Configurar o Máximo de Tentativas de Logon com Falha para o Administrador Local no FTD

Problema

- O objetivo é configurar o número máximo de tentativas de login com falha para contas de administrador local no Cisco Secure Firewall Threat Defense (FTD).
- A solicitação inclui orientação para definir esse limite por meio da interface gráfica do usuário (GUI) e da interface de linha de comando (CLI).
- Verifique se as contas administrativas estão protegidas contra tentativas de login forçado.

Ambiente

- Produto: Cisco Secure Firewall
- Versão do software: qualquer
- Assistência de configuração necessária para definir limites de tentativas de login com falha

Resolução

Há dois casos diferentes, dependendo de como o firewall seguro é gerenciado.

Comportamento padrão

Por padrão, você não pode configurar maxfailedlogins para a conta de administrador local no firewall seguro:

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

Firewall gerenciado pelo FMC

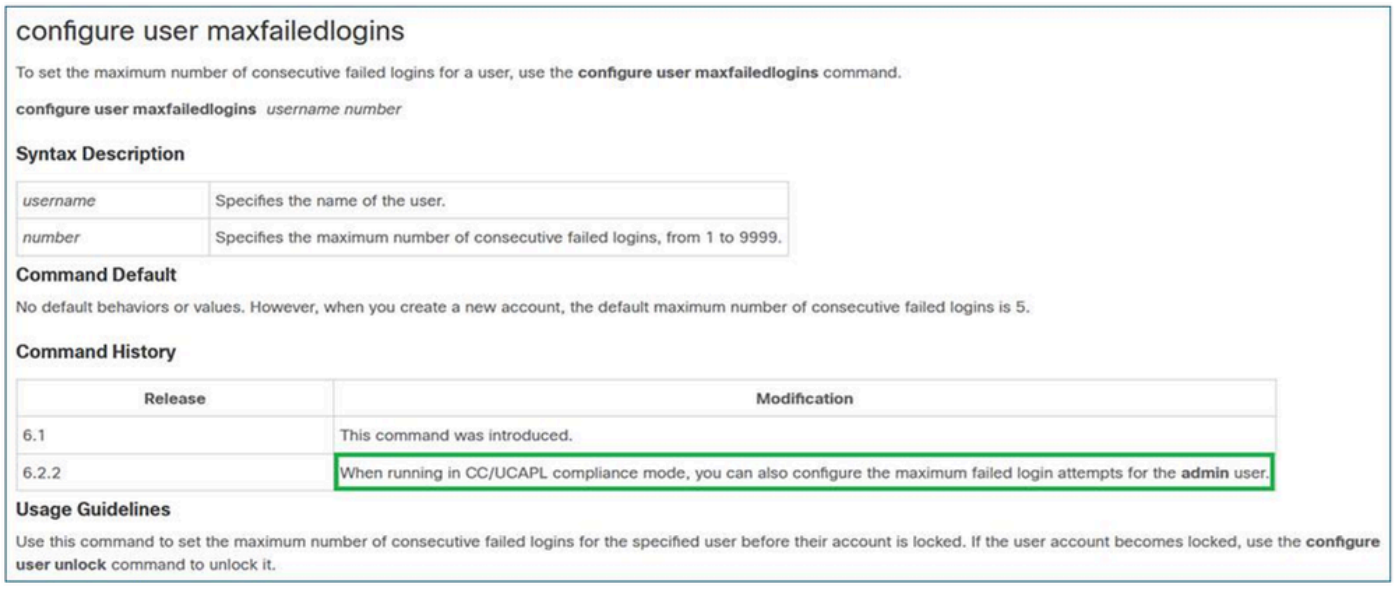
Por padrão, você não pode configurar maxfailedlogins para a conta de administrador local gerenciada pelo Cisco FMC:

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

A solução

Para superar essa restrição, você deve habilitar o modo de conformidade no firewall. Isso está documentado na referência de comando do 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

