Configura numero massimo di tentativi di login non riusciti per l'amministratore locale su FTD

Problema

- L'obiettivo è configurare il numero massimo di tentativi di accesso non riusciti per gli account amministratore locali su Cisco Secure Firewall Threat Defense (FTD).
- La richiesta include istruzioni per l'impostazione di questo limite tramite l'interfaccia utente grafica (GUI) e l'interfaccia della riga di comando (CLI).
- Garantire la protezione degli account amministrativi da tentativi di accesso non autorizzati.

Ambiente

- Prodotto: Cisco Secure Firewall
- Versione del software: Any
- Assistenza per la configurazione necessaria per impostare i limiti dei tentativi di accesso non riusciti

Risoluzione

Esistono due casi diversi a seconda di come viene gestito il firewall protetto.

Comportamento predefinito

Per impostazione predefinita, non è possibile configurare maxfailedlogins per l'account admin locale sul firewall protetto:

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

Firewall gestito da FMC

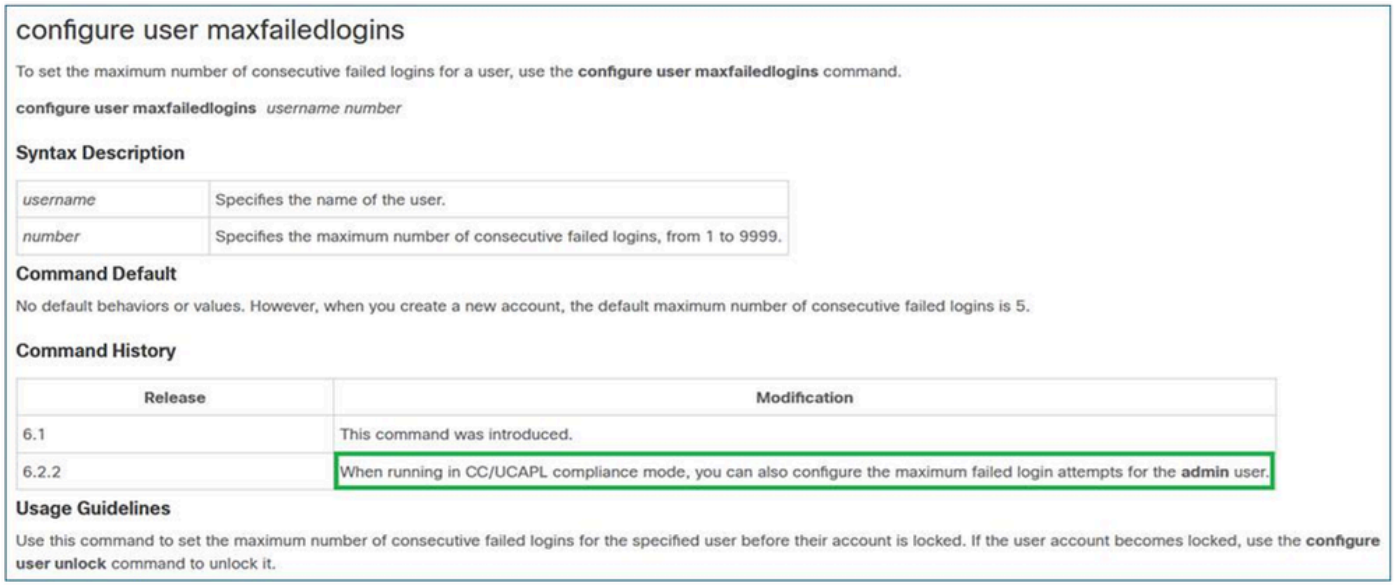
Per impostazione predefinita, non è possibile configurare maxfailedlogins per l'account amministratore locale gestito da Cisco FMC:

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

La soluzione

Per superare questa restrizione, è necessario abilitare la modalità di conformità sul firewall. Questa condizione è documentata nella guida di riferimento dei comandi di Cisco FTD:

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

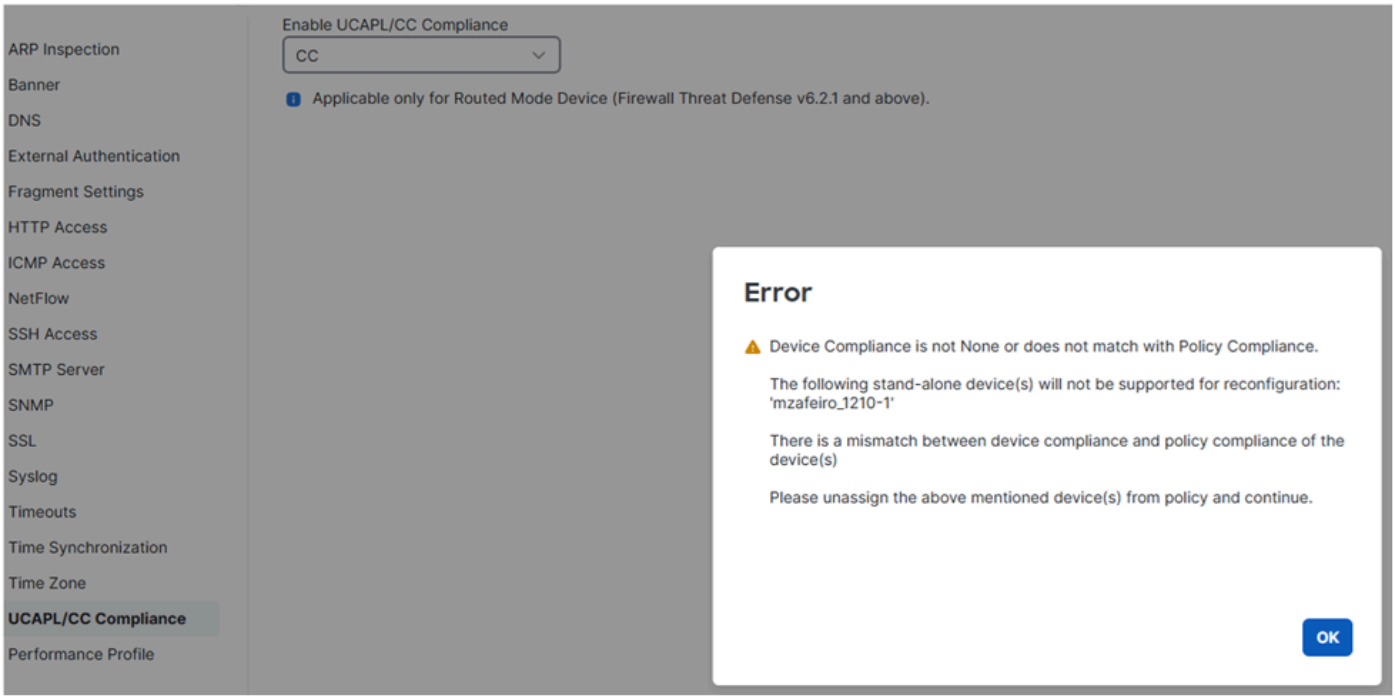
Conformità CC e UCAPL

Si tratta di standard di conformità alla sicurezza che specificano i requisiti per i prodotti di sicurezza di protezione avanzata.

Nel caso di maxfailedlogins, le informazioni correlate si trovano in Conformità alle Certificazioni di sicurezza.

Note importanti

Innanzitutto, una volta abilitata la conformità Cc o UCAPL su FTD, non è possibile annullare la modifica. Se si tenta di annullare, si ottiene:



inline_image_0.png

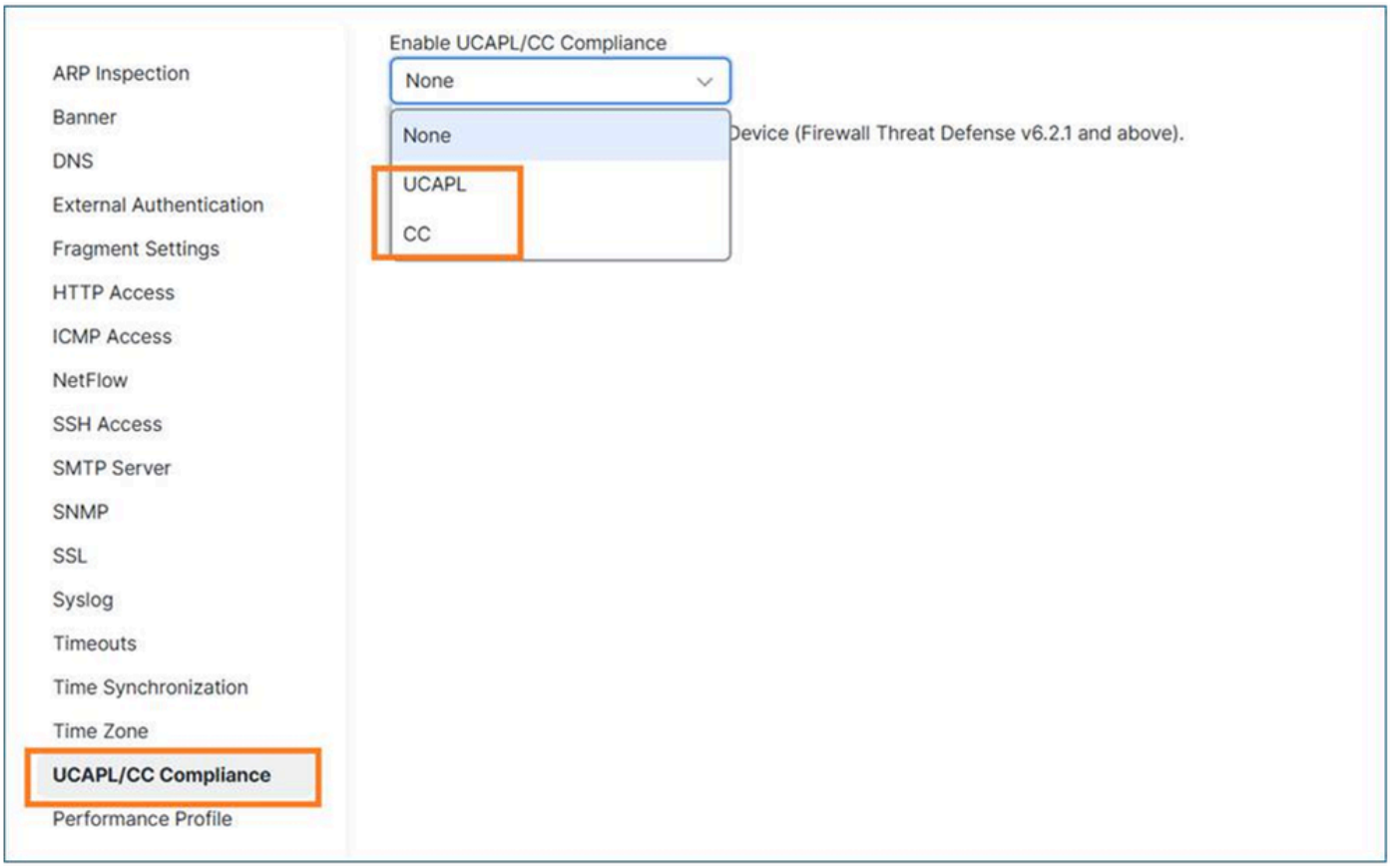
Dopo aver attivato una modalità di conformità e distribuito il criterio, l'FTD viene riavviato.

