Maximale Anzahl fehlgeschlagener Anmeldeversuche für lokalen Administrator auf FTD konfigurieren

Problem

- Ziel ist es, die maximale Anzahl fehlgeschlagener Anmeldeversuche für lokale Administratorkonten in Cisco Secure Firewall Threat Defense (FTD) zu konfigurieren.
- Die Anforderung enthält Anweisungen zum Festlegen dieses Grenzwerts sowohl über die grafische Benutzeroberfläche (GUI) als auch über die Befehlszeilenschnittstelle (CLI).
- Stellen Sie sicher, dass die Administratorkonten vor Brute-Force-Anmeldeversuchen geschützt sind.

Umwelt

- Produkt: Cisco Secure Firewall
- Softwareversion: Beliebige
- Konfigurationsunterstützung erforderlich, um Grenzwerte für fehlgeschlagene Anmeldeversuche festzulegen

Auflösung

Je nachdem, wie die sichere Firewall verwaltet wird, gibt es zwei verschiedene Fälle.

Standardverhalten

Standardmäßig können Sie keine MAXFAL-Anmeldungen für das lokale Admin-Konto auf der sicheren Firewall konfigurieren:

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

Firewall von FMC verwaltet

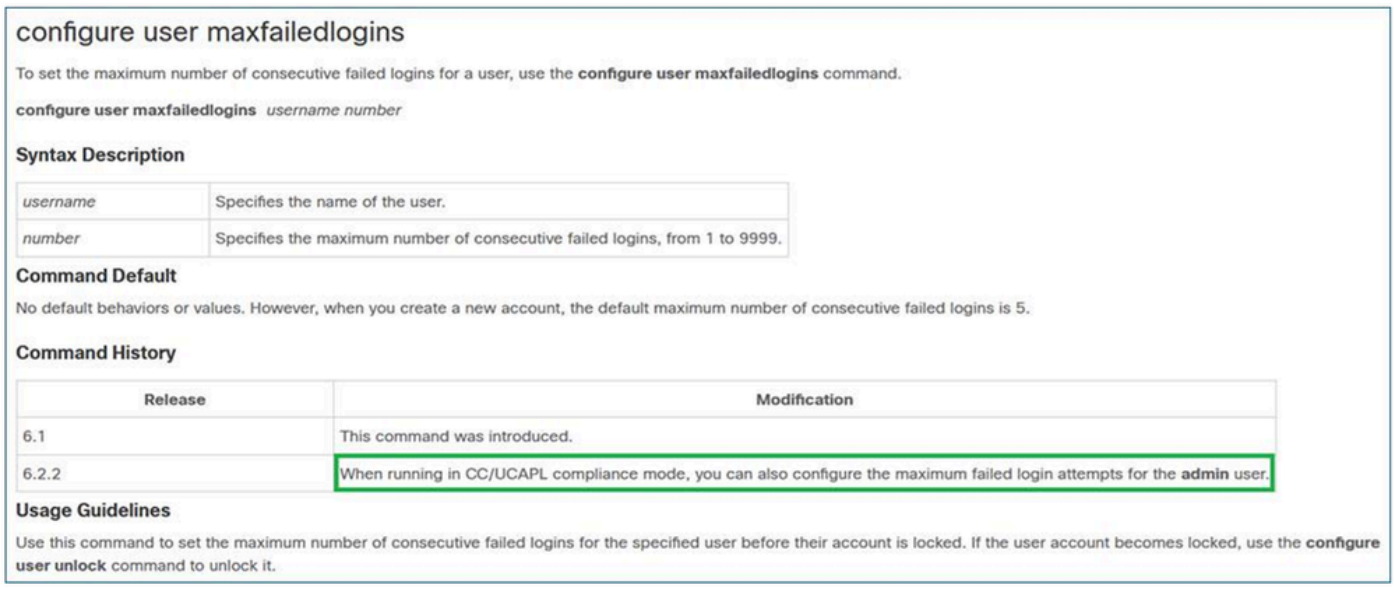
Standardmäßig können Sie keine MAXFAL-Anmeldungen für das von Cisco FMC verwaltete lokale Administratorkonto konfigurieren:

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

Die Lösung

Um diese Einschränkung zu überwinden, müssen Sie den Compliance-Modus auf der Firewall aktivieren. Dies wird in der Cisco FTD-Befehlsreferenz dokumentiert:

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

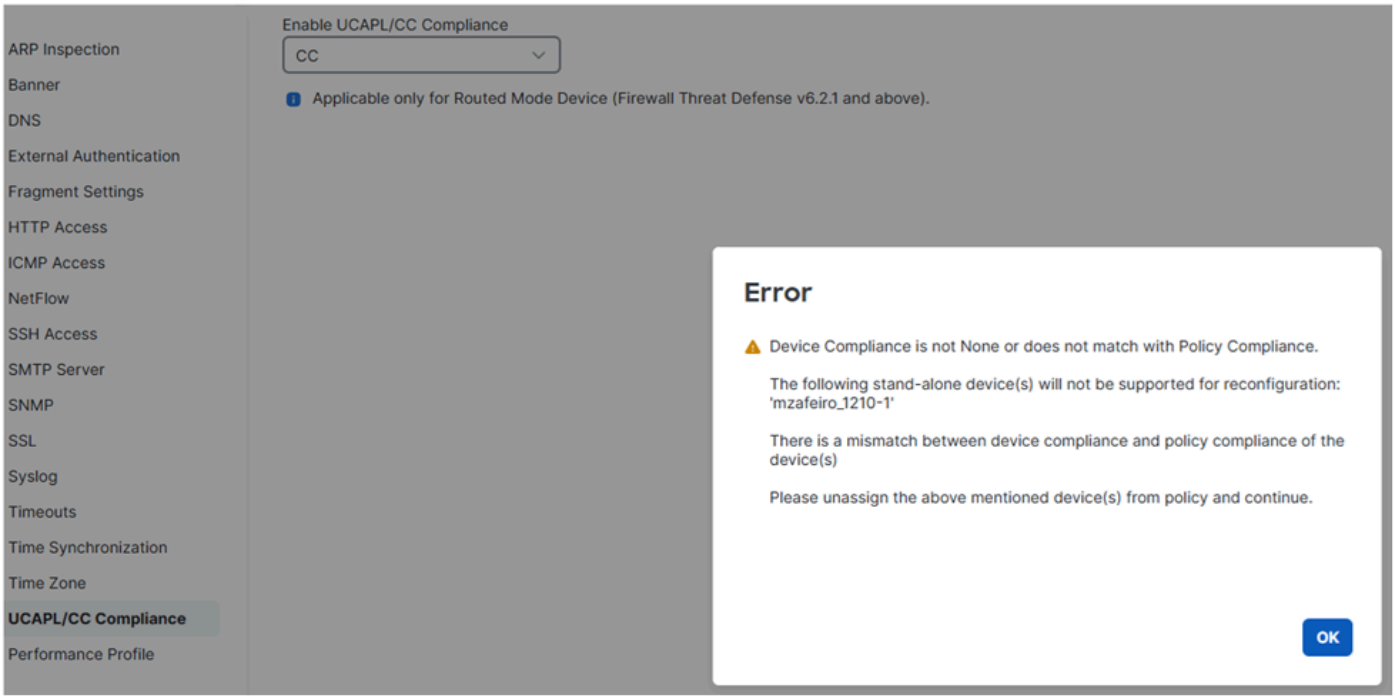
CC- und UCAPL-Konformität

Es handelt sich um Sicherheits-Compliance-Standards, die Anforderungen für die Härtung von Sicherheitsprodukten festlegen.

Im Fall von MAXFALEL-Anmeldungen sind die zugehörigen Informationen in Übereinstimmung mit Sicherheitszertifizierungen aufgeführt.

