Configuration du nombre maximal de tentatives de connexion infructueuses pour l'administrateur local sur FTD

Problème

- L'objectif est de configurer le nombre maximal de tentatives de connexion ayant échoué pour les comptes d'administrateur local sur Cisco Secure Firewall Threat Defense (FTD).
- La demande inclut des conseils pour définir cette limite via l'interface utilisateur graphique (GUI) et l'interface de ligne de commande (CLI).
- Assurez-vous que les comptes d'administration sont protégés contre les tentatives de connexion en force.

Environnement

- Produit : Cisco Secure Firewall
- Version du logiciel : Any
- Assistance de configuration requise pour définir les limites de tentatives de connexion ayant échoué

Résolution

Il existe deux cas différents selon la façon dont le pare-feu sécurisé est géré.

Comportement par défaut

Pare-feu géré par FDM

Par défaut, vous ne pouvez pas configurer maxfailedlogins pour le compte d'administrateur local sur le pare-feu sécurisé géré par le Gestionnaire de périphériques de pare-feu (FDM) :

```
<#root>

>

configure user maxfailedlogins admin 5

Unable to modify admin account.
```

Pare-feu géré par FMC

Par défaut, vous ne pouvez pas configurer maxfailedlogins pour le compte d'administrateur local géré par Cisco Firewall Management Center (FMC) :

```
<#root>

>

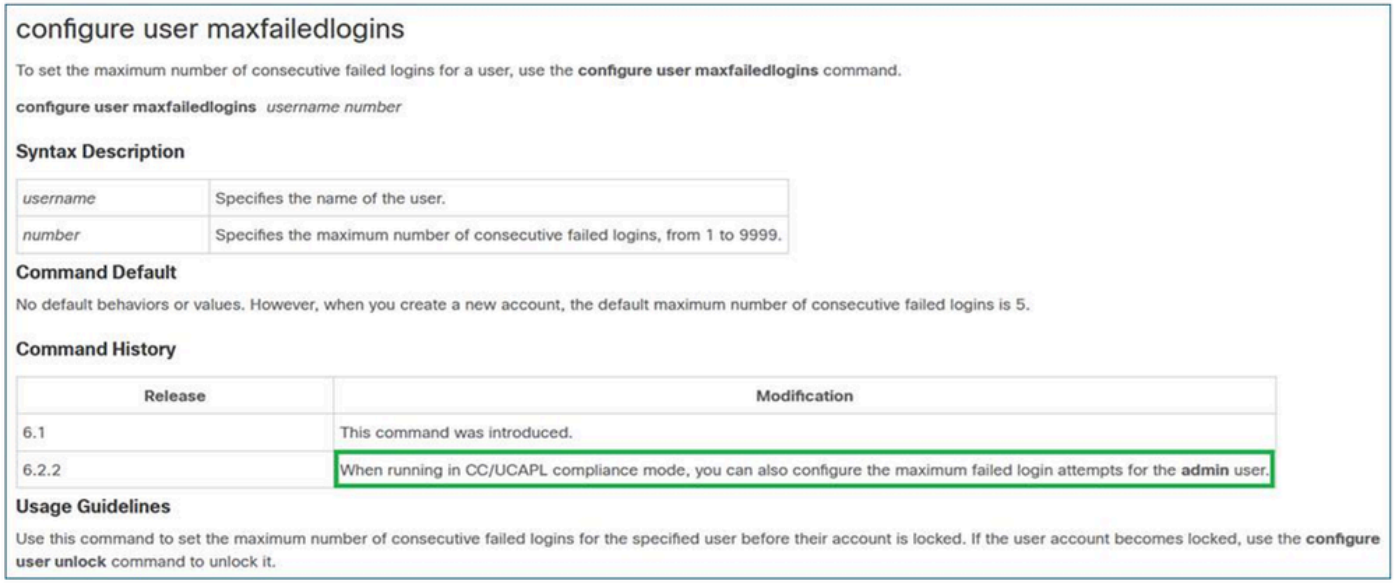
configure user maxfailedlogins admin 5

Unable to modify admin account.
```

