Configuración del número máximo de intentos fallidos de inicio de sesión para el administrador local en FTD

Problema

- El objetivo es configurar el número máximo de intentos fallidos de inicio de sesión para las cuentas de administrador local en Cisco Secure Firewall Threat Defence (FTD).
- La solicitud incluye instrucciones para establecer este límite a través de la interfaz gráfica de usuario (GUI) y la interfaz de línea de comandos (CLI).
- Asegúrese de que las cuentas administrativas estén protegidas contra intentos de inicio de sesión por fuerza bruta.

Entorno

- Producto: Cisco Secure Firewall
- Versión del software: Cualquiera
- Se necesita ayuda para configurar los límites de intentos de inicio de sesión fallidos

Resolución

Existen dos casos diferentes en función de cómo se gestione Secure Firewall.

Comportamiento predeterminado

De forma predeterminada, no puede configurar maxfailedlogins para la cuenta de administrador local en el firewall seguro:

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

Firewall gestionado por FMC

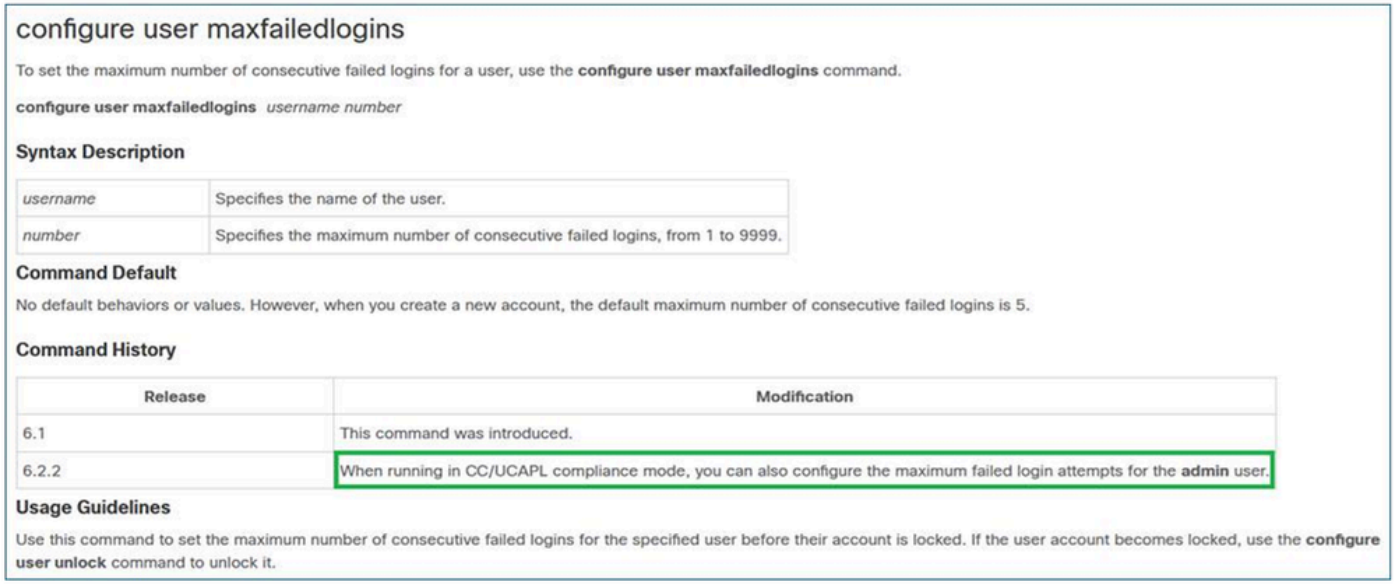
De forma predeterminada, no puede configurar maxfailedlogins para la cuenta de administrador local administrada por Cisco FMC:

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

La solución

Para superar esta restricción, debe habilitar el modo de cumplimiento en el firewall. Esto se documenta en la referencia de comandos de 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

