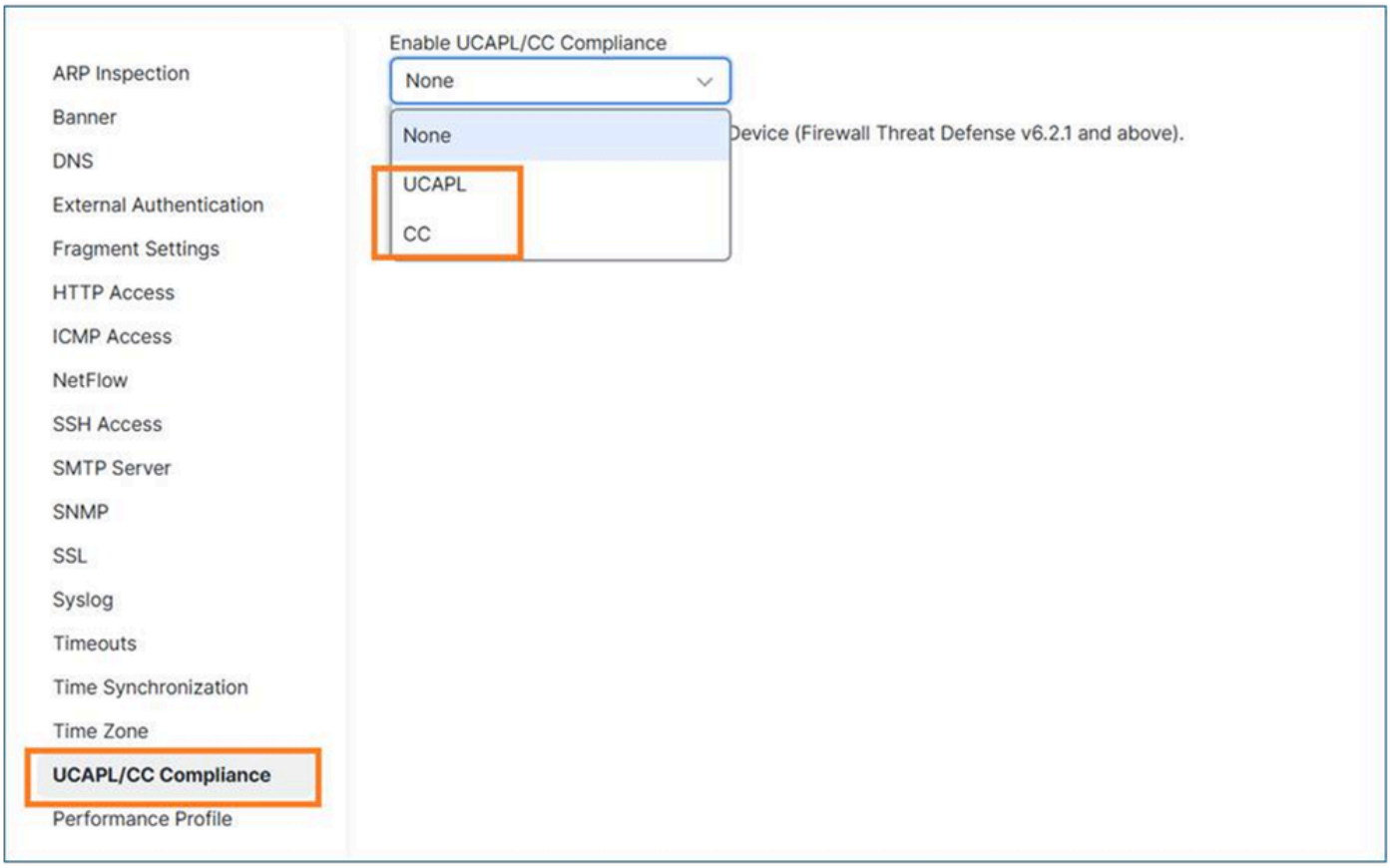
규정 준수 모드를 활성화하고 정책을 구축하면 FTD가 재부팅됩니다.

최대 장애 로그인의 경우, CC에서는 최대 9999개의 실패 시도를 구성할 수 있으며, UCAPL에서는 최대 3개까지 구성할 수 있습니다.

FTD에서 CC 또는 UCAPL 규정 준수 활성화

1단계: FMC에서 Devices/Platform Settings(디바이스/플랫폼 설정)로 이동합니다.

2단계: 두 가지 규정 준수 모드(UCAP 또는 CC) 중 하나를 사용하도록 설정합니다. 변경 내용은 되돌릴 수 없으므로 보안 인증 규정 준수 설명서를 주의 깊게 읽는 것이 좋습니다.



inline_image_0.png

3단계: 이 작업을 마치면 FTD에 플랫폼 설정 정책을 할당하고(아직 할당되지 않은 경우) Deploy를 수행해야 합니다.