Wichtige Hinweise

Beachten Sie zunächst, dass Sie die Änderung nicht mehr rückgängig machen können, sobald Sie die CC- oder UCAPL-Konformität auf FTD aktiviert haben. Wenn Sie versuchen, die Änderung rückgängig zu machen, erhalten Sie:



inline_image_0,png

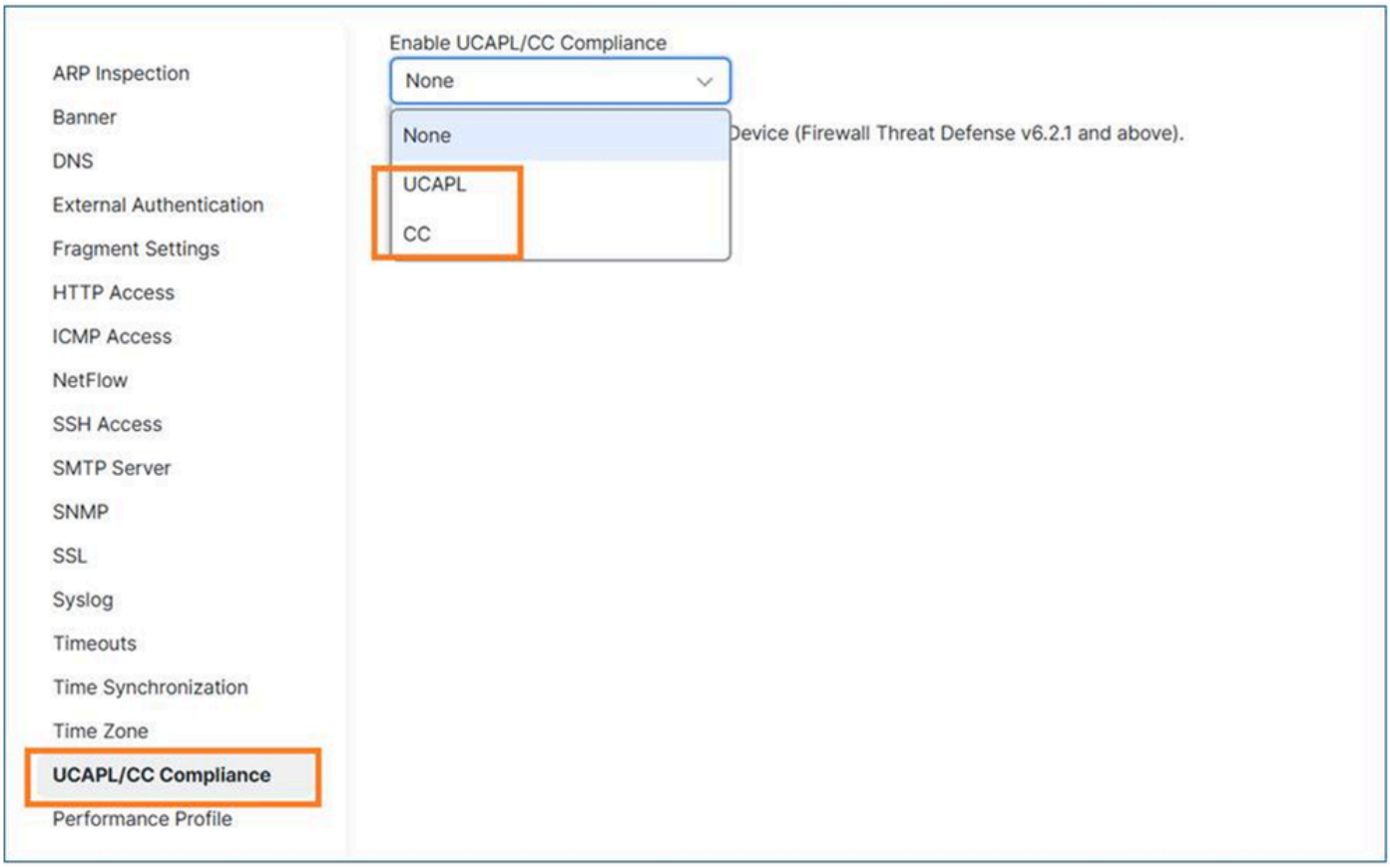
Sobald Sie einen Compliance-Modus aktivieren und die Richtlinie bereitstellen, wird die FTD neu gestartet.

