Configure Maximum Failed Log in Attempts for Local Admin on FTD

Issue

- The objective is to configure the maximum number of failed log in attempts for local administrator accounts on Cisco Secure Firewall Threat Defense (FTD).
- The request includes guidance for setting this limit via both the graphical user interface (GUI) and the comma line interface (CLI).
- Ensure administrative accounts are protected against brute-force log in attempts.

Environment

- Product: Cisco Secure Firewall
- Software version: Any
- Configuration assistance required for setting failed log in attempt limits

Resolution

There are two different cases depending on how the Secure Firewall is managed.

Default Behavior

Firewall Managed by FDM

By default, you cannot configure **maxfailedlogins** for the local admin account on the secure firewall managed by Firewall Device Manager (FDM):

<#root>

```
>

configure user maxfailedlogins admin 5

Unable to modify admin account.
```

Firewall Managed by FMC

By default, you cannot configure **maxfailedlogins** for the local admin account managed by Cisco Firewall Management Center (FMC):

```
<#root>

>

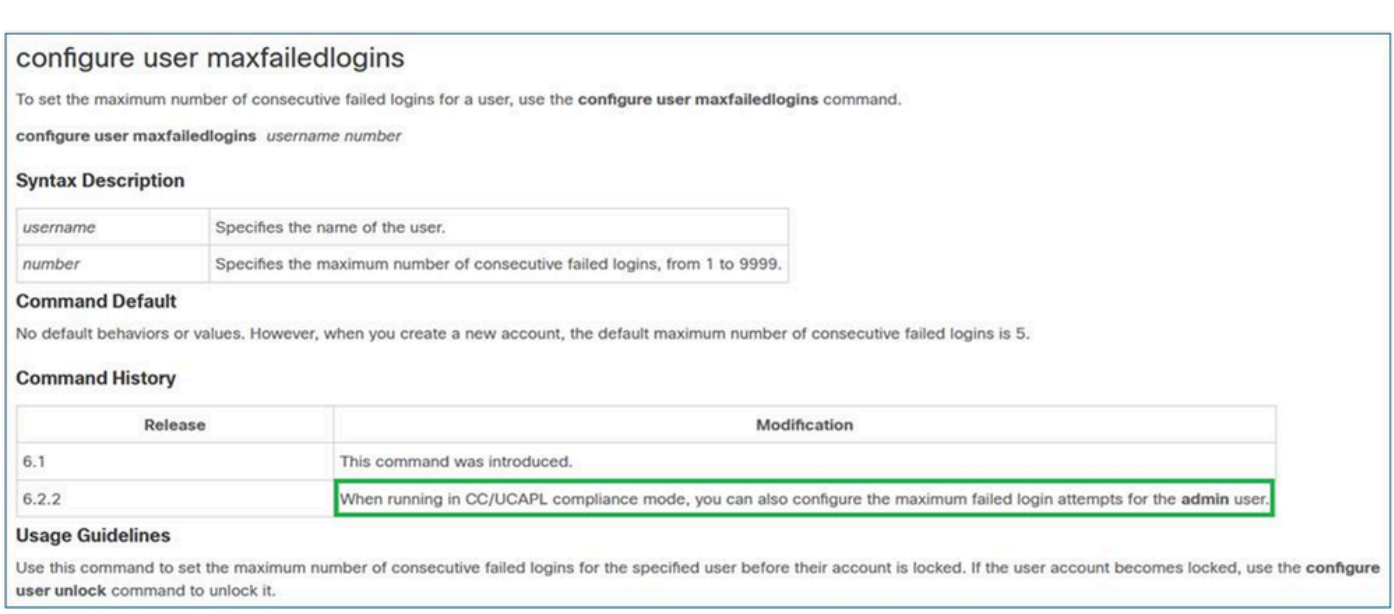
configure user maxfailedlogins admin 5

Unable to modify admin account.
```

The Solution

To overcome this restriction on an FMC-managed firewall, you must enable **compliance mode** on the firewall. This is documented in the Cisco FTD command reference:

