設定FTD上本機管理員的最大失敗登入嘗試次數

問題

- 目標是為思科安全防火牆威脅防禦(FTD)上的本地管理員帳戶配置最大登入嘗試失敗次數。
- 該請求包含有關通過圖形使用者介面(GUI)和命令列介面(CLI)設定此限制的指導。
- 確保管理帳戶受到保護，防止暴力登入嘗試。

環境

- 產品：思科安全防火牆
- 軟體版本：任意
- 設定失敗登入嘗試限制所需的配置幫助

解析

有兩種不同情況，具體取決於安全防火牆的管理方式。

預設行為

預設情況下，您無法在安全防火牆上為本地管理員帳戶配置maxfailedlogins:

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

由FMC管理的防火牆

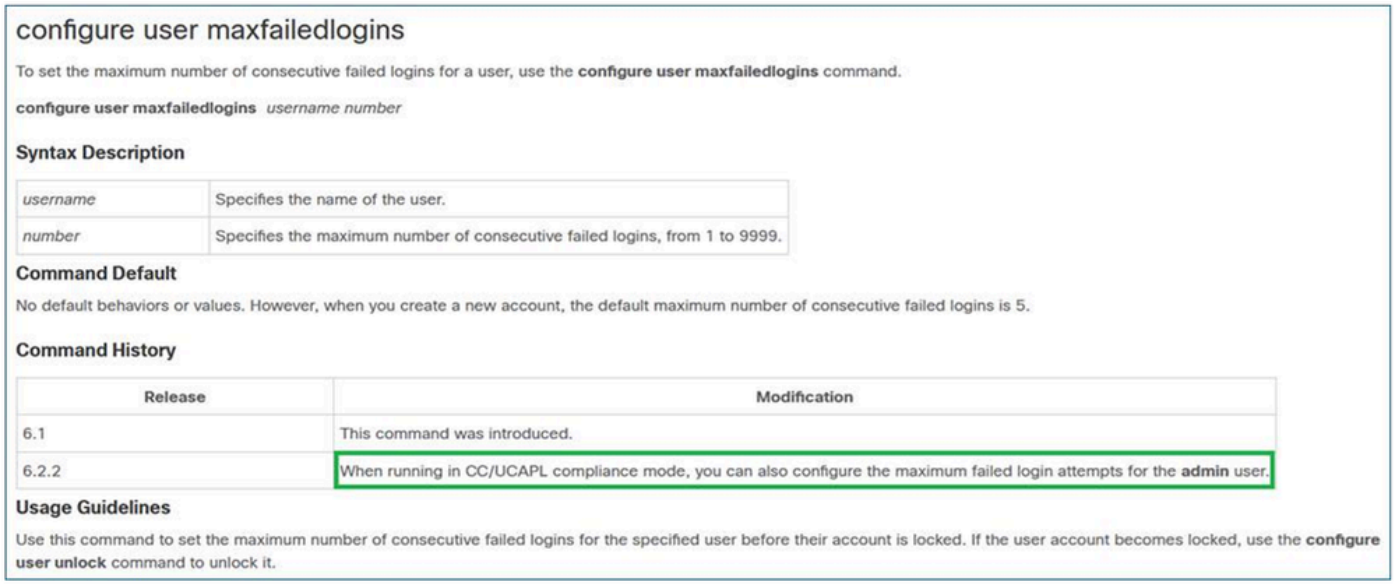
預設情況下，您無法為Cisco FMC管理的本地管理員帳戶配置maxfailedlogins:

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

解決方案

若要克服此限制，您必須在防火牆上啟用遵循性模式。Cisco FTD命令參考中對此進行了說明：

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

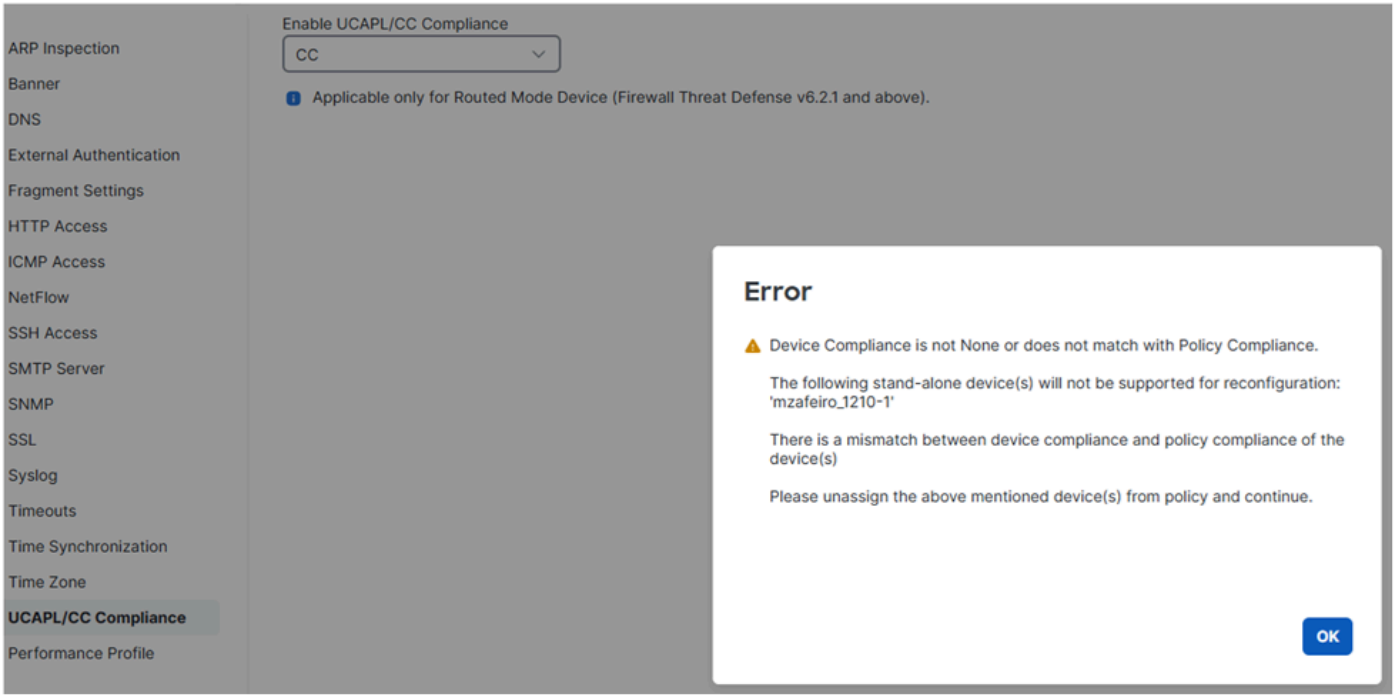
CC和UCAPL合規性

它們是安全合規性標準，指定了強化安全產品的要求。

在maxfailedlogins的情況下，相關資訊位於「Security Certifications Compliance」中。

重要附註

首先，請記住，一旦在FTD上啟用CC或UCAPL符合性，便無法還原更改。如果嘗試還原，將獲得：



inline_image_0.png

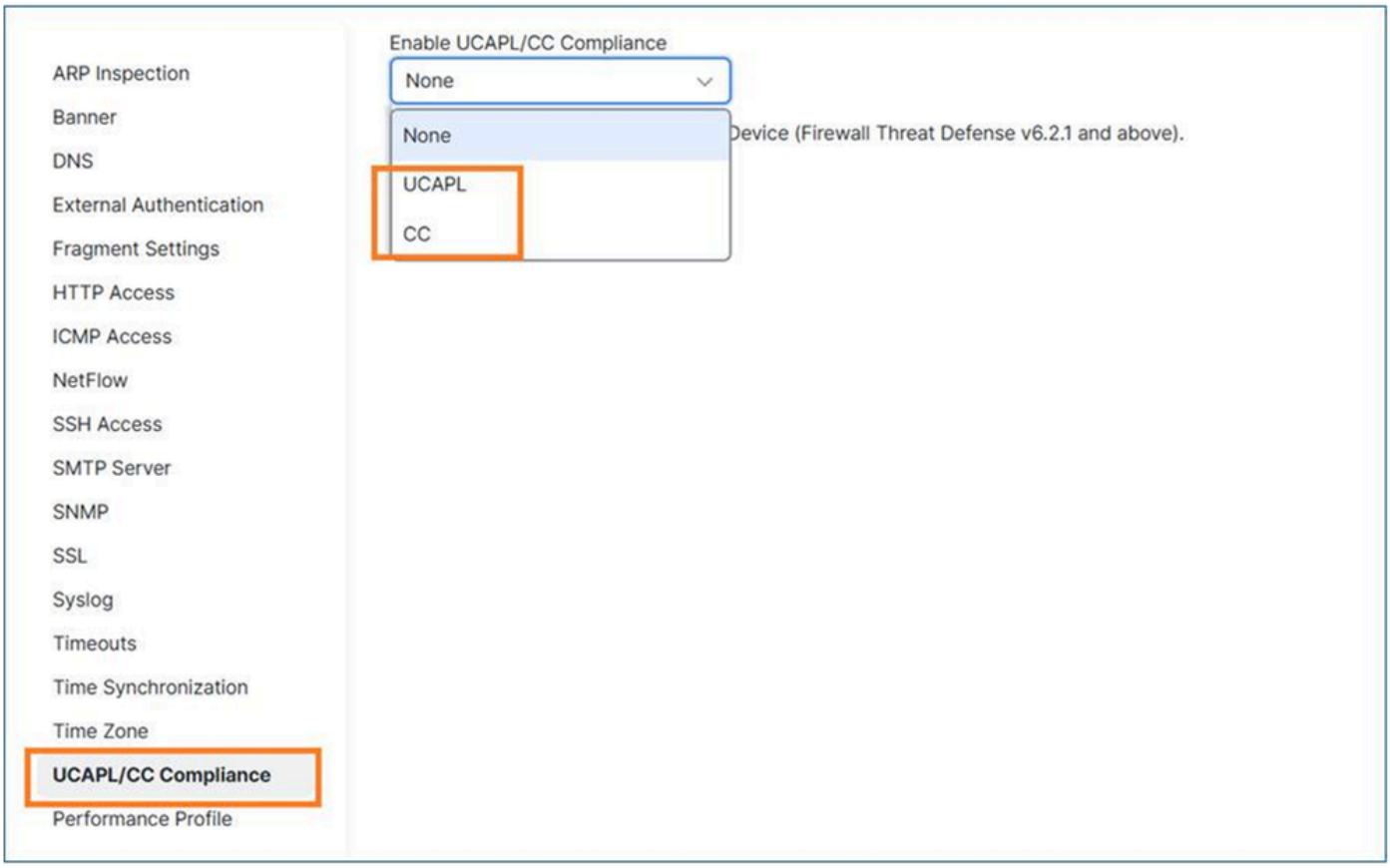
啟用合規模式並部署原則後，FTD會重新啟動。

對於maxfailedlogins，使用CC最多可以配置9999次失敗嘗試，而使用UCAPL最多可以配置3次。

在FTD上啟用CC或UCAPL合規性

第1步：在FMC上，導航至裝置/平台設定。

第2步：啟用兩種合規性模式（UCAP或CC）之一。由於無法撤消更改，因此強烈建議仔細閱讀「安全認證合規性」指南。



inline_image_0.png

第3步：完成此操作後，您必須將平台設定策略分配給FTD（如果尚未）和部署。

部署完成後，FTD裝置會自動重新開機：

```
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 ...
```

第4步：再次啟動防火牆後，可以配置maxfailedlogins 設定。如果您選擇UCAPL，最多可以配置3次失敗的登入嘗試：

```
> configure user maxfailedlogins admin 5
```

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

>
```

在抄送的情況下，您可以設定為9999:

```
> configure user maxfailedlogins admin 9999