구축이 완료되면 FTD 디바이스는 자동으로 재부팅됩니다.

```
Broadcast message from root@secure_fw (Tue Jan 13 10:10:49 2026):

A reboot has been scheduled to occur 10 seconds from now.

Jan 13 2026 10:11:01 INIT: Running /etc/rc6.d/K00all_ports_down.sh stop...
Tue Jan 13 10:11:01 UTC 2026 : Checking for running portmgr process...
Terminating DME and all AGs bfore bring down all ports...
Tue Jan 13 10:11:01 UTC 2026 : Sending IPC message to portmgr to bring down all ports...
2026-01-13 10:11:02.112 PMLOG:PM IPC UTILITY: Shutting down all ports
Jan 13 2026 10:11:02 INIT: Completed /etc/rc6.d/K00all_ports_down.sh stop...
Jan 13 2026 10:11:02 INIT: Running /etc/rc6.d/K00ftd.sh stop...

Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.7.6.1.291__ftd_001_FOL2751Z03FLKF25W1, FLAG=''
Cisco Firewall Threat Defense stopping ...
```

4단계: 방화벽을 다시 가동하면 maxfailedlogins 설정을 구성할 수 있습니다. UCAPL을 선택한 경우 실패한 로그인 시도를 최대 3개까지 구성할 수 있습니다.

```
> configure user maxfailedlogins admin 5
Unable to set limit, must be 3 or less for UCAPL mode

>
```

CC의 경우 9999까지 설정할 수 있습니다.

```
> configure user maxfailedlogins admin 9999

>
```

5단계: show user 명령을 사용하여 컨피그레이션을 확인합니다.

```
> show user
Login              UID   Auth Access  Enabled Reset   Exp     Warn    Grace MinL Str Lock Max
admin              101  Local Config  Enabled    No Never Disabled Disabled    5 Dis   No   3
```

팁: 관리자 사용자가 잠길 경우에 대비하여 구성 권한을 사용할 수 있는 다른 사용자가 있는지 확인합니다.

잠긴 관리자 사용자 잠금 해제

maxfailedlogins를 3으로 설정하면 3번의 시도가 실패하면 관리자 계정이 잠깁니다.

```
> show user
Login              UID   Auth Access  Enabled Reset   Exp     Warn    Grace MinL Str Lock Max
admin              101  Local Config  Enabled    No Never Disabled Disabled    5 Dis  Yes   3
```

이 경우 다른 사용자로 로그인하고 admin 사용자를 수동으로 잠금 해제해야 합니다.

```
> configure user unlock admin

> show user
Login              UID   Auth Access  Enabled Reset   Exp     Warn    Grace MinL Str Lock Max
admin              101  Local Config  Enabled    No Never Disabled Disabled    5 Dis   No   3
```

FDM(Device Manager)에서 관리되는 방화벽

FDM은 현재 CC 또는 UCAPL 규정 준수 모드를 지원하지 않습니다.

관련 개선 사항: CSCws76567 ENH: Firepower 장치 관리자에 CC/UCAPL 지원 추가

이 기능이 중요한 경우 CSCws76567으로 참조되는 관련 개선 요청의 우선 순위를 계정 관리자와 논의하는 것이 좋습니다.

웹 GUI 액세스에 대해 실패한 최대 로그인 시도 횟수 설정

CLI 로그인과 마찬가지로, 이 기능은 CC 또는 UCAPL 규정 준수 모드가 활성화된 경우에만 사용할 수 있습니다.

웹 GUI 액세스에 대해 실패한 최대 로그인 시도 횟수 설정

CLI 로그인과 마찬가지로, 이 기능은 CC 또는 UCAPL 규정 준수 모드가 활성화된 경우에만 사용할 수 있습니다.

Security Certifications Compliance Characteristics

The following table describes behavior changes when you enable CC or UCAPL mode. (Restrictions on login accounts refers to command line access, not web interface access.)

System Change	Secure Firewall Management Center		Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
FIPS compliance is enabled.	Yes	Yes	Yes	Yes	Yes	Yes
The system does not allow remote storage for backups or reports.	Yes	Yes	–	–	–	–
The system starts an additional system audit daemon.	No	Yes	No	Yes	No	No
The system boot loader is secured.	No	Yes	No	Yes	No	No
The system applies additional security to login accounts.	No	Yes	No	Yes	No	No
The system disables the reboot key sequence Ctrl+Alt+Del.	No	Yes	No	Yes	No	No
The system enforces a maximum of ten simultaneous login sessions.	No	Yes	No	Yes	No	No
Passwords must be at least 15 characters long, and must consist of alphanumeric characters of mixed case and must include at least one numeric character.	No	Yes	No	Yes	No	No
The minimum required password length for the local `admin` user can be configured using the local device CLI.	No	No	No	No	Yes	Yes
Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.	No	Yes	No	Yes	No	No
The system locks out users other than `admin` after three failed login attempts in a row. In this case, the password must be reset by an administrator.	No	Yes	No	Yes	No	No
The system stores password history by default.	No	Yes	No	Yes	No	No
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the web interface.	Yes	Yes	Yes	Yes	–	–
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the local appliance CLI.	No	No	Yes, regardless of security certifications compliance enablement.	Yes, regardless of security certifications compliance enablement.	Yes	Yes
The system automtically rekeys an SSH session with an appliance: • After a key has been in use for one hour of session activity • After a key has been used to transmit 1 GB of data over the connection	Yes	Yes	Yes	Yes	Yes	Yes
The system performs a file system integrity check (FSIC) at boot-time. If the FSIC fails, Secure Firewall software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.	Yes	Yes	Yes	Yes	Yes	Yes

inline_image_0.png

참조

- 보안 인증 규정 준수 특성

FDM 관리 디바이스에서는 CC 또는 UCAPL 모드를 사용할 수 없으므로 웹 GUI 액세스에 대해 실패한 최대 로그인 시도 횟수를 설정할 수 없습니다(개선 사항 CSCws76567 참조).

원인

- FMC 관리 디바이스의 경우 이 옵션은 CC 또는 UCAPL 규정 준수 모드가 활성화된 경우에만 사용할 수 있습니다.
- FDM 관리 디바이스의 경우 이 기능 격차를 해결하고 방화벽 디바이스 관리자에서 CC(Common Criteria) 및 UCAPL 규정 준수에 대한 지원을 추가하기 위한 개선 요청(CSCws76567)이 제출되었습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드
- Cisco 버그 ID CSCws76567

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.