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



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

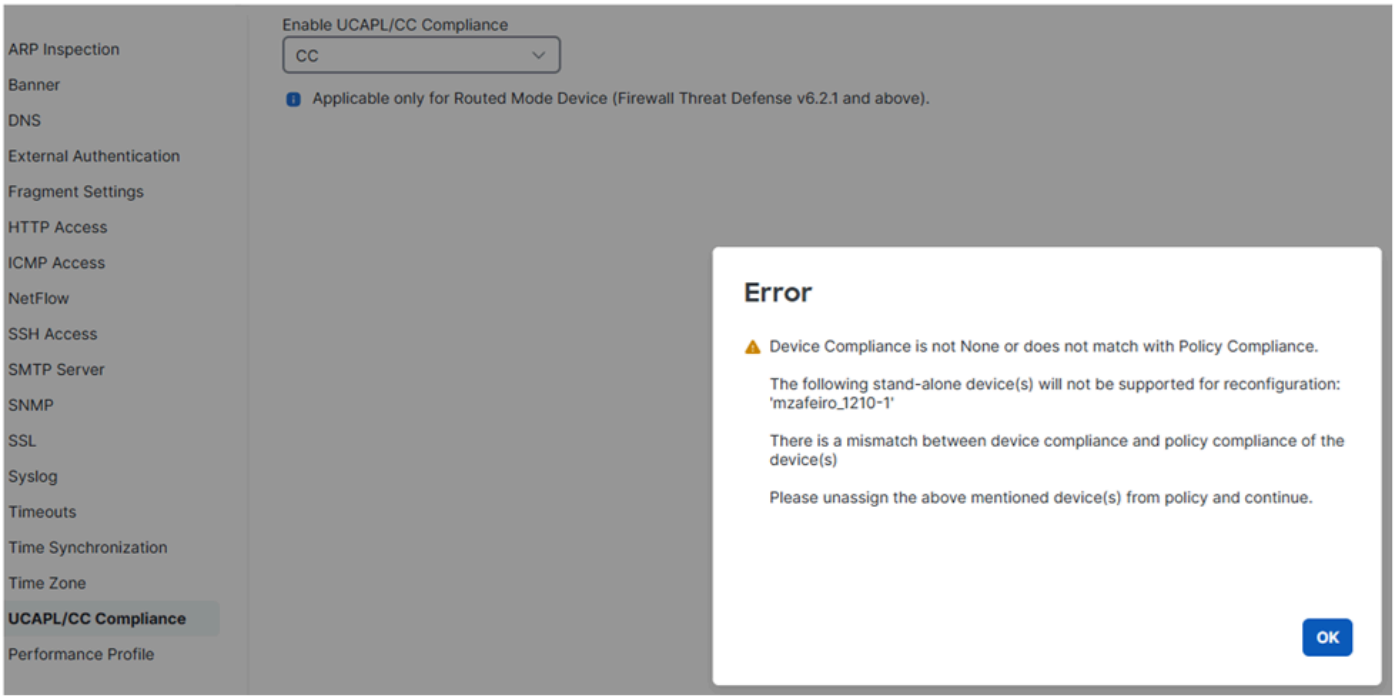
CC and UCAPL Compliance

They are security compliance standards that specify requirements for hardening security products.

In the case of **maxfailedlogins**, the related information is in Security Certifications Compliance.

Important Notes

First, remember that once you enable CC or UCAPL compliance on FTD, you cannot revert the change. If you try to



