FTDでのローカル管理者のログイン失敗最大回数の設定

お問い合わせ内容

- 目的は、Cisco Secure Firewall Threat Defense(FTD)のローカル管理者アカウントで失敗するログイン試行の最大数を設定することです。
- 要求には、グラフィカルユーザインターフェイス(GUI)とコマンドラインインターフェイス(CLI)の両方を使用してこの制限を設定するためのガイダンスが含まれています。
- 管理アカウントをブルートフォースログインの試行から保護する。

環境

- 製品：Cisco Secure Firewall
- ソフトウェアバージョン：任意
- 失敗したログイン試行の制限の設定に必要な設定のサポート

解決策

セキュアファイアウォールの管理方法に応じて、2つの異なるケースがあります。

デフォルト動作

デフォルトでは、セキュアファイアウォールのローカル管理者アカウントにmaxfailedloginsを設定することはできません。

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

FMCで管理されるファイアウォール

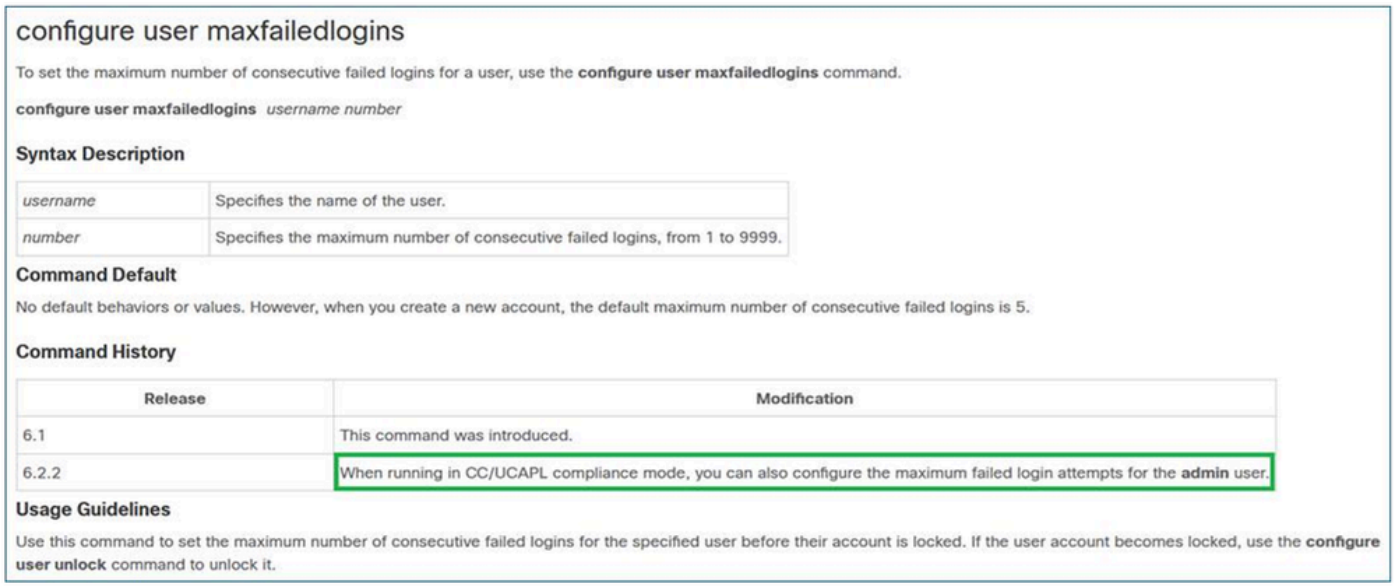
デフォルトでは、Cisco FMCによって管理されるローカル管理者アカウントにmaxfailedloginsを設定することはできません。

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

解決策

この制限を克服するには、ファイアウォールでコンプライアンスモードを有効にする必要があります。 これは、Cisco FTDコマンドリファレンスに記載されています。

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 (インラインイメージ_0.png)