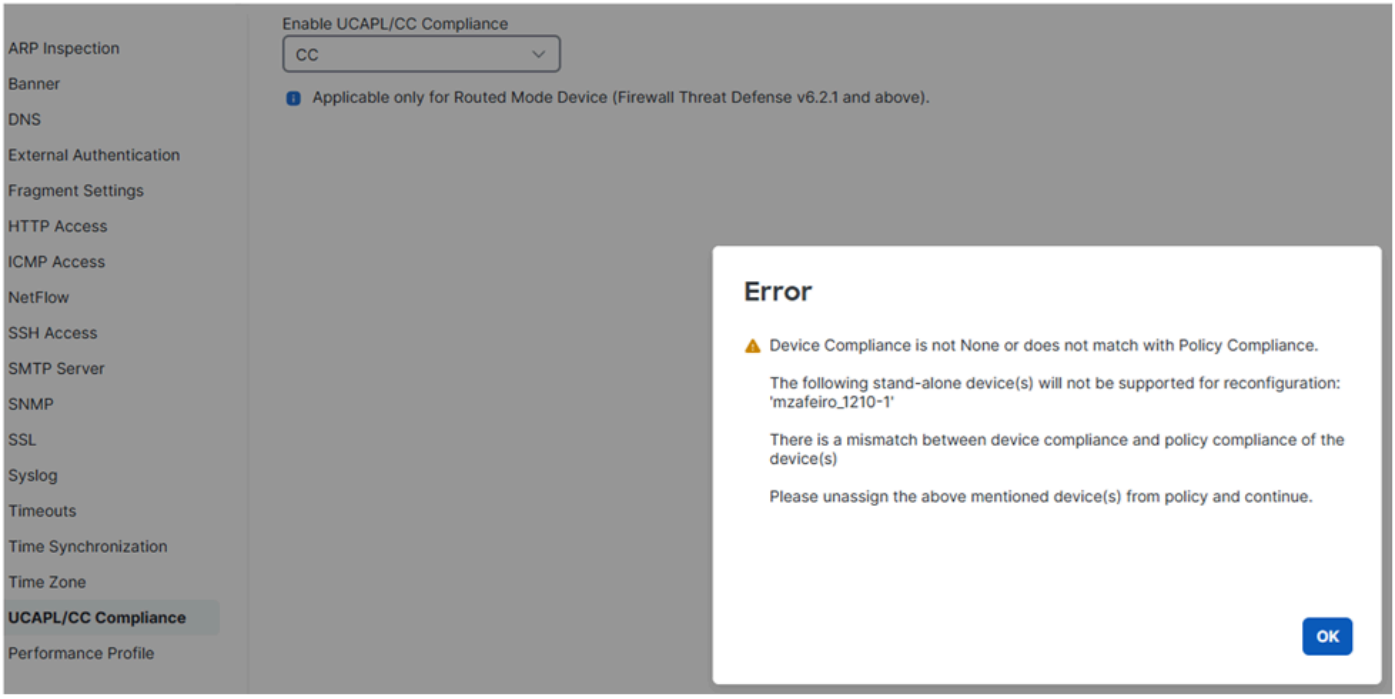
Conformidad con CC y UCAPL

Se trata de estándares de seguridad que especifican requisitos para reforzar los productos de seguridad.

En el caso de maxfailedlogins, la información relacionada se encuentra en Cumplimiento de Certificaciones de Seguridad.

Notas importantes

En primer lugar, recuerde que una vez que active la conformidad con CC o UCAPL en FTD, no podrá revertir el cambio. Si intenta revertir, obtendrá:



