Maximale mislukte inlogpogingen configureren voor lokale beheerder op FTD

uitgeven

- Het doel is om het maximale aantal mislukte inlogpogingen voor lokale beheerdersaccounts op Cisco Secure Firewall Threat Defense (FTD) te configureren.
- Het verzoek bevat richtlijnen voor het instellen van deze limiet via zowel de grafische gebruikersinterface (GUI) als de opdrachtregelinterface (CLI).
- Zorg ervoor dat beheerdersaccounts zijn beveiligd tegen brute-force inlogpogingen.

milieu

- Product: Cisco Secure Firewall
- Softwareversie: Alle
- Hulp bij configuratie vereist voor instellen van limieten voor mislukte inlogpogingen

resolutie

Er zijn twee verschillende gevallen, afhankelijk van hoe de beveiligde firewall wordt beheerd.

Standaardgedrag

Standaard kunt u maxfailedlogins niet configureren voor de lokale beheerdersaccount op de beveiligde firewall:

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

Firewall beheerd door FMC

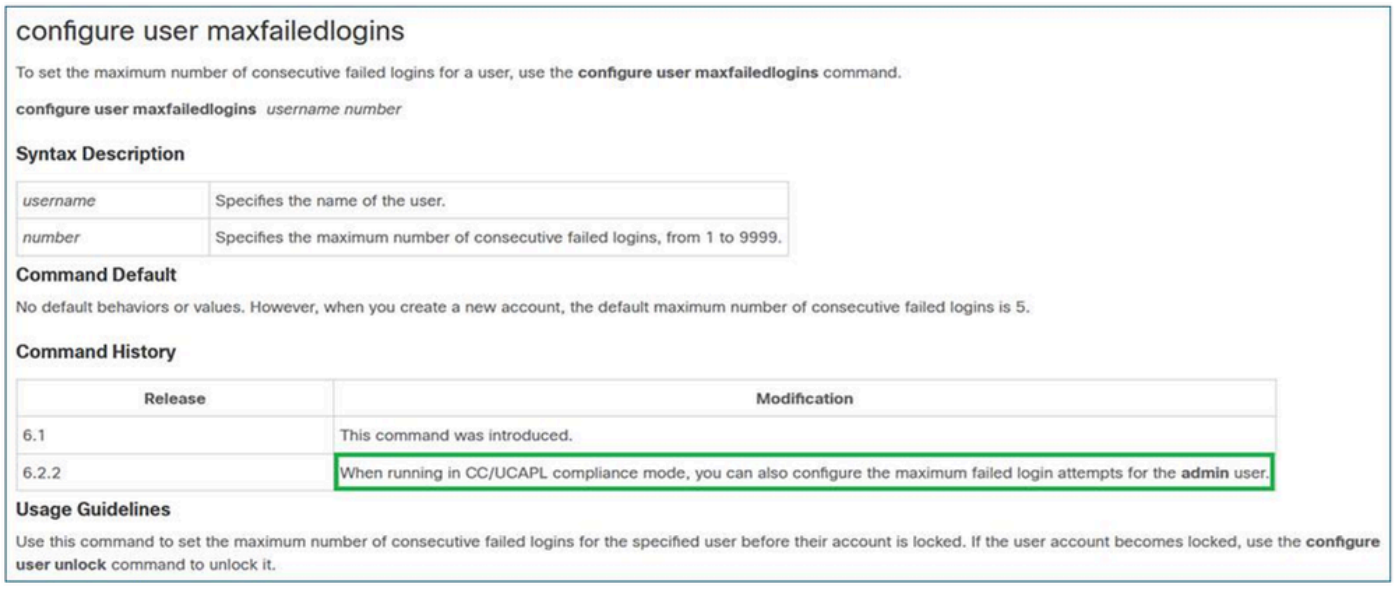
Standaard kunt u geen maxfailedlogins configureren voor de lokale beheerdersaccount die wordt beheerd door Cisco FMC:

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

De oplossing

Om deze beperking te overwinnen, moet u de nalevingsmodus op de firewall inschakelen. Dit wordt gedocumenteerd in de verwijzing naar Cisco FTD-opdrachten:

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

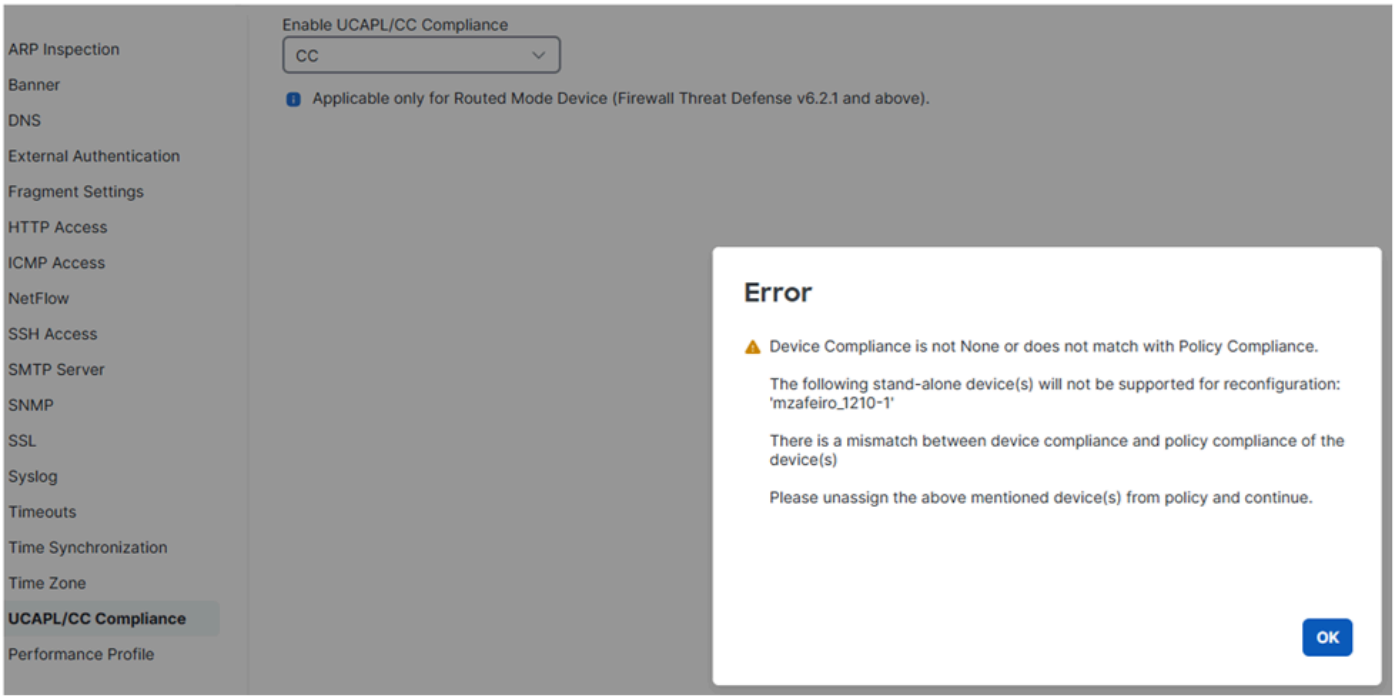
Naleving van CC en UCAPL

Het zijn normen voor de naleving van de beveiliging die eisen voor het verharden van beveiligingsproducten specificeren.

In het geval van maxfailedlogins, is de gerelateerde informatie in Security Certifications Compliance.