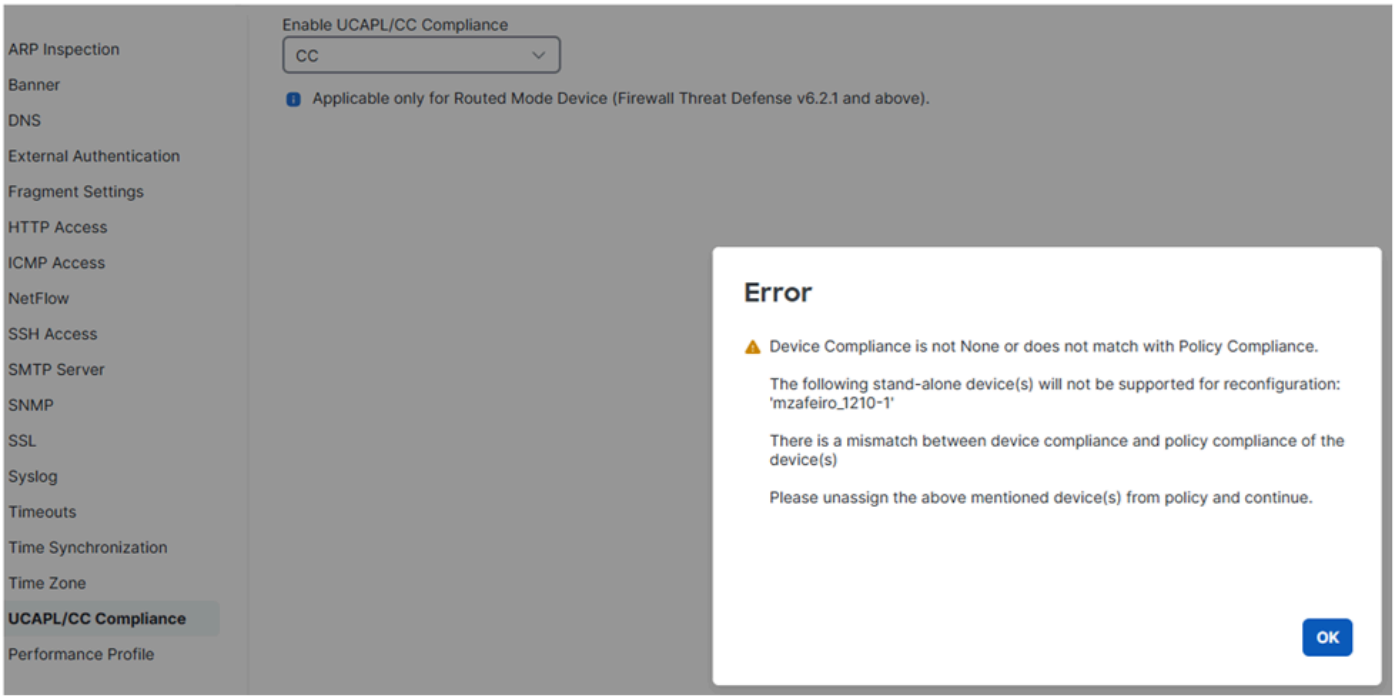
CCおよびUCAPL準拠

セキュリティ製品を強化するための要件を指定するセキュリティコンプライアンス標準です。

maxfailedloginsの場合、関連情報はSecurity Certifications Complianceにあります。

重要事項

まず、FTDでCCまたはUCAPLコンプライアンスを有効にすると、変更を元に戻せなくなります。 元に戻そうとすると、次のようになります。



inline_image_0.png（インラインイメージ_0.png）

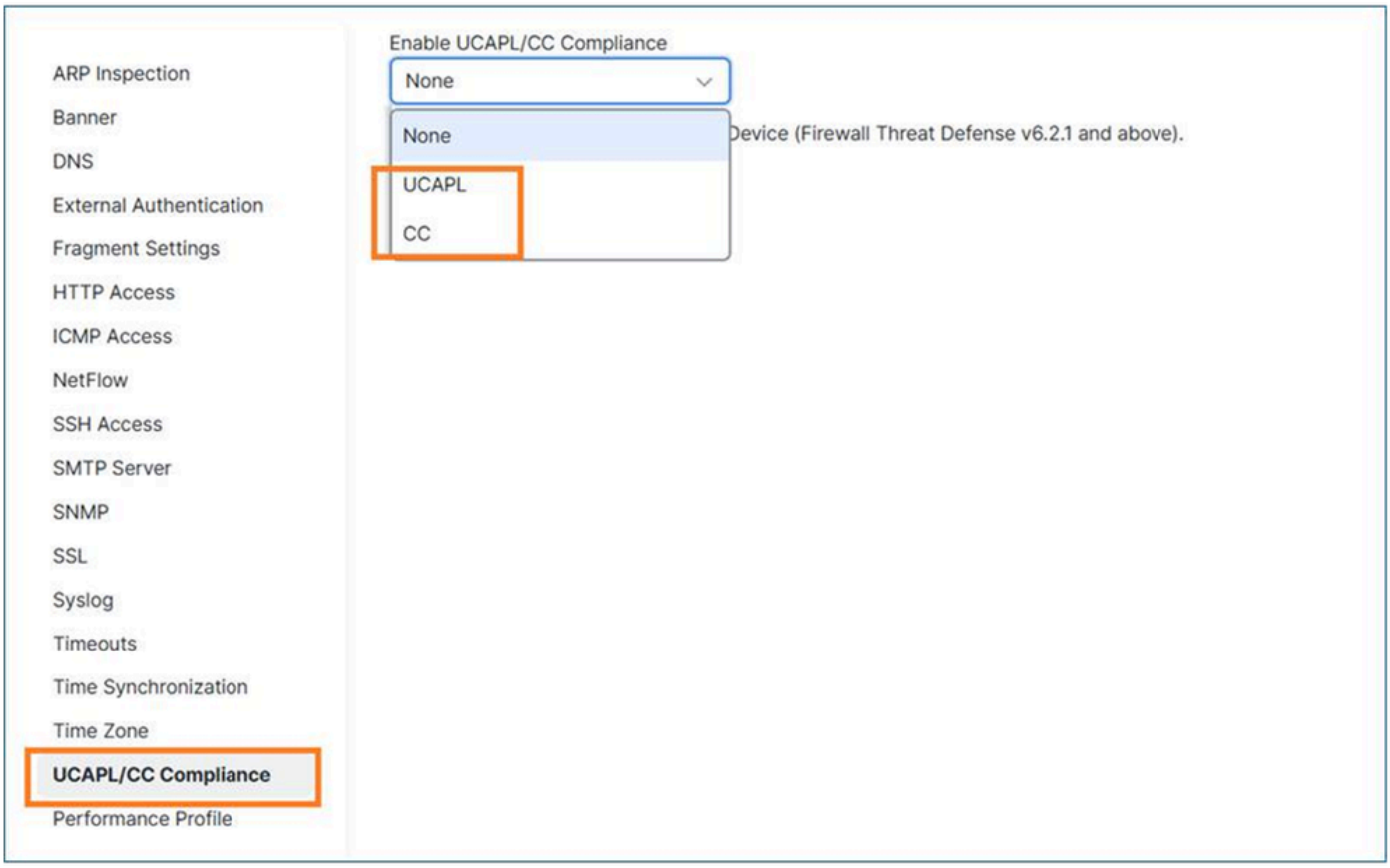
コンプライアンスモードを有効にしてポリシーを展開すると、FTDがリブートします。