La solution

Pour surmonter cette restriction sur un pare-feu géré par FMC, vous devez activer le mode de conformité sur le pare-feu. Ceci est documenté dans la référence de commande FTD de Cisco :

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.

image_en_ligne_0.png

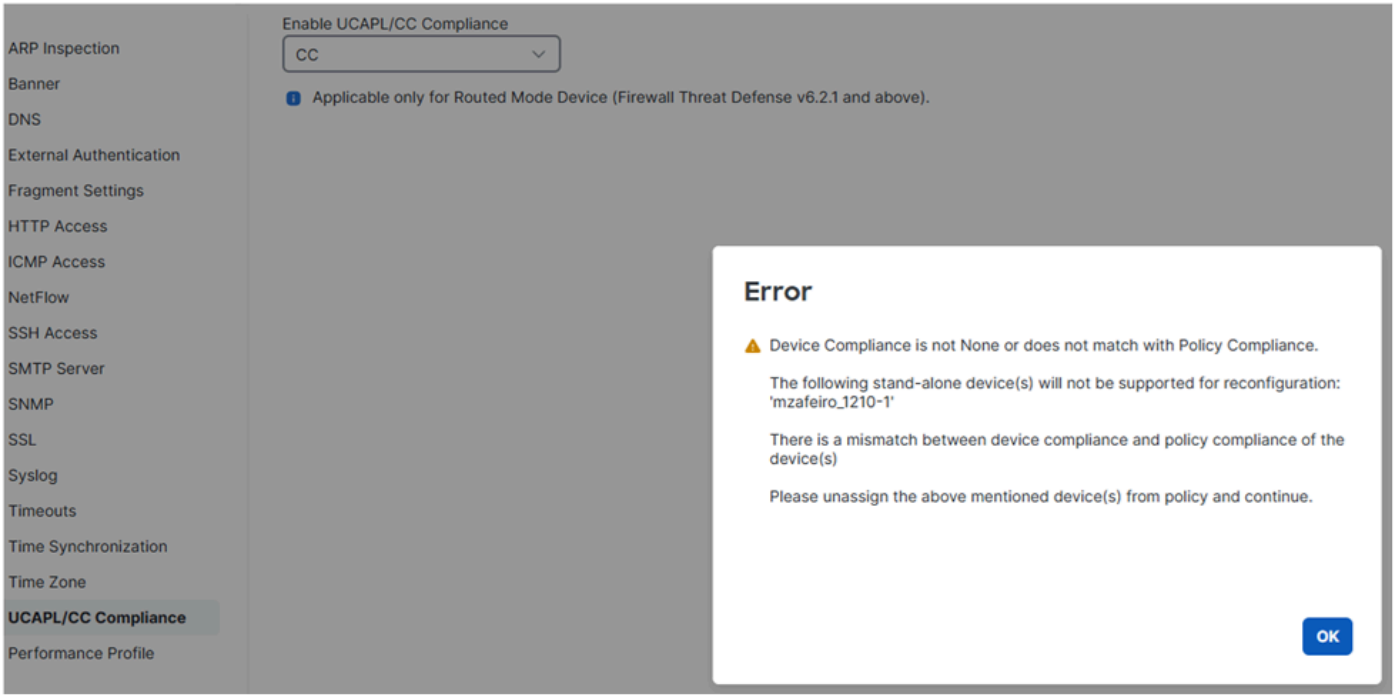
Conformité CC et UCAPL

Il s'agit de normes de conformité de sécurité qui spécifient les exigences relatives au renforcement des produits de sécurité.

Dans le cas de maxfailedlogins, les informations associées se trouvent dans Conformité des certifications de sécurité.