Belangrijke opmerkingen

Ten eerste, onthoud dat wanneer u CC- of UCAPL-naleving inschakelt op FTD, u de wijziging niet kunt herstellen. Als u probeert terug te keren, krijgt u:



inline_image_0.png

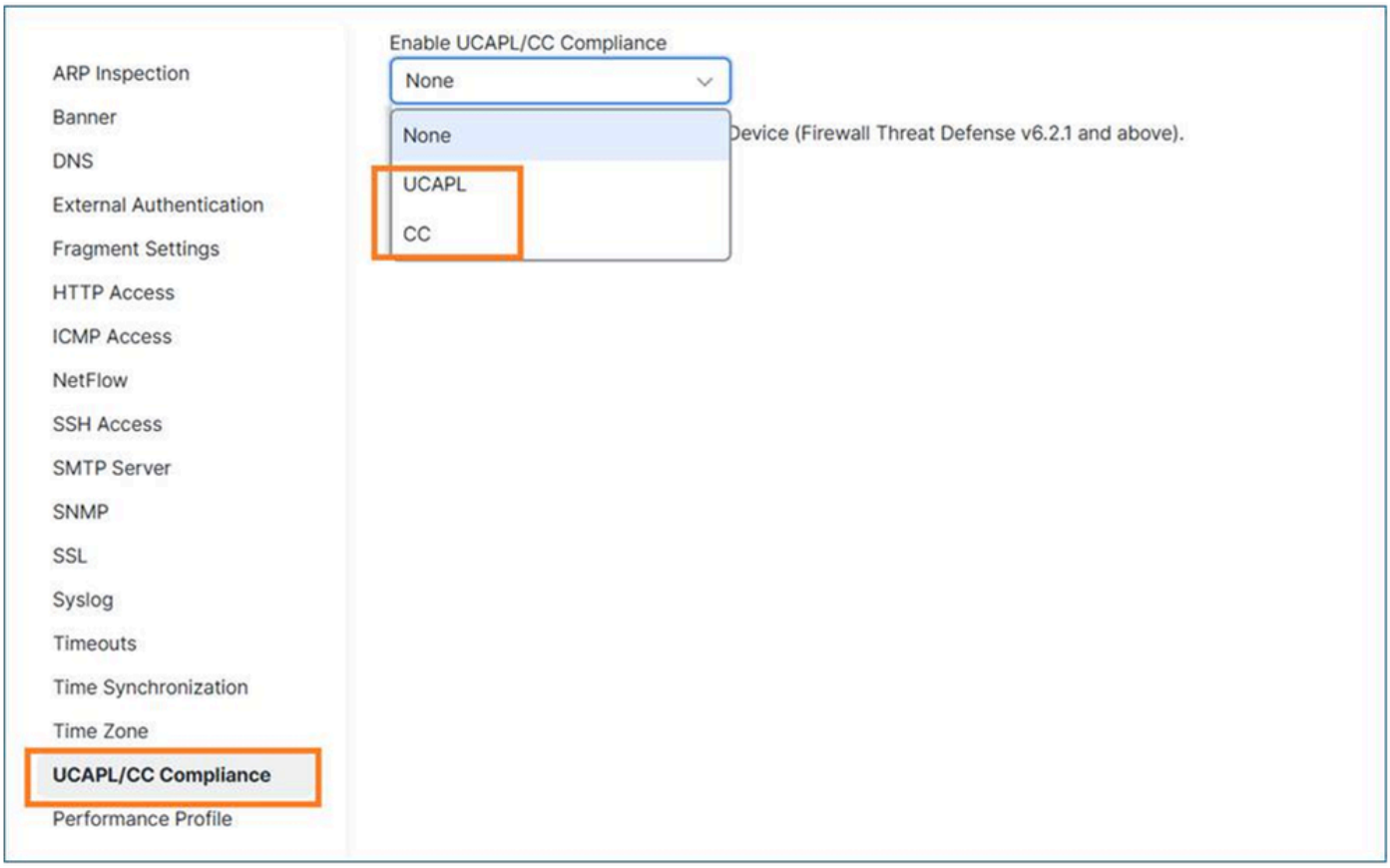
Zodra u een nalevingsmodus inschakelt en het beleid implementeert, wordt de FTD opnieuw opgestart.