inline_image_0.png

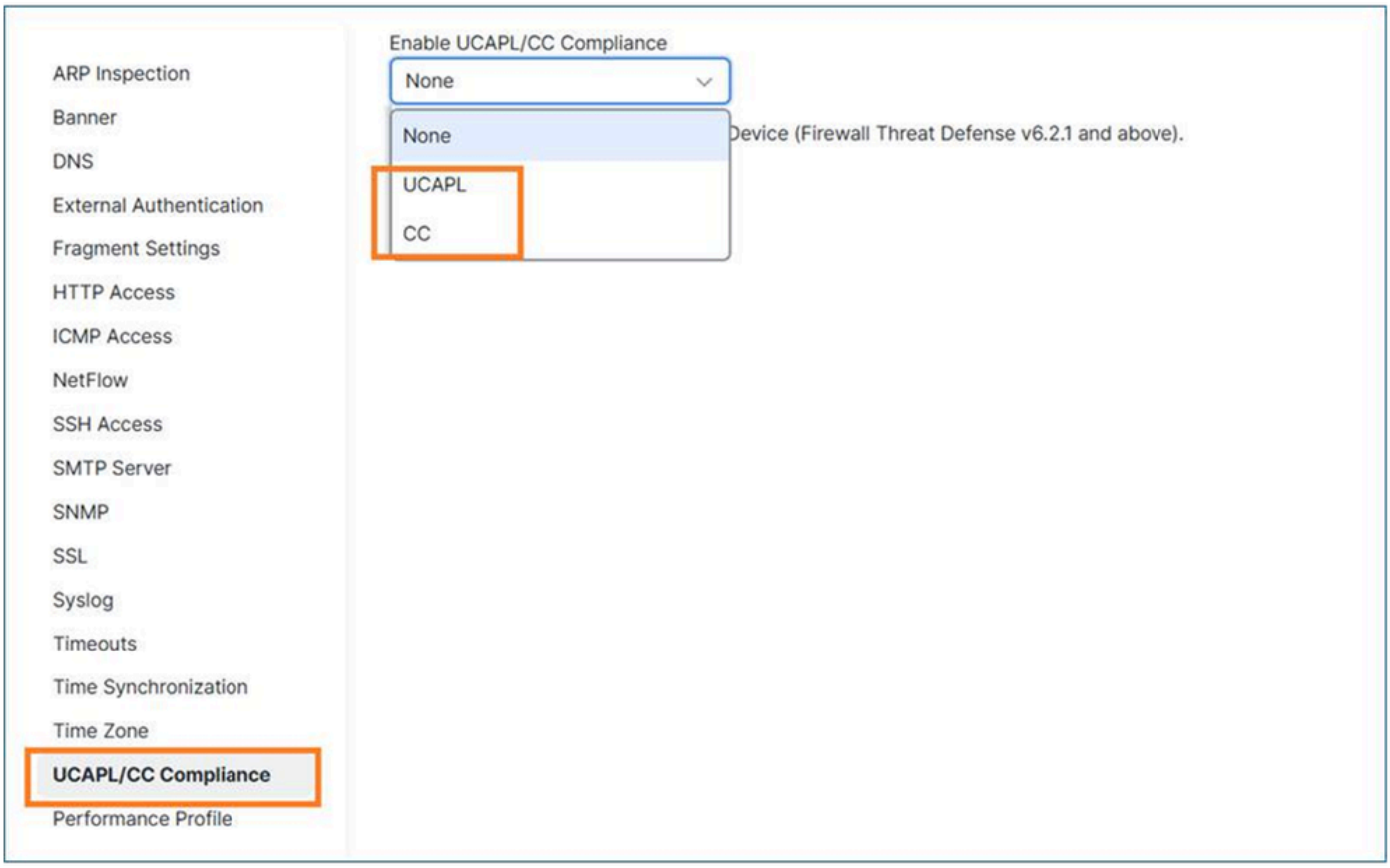
Una vez que se activa un modo de conformidad e implementa la política, el FTD se reinicia.

Cuando se trata de maxfailedlogins, con CC puede configurar hasta 9999 intentos fallidos, mientras que con UCAPL hasta 3.

Habilitación del cumplimiento de CC o UCAPL en FTD

Paso 1: En FMC, acceda a Devices / Platform Settings (Dispositivos / Parámetros de la plataforma).

Paso 2: Habilite uno de los dos modos de cumplimiento (UCAP o CC). Dado que el cambio no se puede revertir, se recomienda leer detenidamente la guía de cumplimiento de certificaciones de seguridad.



inline_image_0.png

Paso 3: Una vez hecho esto, debe asignar la directiva de configuración de la plataforma al FTD (si aún no lo está) y a la implementación.

Una vez finalizada la implementación, el dispositivo FTD se reinicia automáticamente:

```
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 ...
```

Paso 4: Una vez que el firewall esté activo de nuevo, puede configurar el valor maxfailedlogins. En caso de que elija UCAPL, puede configurar hasta 3 intentos de inicio de sesión fallidos:

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

>
```

En el caso de CC, puede configurar hasta 9999:

```
> configure user maxfailedlogins admin 9999

>
```

Paso 5: Verifique la configuración mediante el 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
```

Consejo: Asegúrese de que tiene otro usuario con privilegios de configuración disponibles en caso de que el usuario administrador se bloquee.

Desbloqueo de un usuario administrador bloqueado

Suponiendo que establece maxfailedlogins 3, después de 3 intentos fallidos la cuenta de administrador se bloquea:

```
> 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
```