Quando si tratta di accessi maxfailedlogins, con Cc è possibile configurare fino a 9999 tentativi non riusciti, mentre con UCAPL fino a 3.

Abilita conformità CC o UCAPL su FTD

Passaggio 1: In FMC, passare a Dispositivi/Impostazioni piattaforma.

Passaggio 2: abilitare una delle due modalità di conformità (UCAP o CC). Poiché la modifica non può essere annullata, si consiglia di leggere attentamente la guida alla conformità delle certificazioni di sicurezza.



inline_image_0.png

Passo 3: Una volta fatto, è necessario assegnare il criterio Impostazioni piattaforma all'FTD (se non è già stato fatto) e Distribuire.

Al termine della distribuzione, il dispositivo FTD si riavvia automaticamente:

```
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 ...
```

Passaggio 4: Una volta riattivato il firewall, è possibile configurare l'impostazione maxfailedlogins. Se si sceglie UCAPL, è possibile configurare fino a 3 tentativi di accesso non riusciti:

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

>
```

In caso di licenza CC, è possibile impostare fino a 9999:

```
> configure user maxfailedlogins admin 9999

>
```

Passaggio 5: Verificare la configurazione utilizzando il comando 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
```

Suggerimento: Assicurarsi di disporre di un altro utente con privilegi di configurazione disponibili nel caso in cui l'utente amministratore venga bloccato.

Sbloccare un utente amministratore bloccato

Se si imposta maxfailedlogins su 3, dopo 3 tentativi non riusciti l'account admin viene bloccato:

```
> 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 tal caso, è necessario accedere con un altro utente e sbloccare manualmente l'utente amministratore:

```
> 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 gestito da Gestione dispositivi (FDM)

FDM attualmente non supporta le modalità di conformità CC o UCAPL.

Miglioramenti correlati: CSCws76567 ENH: aggiunta del supporto CC/UCAPL in Gestione periferiche di Firepower

Se questa funzionalità è fondamentale, è consigliabile discutere con l'Account Manager la definizione delle priorità della richiesta di miglioramento, a cui si fa riferimento come CSCws76567.

Impostazione del numero massimo di tentativi di login non riusciti per l'accesso tramite GUI Web

Analogamente all'accesso CLI, questa funzionalità è disponibile solo quando è abilitata la modalità di conformità CC o UCAPL:

Impostazione del numero massimo di tentativi di login non riusciti per l'accesso tramite GUI Web

Analogamente all'accesso CLI, questa funzionalità è disponibile solo quando è abilitata la modalità di conformità CC o UCAPL:

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

Riferimento

- Caratteristiche di conformità delle certificazioni di sicurezza

Poiché non è possibile utilizzare le modalità CC o UCAPL sui dispositivi gestiti da FDM, non è possibile impostare il numero massimo di tentativi di login non riusciti per l'accesso tramite GUI Web (vedere il miglioramento CSCws76567).

Causa

- Per i dispositivi gestiti da FMC, l'opzione è disponibile solo quando è attivata la modalità di conformità CC o UCAPL.
- Per i dispositivi gestiti da FDM, è stata inviata una richiesta di miglioramento (CSCws76567) per risolvere questa lacuna delle funzionalità e per aggiungere il supporto per la conformità ai Common Criteria (CC) e UCAPL in Gestione dispositivi firewall.

Contenuto correlato

- Supporto tecnico Cisco e download
- Cisco ID bug CSCws76567

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).