>
```

步驟5：使用show user 命令驗證配置：

```
> 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
```

提示：確保您有另一個具有config許可權的使用者，以防管理員使用者被鎖定！

解除鎖定管理員使用者的鎖定

假設您設定maxfailedlogins 3，在嘗試3次失敗後，管理員帳戶將被鎖定：

```
> 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
```

在這種情況下，您必須使用其他使用者登入並手動解鎖管理員使用者：

```
> 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
```

由裝置管理器(FDM)管理的防火牆

FDM當前不支援CC或UCAPL合規性模式。

相關增強：CSCws76567增強版：在Firepower裝置管理器上新增CC/UCAPL支援

如果此功能非常重要，建議與您的客戶經理討論相關增強請求(稱為CSCws76567)的優先順序。

設定Web GUI訪問的最大失敗登入嘗試次數

與CLI登入類似，此功能僅在啟用CC或UCAPL合規性模式時可用：

設定Web GUI訪問的最大失敗登入嘗試次數

與CLI登入類似，此功能僅在啟用CC或UCAPL合規性模式時可用：

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

參考

- 安全認證合規性特徵

由於CC或UCAPL模式不能在FDM管理的裝置上使用，因此您無法設定Web GUI訪問的最大失敗登入嘗試次數(請參閱增強功能CSCws76567)。

原因

- 對於FMC管理的裝置，此選項僅在啟用CC或UCAPL合規性模式時可用。
- 對於FDM管理的裝置，已提交增強請求(CSCws76567)，以解決此功能差距並在防火牆裝置管理器中新增對通用標準(CC)和UCAPL合規性的支援。

相關內容

- 思科技術支援與下載
- 思科錯誤ID CSCws76567

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。