Remarques importantes

Tout d'abord, n'oubliez pas qu'une fois que vous avez activé la conformité CC ou UCAPL sur FTD, vous ne pouvez pas annuler la modification. Si vous essayez d'annuler, vous obtenez :



image_en_ligne_0.png

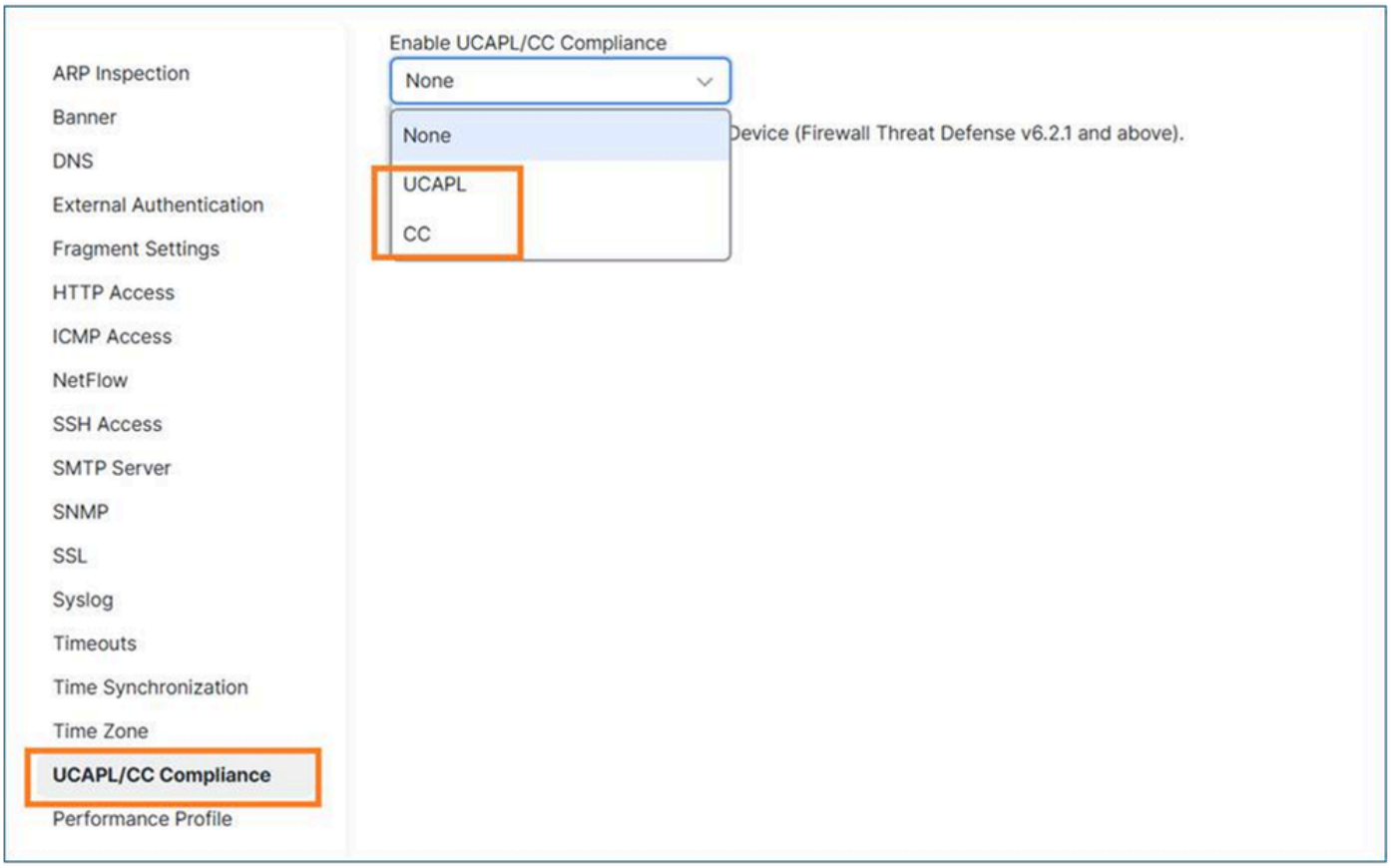
Une fois que vous avez activé un mode de conformité et déployé la stratégie, le FTD redémarre.