Als het gaat om maxfailedlogins, kunt u met CC tot 9999 mislukte pogingen configureren, terwijl u met UCAPL tot 3 kunt werken.

CC- of UCAPL-naleving op FTD inschakelen

Stap 1: Op FMC navigeert u naar de Apparaten / Platforminstellingen.

Stap 2: Schakel een van de twee nalevingsmodi in (UCAP of CC). Aangezien de wijziging niet ongedaan kan worden gemaakt, wordt het ten zeerste aanbevolen om de handleiding voor naleving van beveiligingscertificaten aandachtig te lezen.



inline_image_0.png

Stap 3: Zodra dit is gebeurd, moet u het beleid voor platforminstellingen toewijzen aan de FTD (als dit nog niet is gebeurd) en implementeren.

Zodra de implementatie is voltooid, wordt het FTD-apparaat automatisch opnieuw opgestart:

```
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 ...
```

Stap 4: Zodra de firewall weer is ingeschakeld, kunt u de instelling voor maximale aanmelding configureren. Als u UCAPL kiest, kunt u maximaal 3 mislukte aanmeldpogingen configureren:

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

>
```

In het geval van CC kunt u instellen op 9999:

```
> configure user maxfailedlogins admin 9999

>
```

Stap 5: Verifieer de configuratie met de opdracht show user:

```
> 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
```

Tip: zorg ervoor dat er een andere gebruiker met configuratiebevoegdheden beschikbaar is voor het geval de beheerdersgebruiker wordt vergrendeld!

Een vergrendelde beheerdersgebruiker ontgrendelen

Ervan uitgaande dat u maxfailedlogins 3 instelt, wordt de beheerdersaccount na 3 mislukte pogingen vergrendeld:

```
> 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
```

In dat geval moet u inloggen met een andere gebruiker en de beheerder handmatig ontgrendelen:

```
> 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
```

Firewall beheerd door Apparaatbeheer (FDM)

FDM ondersteunt momenteel geen CC- of UCAPL-nalevingsmodi.

Gerelateerde verbetering: CSCws76567 ENH: CC/UCAPL-ondersteuning toevoegen aan Firepower Device Manager

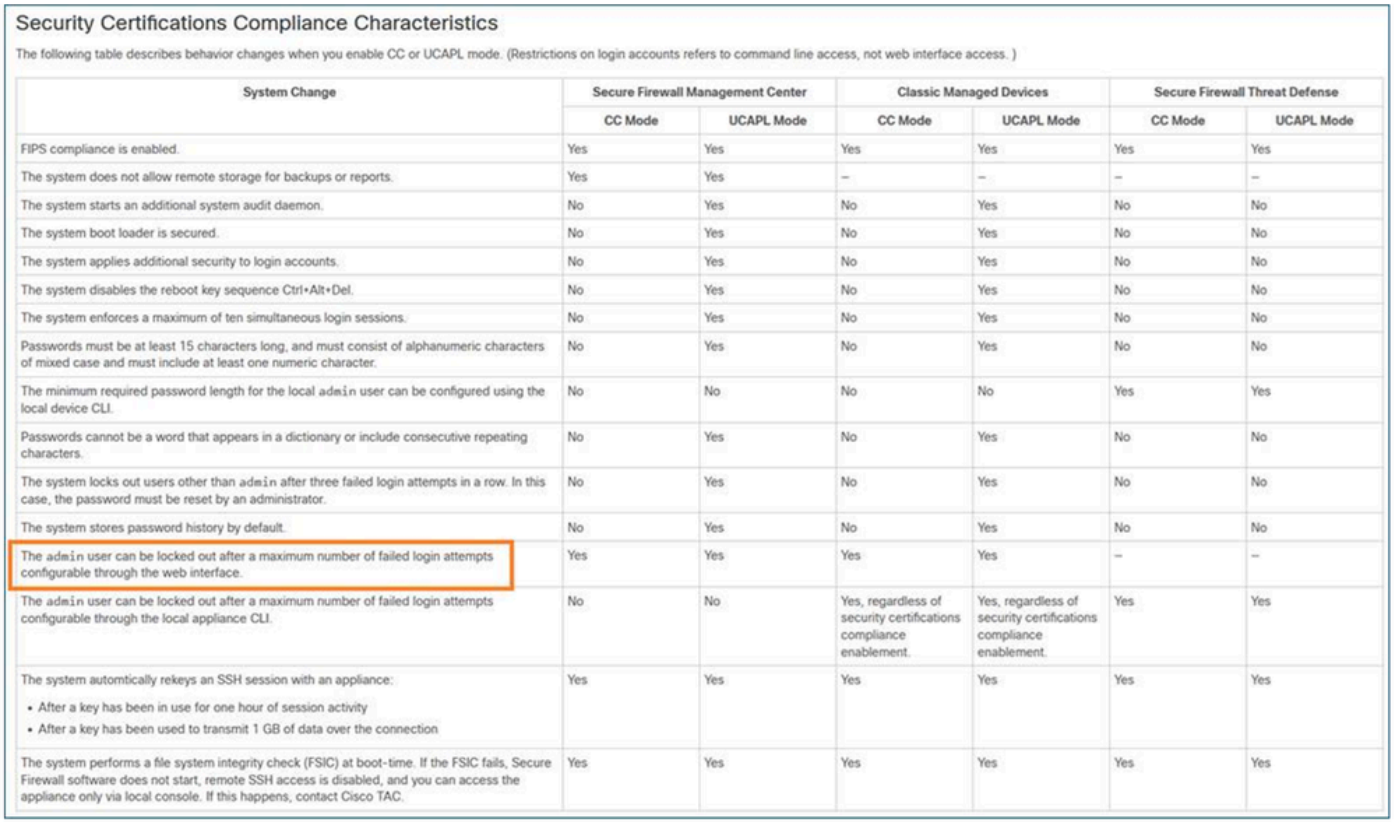
Als deze functionaliteit van cruciaal belang is, is het raadzaam om de prioritering van het gerelateerde verbeteringsverzoek, waarnaar wordt verwezen als CSCws76567, te bespreken met uw accountmanager.

Het maximum aantal mislukte aanmeldingspogingen voor Web GUI-toegang instellen

Net als bij de CLI-aanmelding is deze functionaliteit alleen beschikbaar als de nalevingsmodus CC of UCAPL is ingeschakeld:

Het maximum aantal mislukte aanmeldingspogingen voor Web GUI-toegang instellen

Net als bij de CLI-aanmelding is deze functionaliteit alleen beschikbaar als de nalevingsmodus CC of UCAPL is ingeschakeld:



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

referentie

- conformiteitskarakteristieken voor beveiligingscertificaten

Aangezien de CC- of UCAPL-modi niet kunnen worden gebruikt op door FDM beheerde apparaten, kunt u het maximale aantal mislukte inlogpogingen voor web GUI-toegang niet instellen (zie uitbreiding CSCws76567).

Oorzaak

- Voor apparaten die door de FMC worden beheerd, is de optie alleen beschikbaar als de nalevingsmodus CC of UCAPL is ingeschakeld.
- Voor door FDM beheerde apparaten is een verzoek tot verbetering (CSCws76567) ingediend om deze functiekloof aan te pakken en ondersteuning toe te voegen voor Common Criteria (CC) en UCAPL-naleving in Firewall Device Manager.

Verwante inhoud

- Cisco Technical Support en downloads
- Cisco Bug ID CSCws76567

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.