En ese caso, debe iniciar sesión con otro usuario y desbloquear el usuario administrador manualmente:

```
> 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 administrado por el administrador de dispositivos (FDM)

FDM no admite actualmente los modos de conformidad con CC o UCAPL.

Mejora relacionada: CSCws76567 ENH: añada compatibilidad con CC/UCAPL en el administrador de dispositivos Firepower

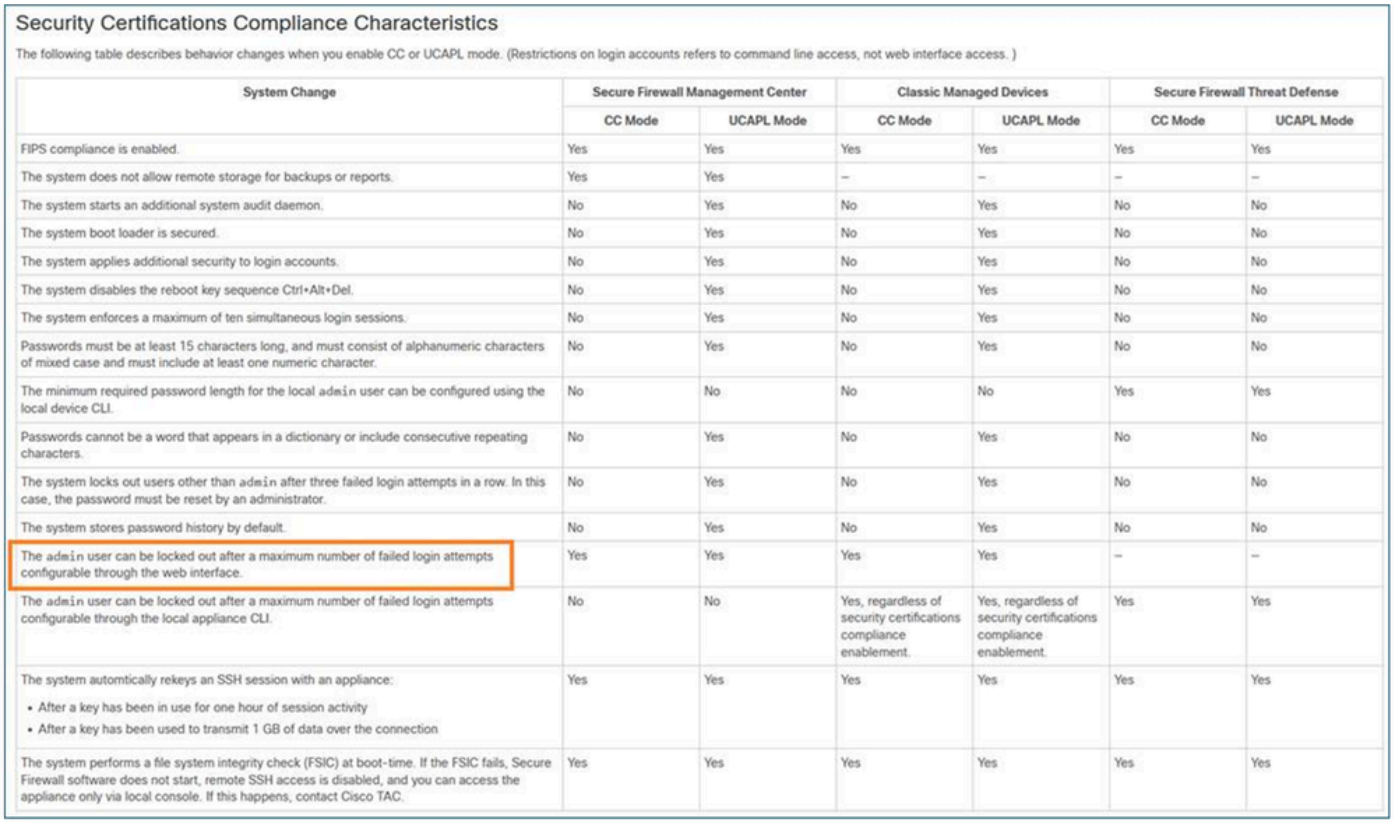
Si esta funcionalidad es crítica, se recomienda discutir la priorización de la solicitud de mejora relacionada, a la que se hace referencia como CSCws76567, con su gerente de cuentas.

Establecer el número máximo de intentos fallidos de inicio de sesión para el acceso a la GUI web

De forma similar al inicio de sesión de CLI, esta funcionalidad solo está disponible cuando el modo de cumplimiento de CC o UCAPL está habilitado:

Establecer el número máximo de intentos fallidos de inicio de sesión para el acceso a la GUI web

De forma similar al inicio de sesión de CLI, esta funcionalidad solo está disponible cuando el modo de cumplimiento de CC o UCAPL está habilitado:



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

Referencia

- Características de cumplimiento de certificaciones de seguridad

Dado que los modos CC o UCAPL no se pueden utilizar en dispositivos gestionados por FDM, no puede establecer el número máximo de intentos fallidos de inicio de sesión para el acceso a la GUI web (consulte la mejora CSCws76567).

Causa

- En el caso de los dispositivos gestionados por FMC, esta opción solo está disponible cuando está activado el modo de conformidad con CC o UCAPL.
- En el caso de los dispositivos gestionados por FDM, se ha cursado una solicitud de mejora (CSCws76567) para subsanar esta carencia de funciones y añadir compatibilidad con Common Criteria (CC) y UCAPL en el administrador de dispositivos de firewall.

Contenido relacionado

- Soporte técnico y descargas de Cisco
- ID de bug de Cisco CSCws76567

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).