Quand il s'agit de maxfailedlogins, avec CC vous pouvez configurer jusqu'à 999 tentatives échouées, alors qu'avec UCAPL jusqu'à 3.

Activer la conformité CC ou UCAPL sur FTD

Étape 1 : sur FMC, accédez à Périphériques / Paramètres de plate-forme.

Étape 2 : activez l'un des deux modes de conformité (UCAP ou CC). Comme la modification ne peut pas être annulée, il est vivement recommandé de lire attentivement le guide Security Certifications Compliance.



image_en_ligne_0.png

Étape 3 : Une fois cela fait, vous devez attribuer la stratégie des paramètres de la plate-forme au FTD (si ce n'est pas déjà fait) et Déployer.

Une fois le déploiement terminé, le périphérique FTD redémarre automatiquement :

<#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 ...
```

Étape 4 : Une fois que le pare-feu est de nouveau activé, vous pouvez configurer le paramètre maxfailed logins. Si vous choisissez UCAPL, vous pouvez configurer jusqu'à 3 tentatives de connexion ayant échoué :

```
<#root>

>

configure user maxfailedlogins admin 5

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

>
```

Dans le cas de CC, vous pouvez configurer jusqu'à 9999 :

```
<#root>

>

configure user maxfailedlogins admin 9999


>
```

Étape 5 : vérifiez la configuration à l'aide de la commande show user :

```
<#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
```



Conseil : Assurez-vous que vous avez un autre utilisateur avec des privilèges de configuration disponibles au cas où l'utilisateur admin serait verrouillé !

Déverrouiller un utilisateur administrateur verrouillé

En supposant que vous définissez maxfailedlogins 3, après 3 tentatives infructueuses, le compte d'administrateur est verrouillé :

<#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

Dans ce cas, vous devez vous connecter avec un autre utilisateur et déverrouiller l'utilisateur admin manuellement :

<#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
```

Pare-feu géré par le gestionnaire de périphériques (FDM)

FDM ne prend actuellement pas en charge les modes de conformité CC ou UCAPL.

Améliorations associées : CSCws76567 ENH : Ajout de la prise en charge CC/UCAPL sur Firepower Device Manager

Si cette fonctionnalité est essentielle, il est conseillé de discuter de la hiérarchisation de la demande d'amélioration associée, référencée CSCws76567, avec votre gestionnaire de compte.

Définir le nombre maximal de tentatives de connexion ayant échoué pour l'accès Web à l'interface utilisateur graphique

Comme pour la connexion à l'interface de ligne de commande, cette fonctionnalité n'est disponible que lorsque le mode de conformité CC ou UCAPL est activé :

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

image_en_ligne_0.png

Référence

- Caractéristiques de conformité des certifications de sécurité

Étant donné que les modes CC ou UCAPL ne peuvent pas être utilisés sur les périphériques gérés par FDM, vous ne pouvez pas définir le nombre maximal de tentatives de connexion ayant échoué pour l'accès à l'interface utilisateur graphique Web (voir l'amélioration CSCws76567).

Motif

- Pour les périphériques gérés par FMC, l'option n'est disponible que lorsque le mode de conformité CC ou UCAPL est activé.
- Pour les périphériques gérés par FDM, une demande d'amélioration (CSCws76567) a été déposée afin de remédier à cette lacune et d'ajouter la prise en charge des critères communs (CC) et de la conformité UCAPL dans Firewall Device Manager.

Autres informations utiles

- Assistance technique de Cisco et téléchargements
- ID de bogue Cisco CSCws76567

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.