inline_image_0.png

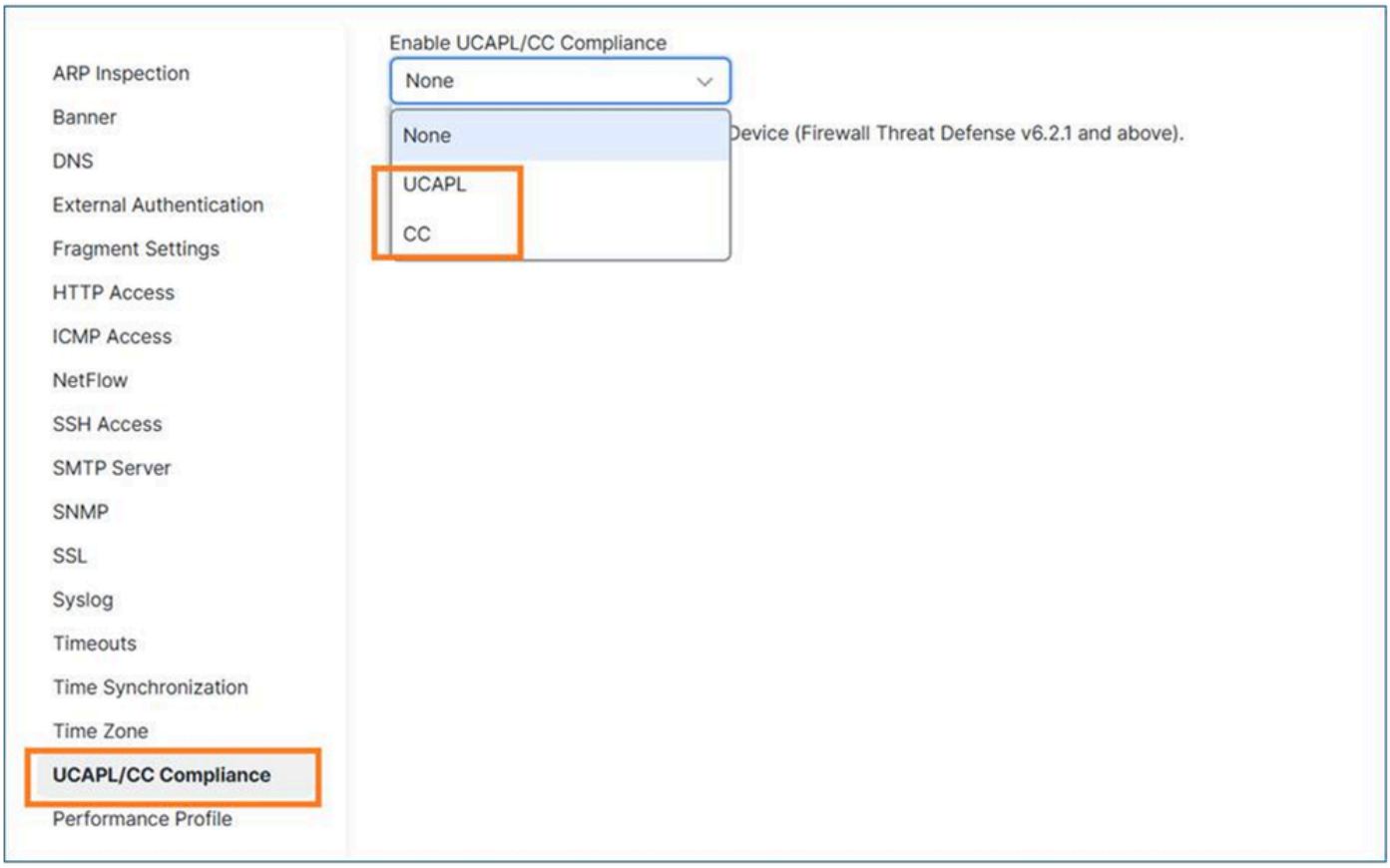
Once you enable a compliance mode and deploy the policy, the FTD reboots.

When it comes to **maxfailedlogins**, with CC you can configure up to 9999 failed attempts, while with UCAPL up to

Enable CC or UCAPL Compliance on FTD

Step 1: On FMC, you navigate to the **Devices / Platform Settings.**

Step 2: Enable one of the two compliance modes (UCAP or CC). Since the change cannot be reversed, it is highly re



inline_image_0.png

Step 3: Once this
is done, you have to assign the Platform Settings policy to the FTD (if it is not already) and **Deploy.**

Once the deployment is done, the FTD device reboots automatically:

<#root>

```
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 ...
```

Step 4: Once the firewall is up again, you can configure the **maxfailedlogins** setting. In case you chose **UCAPL**, you
in attempts:

```
<#root>

>

configure user maxfailedlogins admin 5

Unable to set limit, must be 3 or less for UCAPL mode

>
```

In case of CC, you can set up to 9999:

```
<#root>

>

configure user maxfailedlogins admin 9999


>
```

Step 5: Verify the configuration using the **show user** command:

```
<#root>

>

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

 5
```



Tip:
Ensure you have another user with **config** privileges available in case the admin user gets locked!

Unlock a Locked Admin User

Assuming you set **maxfailedlogins 3**, after 3 failed attempts the admin account gets locked:

```
<#root>

>

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 that case you have to log in with another user and unlock the admin user manually:

```
<#root>

>

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 Managed by Device Manager (FDM)

FDM does not currently support CC or UCAPL compliance modes.

Related enhancement: *CSCws76567 ENH: Add CC/UCAPL support on Firepower Device Manager*

If this functionality is critical, it is advised to discuss the prioritization of the related enhancement request, reference

Set the Maximum Number of Failed Login Attempts for Web GUI Access

Similar to the CLI log
in, this functionality is only available when CC or UCAPL compliance mode is enabled:

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

Reference

- Security Certifications Compliance Characteristics

Since CC or UCAPL modes cannot be used on FDM-
managed devices, you cannot set the maximum number of failed log
in attempts for web GUI access (see enhancement CSCws76567).

Cause

- For FMC-
  managed devices, the option is only available when CC or UCAPL compliance mode is enabled.
- For FDM-
  managed devices, an enhancement request (CSCws76567) has been filed to address this feature gap and to add

Related Content

- Cisco Technical Support & Downloads
- Cisco bug ID CSCws76567