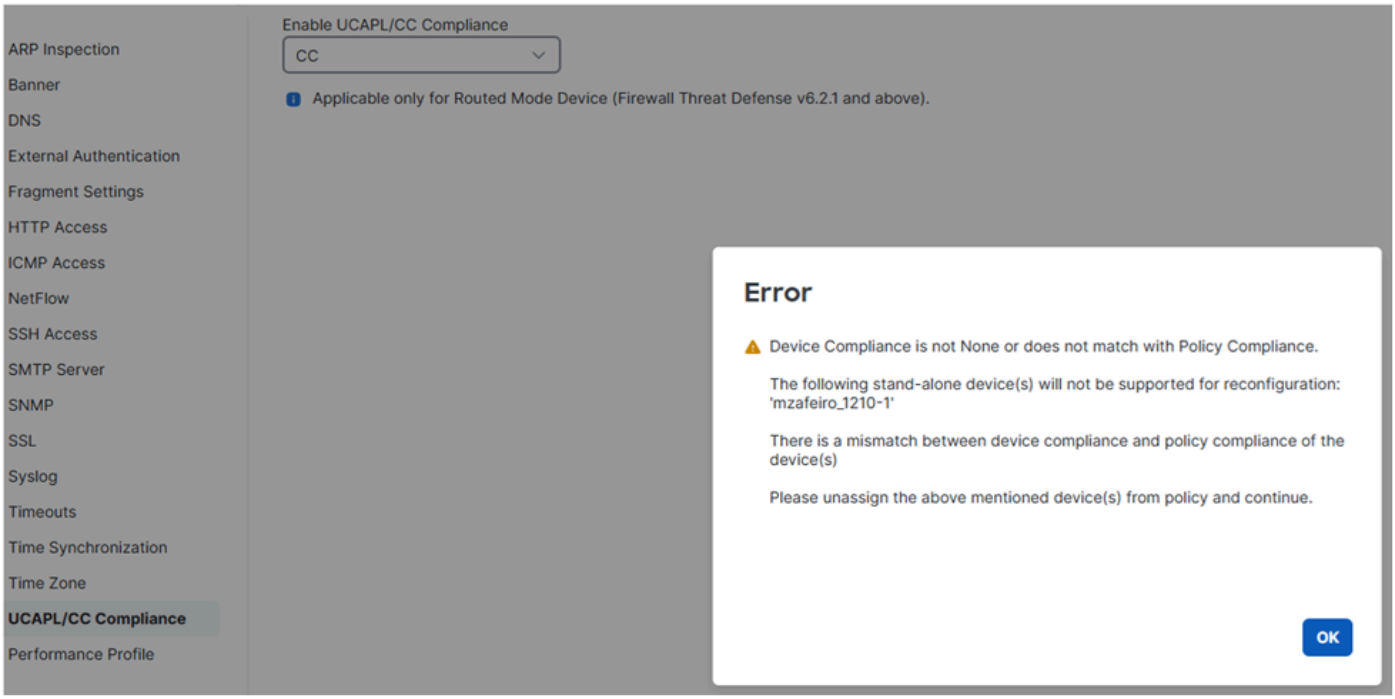
Conformidade com CC e UCAPL

São padrões de conformidade de segurança que especificam requisitos para fortalecer produtos de segurança.

No caso de maxfailedlogins, as informações relacionadas estão em Conformidade com certificações de segurança.

Notas importantes

Primeiro, lembre-se de que, depois de ativar a conformidade com CC ou UCAPL no FTD, você não poderá reverter a alteração. Se tentar reverter, você obterá:



inline_image_0.png

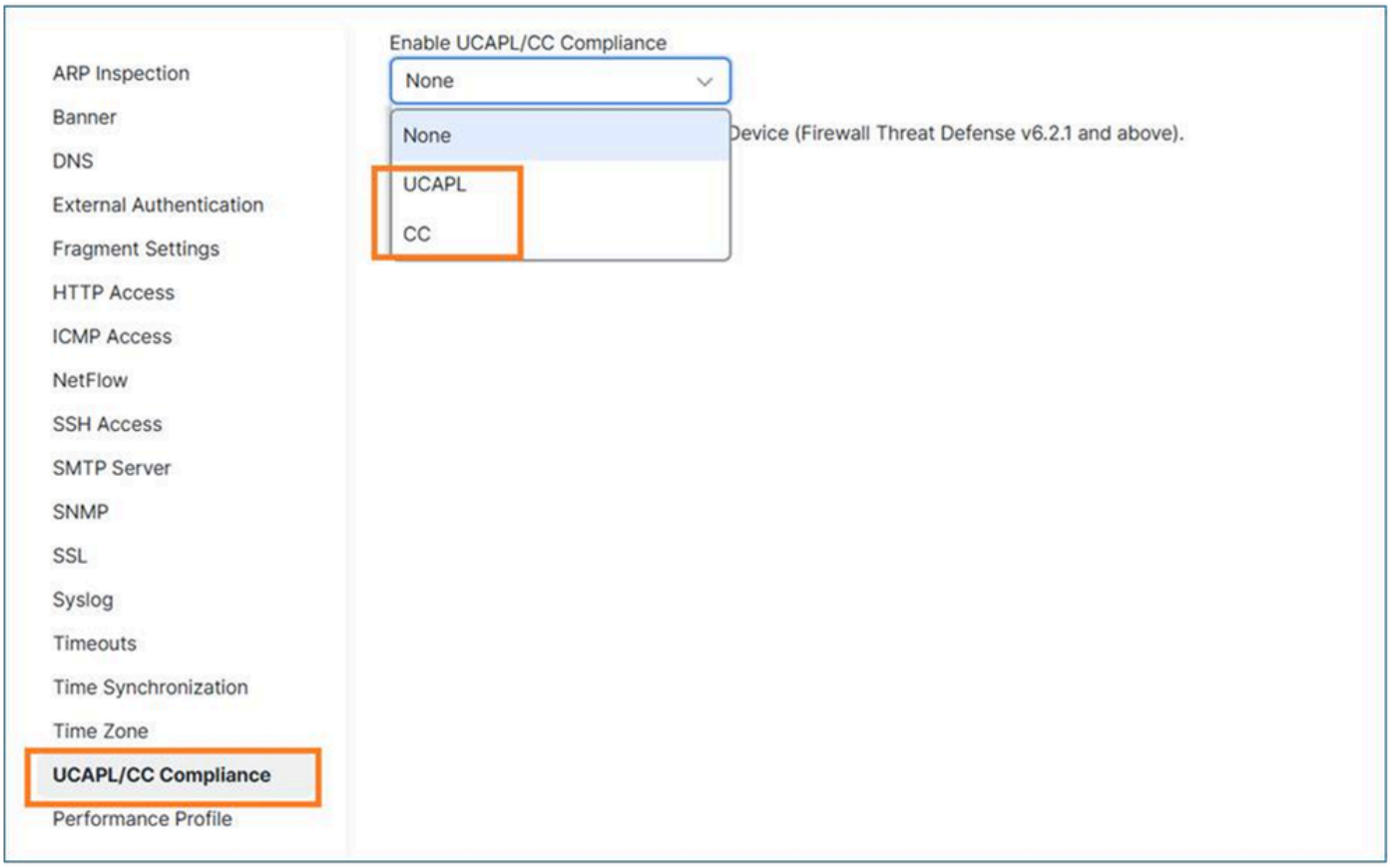
Quando você habilita um modo de conformidade e implanta a política, o FTD é reinicializado.

Quando se trata de maxfailedlogins, com o CC você pode configurar até 9999 tentativas falhas, enquanto com o UCAPL pode configurar até 3.

Habilitar conformidade com CC ou UCAPL no FTD

Etapa 1: no FMC, você navegará para Devices / Platform Settings.

Etapa 2: Ative um dos dois modos de conformidade (UCAP ou CC). Como a alteração não pode ser revertida, é altamente recomendável ler atentamente o Guia de Conformidade de Certificações de Segurança.



inline_image_0.png

Etapa 3: depois que isso for feito, você deve atribuir a política Configurações de plataforma ao FTD (se ainda não estiver) e Implantar.

Quando a implantação estiver concluída, o dispositivo FTD será reinicializado 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 ...
```

Etapa 4: Quando o firewall estiver ativo novamente, você poderá configurar a configuração maxfailedlogins . Caso você escolha UCAPL, poderá configurar até 3 tentativas de login com falha:

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

>
```

No caso de CC, você pode configurar até 9999:

```
> configure user maxfailedlogins admin 9999

>
```

Etapa 5: Verifique a configuração usando o 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
```

Tip: Verifique se você tem outro usuário com privilégios config disponíveis, caso o usuário administrador seja bloqueado!

Desbloquear um usuário administrador bloqueado

Supondo que você defina maxfailedlogins 3, depois de 3 tentativas com falha a conta de administrador é bloqueada:

```
> 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
```

Nesse caso, você terá que fazer login com outro usuário e desbloquear o usuário 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 Gerenciado pelo Gerenciador de Dispositivos (FDM)

No momento, o FDM não oferece suporte aos modos de conformidade CC ou UCAPL.

Aprimoramento relacionado: CSCws76567 ENH: adicionar suporte a CC/UCAPL no Gerenciador de dispositivos do Firepower

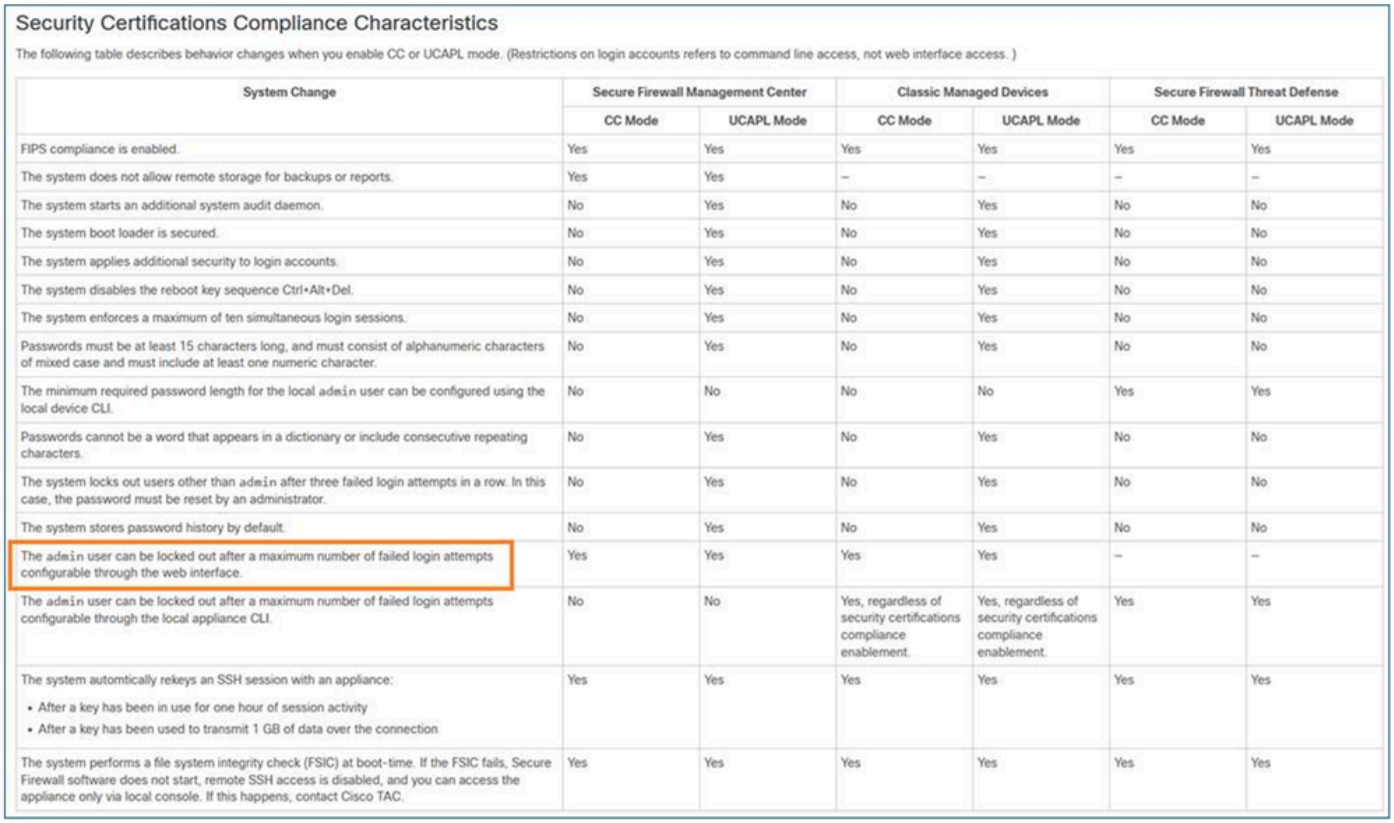
Se essa funcionalidade for crítica, é aconselhável discutir a priorização da solicitação de melhoria relacionada, conhecida como CSCws76567, com seu gerente de contas.

Defina o número máximo de tentativas de login com falha para acesso à GUI da Web

Semelhante ao login CLI, esta funcionalidade está disponível somente quando o modo de conformidade CC ou UCAPL está habilitado:

Defina o número máximo de tentativas de login com falha para acesso à GUI da Web

Semelhante ao login CLI, esta funcionalidade está disponível somente quando o modo de conformidade CC ou 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

Referência

- Características de conformidade das certificações de segurança

Como os modos CC ou UCAPL não podem ser usados em dispositivos gerenciados pelo FDM, você não pode definir o número máximo de tentativas de login com falha para o acesso à GUI da Web (consulte o aprimoramento CSCws76567).

Causa

- Para dispositivos gerenciados por FMC, a opção só está disponível quando o modo de conformidade CC ou UCAPL está habilitado.
- Para dispositivos gerenciados pelo FDM, uma solicitação de aprimoramento (CSCws76567) foi preenchida para resolver essa lacuna de recursos e adicionar suporte para Critérios Comuns (CC) e conformidade com UCAPL no Gerenciador de Dispositivos de Firewall.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco
- ID de bug Cisco CSCws76567

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.