maxfailedloginsの場合、CCを使用すると最大9999件の失敗の試行を設定できますが、UCAPLを使用すると最大3件まで設定できます。

FTDでCCまたはUCAPL準拠を有効にする

ステップ1:FMCで、デバイス/プラットフォーム設定に移動します。

ステップ2:2つのコンプライアンスモード（UCAPまたはCC）のいずれかを有効にします。 変更は取り消すことができないため、『Security Certifications Compliance guide（セキュリティ認定コンプライアンスガイド）』をよくお読みになることを強くお勧めします。



inline_image_0.png (インラインイメージ_0.png)

ステップ3：これが完了したら、プラットフォーム設定ポリシーをFTDに割り当て（まだ割り当てられていない場合）、展開する必要があります。

導入が完了すると、FTDデバイスは自動的にリブートします。

```
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 ...
```

ステップ4：ファイアウォールが再起動したら、maxfailedlogins 設定を構成できます。 UCAPLを選択した場合は、最大3回までのログイン試行の失敗を設定できます。

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

>
```

CCの場合は、9999まで設定できます。

```
> configure user maxfailedlogins admin 9999

>
```

ステップ5:show userコマンドを使用して、設定を確認します。

```
> 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
```

ヒント：管理者ユーザがロックされた場合に備えて、config権限を持つ別のユーザを用意しておいてください。

ロックされた管理者ユーザのロック解除

maxfailedlogins 3を設定していると仮定すると、3回失敗した後に管理者アカウントがロックされます。

```
> 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
```

その場合は、別のユーザでログインし、管理者ユーザのロックを手動で解除する必要があります。

```
> 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
```

デバイスマネージャ(FDM)で管理されるファイアウォール

FDMは現在、CCまたはUCAPLコンプライアンスモードをサポートしていません。

関連する機能拡張：CSCws76567 ENH:Firepower Device ManagerでのCC/UCAPLサポートの追加

この機能が重要な場合は、CSCws76567で参照される関連する機能拡張要求のプライオリティ設定について、担当のアカウントマネージャと話し合うことをお勧めします。

Web GUIアクセスで失敗するログイン試行の最大数の設定

CLIログインと同様に、この機能はCCまたはUCAPLコンプライアンスモードが有効になっている場合にのみ使用できます。

Web GUIアクセスで失敗するログイン試行の最大数の設定

CLIログインと同様に、この機能はCCまたはUCAPLコンプライアンスモードが有効になっている場合にのみ使用できます。

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 (インラインイメージ_0.png)

参考

- セキュリティ認定コンプライアンスの特性

FDM管理対象デバイスではCCまたはUCAPLモードを使用できないため、Web GUIアクセスのログイン試行の失敗回数の最大値を設定できません(拡張機能CSCws76567を参照)。

原因

- FMC管理対象デバイスでは、CCまたはUCAPLコンプライアンスモードが有効になっている場合にのみ、このオプションを使用できます。
- FDM管理対象デバイスに関して、この機能ギャップに対処し、Firewall Device ManagerのCommon Criteria(CC)およびUCAPL準拠のサポートを追加するために、機能拡張要求(CSCws76567)が提出されています。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード
- Cisco Bug ID CSCws76567

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。