Wenn es um maxfailedlogin geht, können Sie mit CC bis zu 9999 fehlgeschlagene Anmeldeversuche konfigurieren, mit UCAPL bis zu 3.

Aktivierung der CC- oder UCAPL-Konformität auf FTD

Schritt 1: Navigieren Sie auf FMC zu Geräte-/Plattformeinstellungen.

Schritt 2: Aktivieren Sie einen der beiden Compliance-Modi (UCAP oder CC). Da die Änderung nicht rückgängig gemacht werden kann, wird dringend empfohlen, den Compliance-Leitfaden für Sicherheitszertifizierungen sorgfältig zu lesen.



inline_image_0,png

Schritt 3: Anschließend müssen Sie die Richtlinie für die Plattformeinstellungen dem FTD zuweisen (falls noch nicht geschehen) und bereitstellen.

Nach Abschluss der Bereitstellung wird das FTD-Gerät automatisch neu gestartet:

```
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 ...
```

Schritt 4: Wenn die Firewall wieder aktiviert ist, können Sie die Einstellung für maxfailedLogins konfigurieren. Falls Sie UCAPL ausgewählt haben, können Sie bis zu 3 fehlgeschlagene Anmeldeversuche konfigurieren:

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

>
```

Im Fall von CC können Sie bis zu 9999 einrichten:

```
> configure user maxfailedlogins admin 9999

>
```

Schritt 5: Überprüfen Sie die Konfiguration mit dem Befehl 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
```

Tipp: Stellen Sie sicher, dass ein anderer Benutzer mit Konfigurationsberechtigungen verfügbar ist, falls der Admin-Benutzer gesperrt wird.

Sperren eines Admin-Benutzers aufheben

Angenommen, Sie setzen maxfailedLogins 3, nach 3 fehlgeschlagenen Versuchen wird das Admin-Konto gesperrt:

```
> 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 diesem Fall müssen Sie sich mit einem anderen Benutzer anmelden und den Admin-Benutzer manuell entsperren:

```
> 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
```

Vom Gerätemanager (FDM) verwaltete Firewall

FDM unterstützt derzeit keinen CC- oder UCAPL-Compliance-Modus.

Zugehörige Erweiterung: CSCws76567 DEU: CC/UCAPL-Unterstützung für FirePOWER Device Manager hinzufügen

Wenn diese Funktion kritisch ist, wird empfohlen, die Priorisierung der zugehörigen Erweiterungsanfrage, die als CSCws76567 bezeichnet wird, mit Ihrem Account Manager zu besprechen.

Festlegen der maximalen Anzahl fehlgeschlagener Anmeldeversuche für den Web-GUI-Zugriff

Ähnlich wie bei der CLI-Anmeldung ist diese Funktion nur verfügbar, wenn der CC- oder UCAPL-Kompatibilitätsmodus aktiviert ist:

Festlegen der maximalen Anzahl fehlgeschlagener Anmeldeversuche für den Web-GUI-Zugriff

Ähnlich wie bei der CLI-Anmeldung ist diese Funktion nur verfügbar, wenn der CC- oder UCAPL-Kompatibilitätsmodus aktiviert ist:

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

Referenz

- Sicherheitszertifizierungen - Compliance-Merkmale

Da der CC- oder UCAPL-Modus auf von FDM verwalteten Geräten nicht verwendet werden kann, können Sie die maximale Anzahl fehlgeschlagener Anmeldeversuche für den Web-GUI-Zugriff nicht festlegen (siehe Erweiterung CSCws76567).

Ursache

- Bei FMC-verwalteten Geräten ist die Option nur verfügbar, wenn der CC- oder UCAPL-Compliance-Modus aktiviert ist.
- Für FDM-verwaltete Geräte wurde eine Erweiterungsanforderung (CSCws76567) eingereicht, um diese Funktionslücke zu schließen und Unterstützung für Common Criteria (CC)- und UCAPL-Konformität im Firewall Device Manager hinzuzufügen.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco
- Cisco Bug-ID CSCws76567

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.