配置FTD上本地管理员的最大失败登录尝试

问题

- 目标是为思科安全防火墙威胁防御(FTD)上的本地管理员帐户配置最大登录尝试失败次数。
- 该请求包含有关通过图形用户界面(GUI)和命令行界面(CLI)设置此限制的指导。
- 确保管理帐户受到保护，防止暴力登录尝试。

环境

- 产品：Cisco Secure Firewall
- 软件版本：任意
- 设置失败登录尝试限制所需的配置帮助

分辨率

有两种不同的情况，具体取决于如何管理安全防火墙。

默认行为

默认情况下，您无法为安全防火墙上的本地管理员帐户配置maxfailedlogins:

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

由FMC管理的防火墙

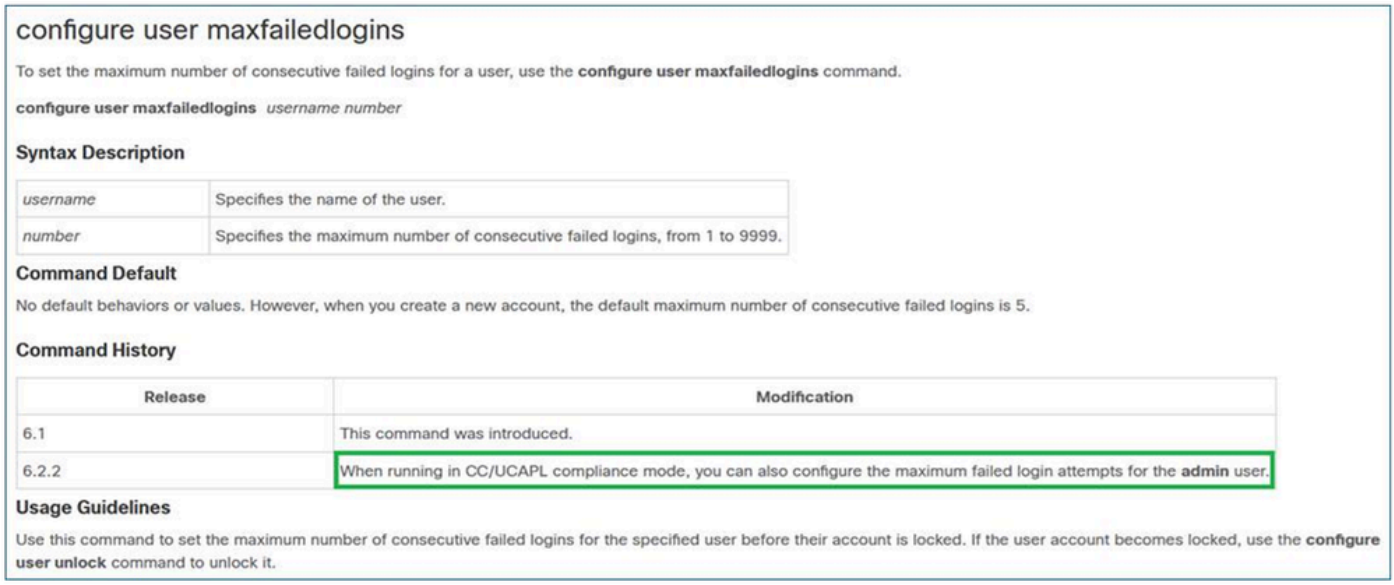
默认情况下，您无法为Cisco FMC管理的本地管理员帐户配置maxfailedlogins:

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

解决方案

要克服此限制，必须在防火墙上启用合规性模式。Cisco FTD命令参考中对此进行了说明：

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

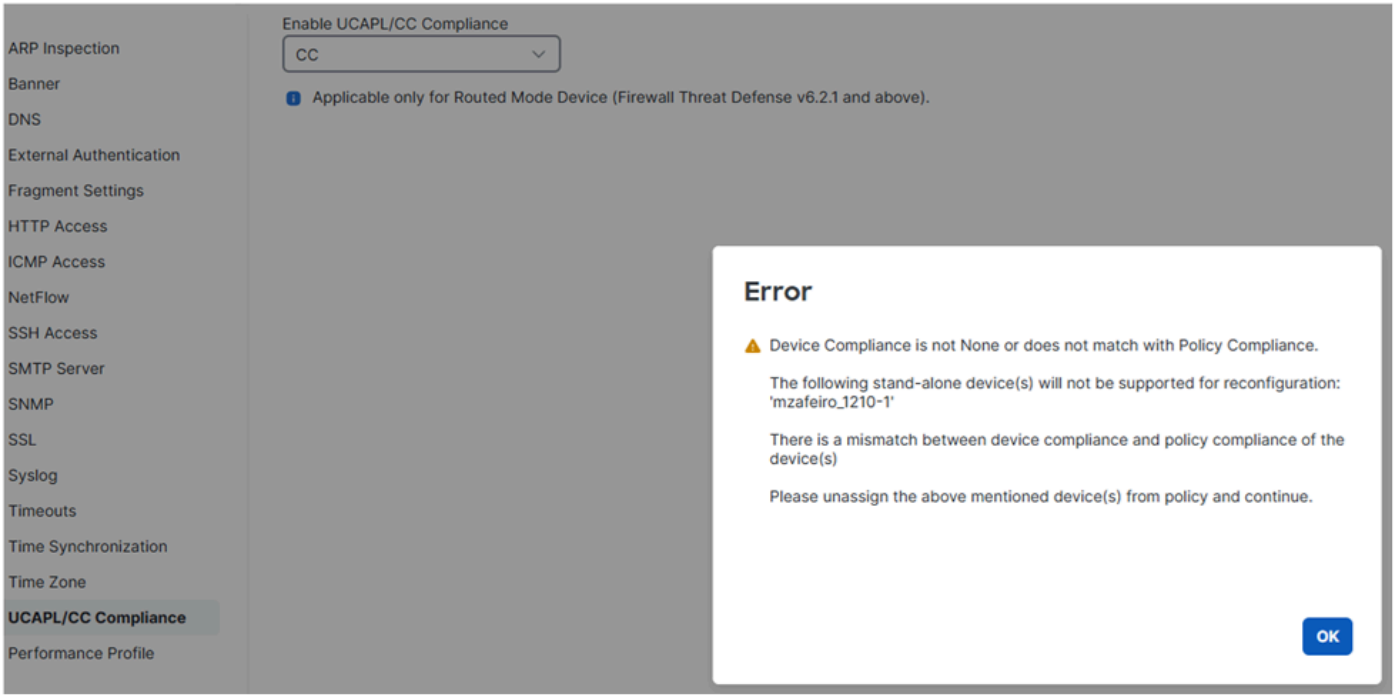
CC和UCAPL合规性

它们是安全合规性标准，指定了加强安全产品的要求。

对于maxfailedlogins，相关信息位于Security Certifications Compliance。

重要说明

首先，请记住，在FTD上启用CC或UCAPL合规性后，将无法还原更改。如果尝试还原，将获得：



inline_image_0.png

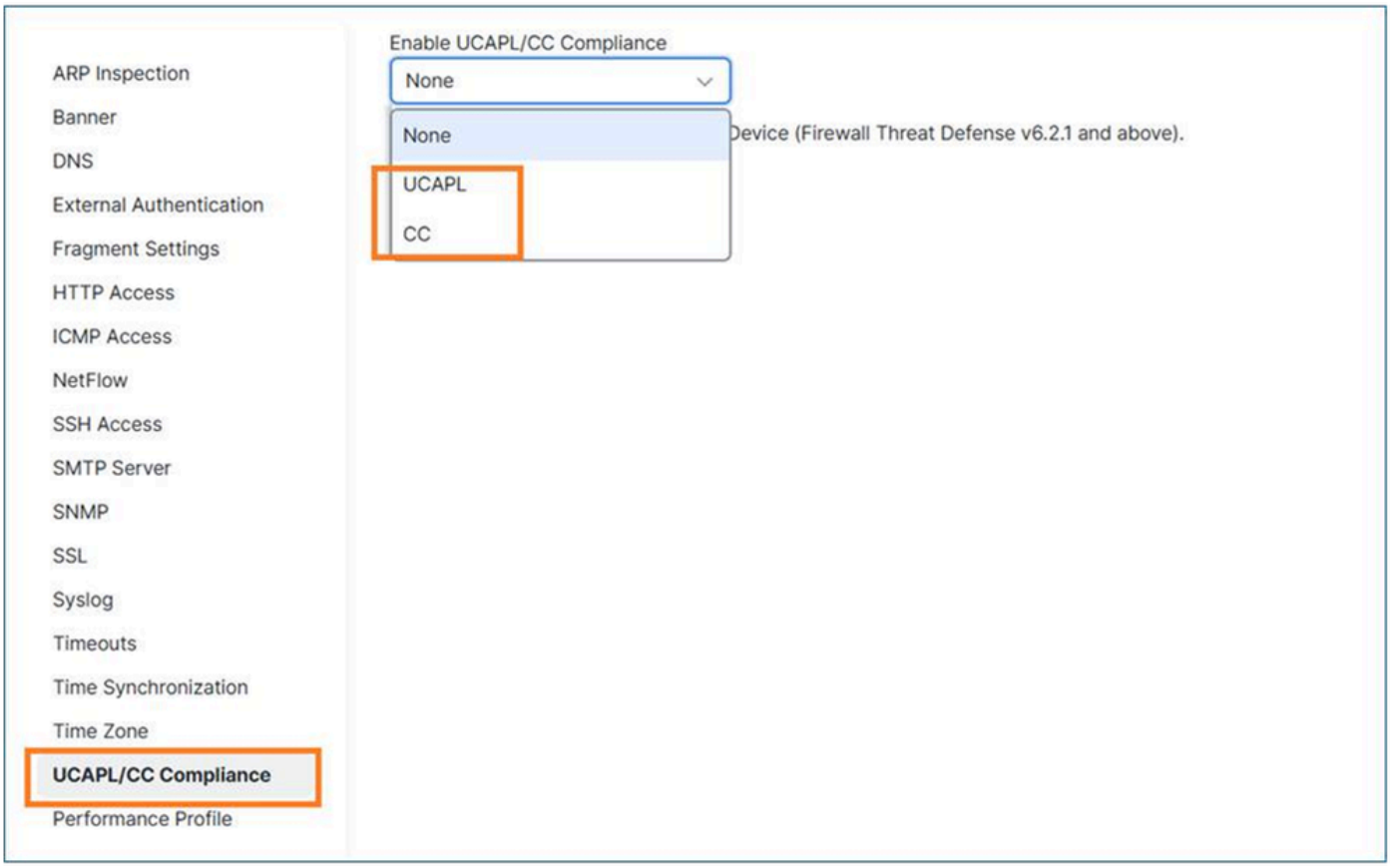
启用合规性模式并部署策略后，FTD将重新启动。

对于maxfailedlogins，使用CC最多可以配置999次失败尝试，而使用UCAPL最多可以配置3次。

在FTD上启用CC或UCAPL合规性

第1步：在FMC上，导航到设备/平台设置。

第2步：启用两种合规性模式（UCAP或CC）之一。由于无法撤消更改，因此强烈建议仔细阅读安全认证合规性指南。



inline_image_0.png

第3步：完成此操作后，您必须将平台设置策略分配给FTD（如果尚未）和部署。

部署完成后，FTD设备自动重新启动：

```
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 ...
```

第4步：防火墙再次启动后，您可以配置maxfailedlogins设置。如果您选择UCAPL，最多可以配置3次失败的登录尝试：

```
> configure user maxfailedlogins admin 5
```

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

>
```

如果为CC，您可以设置到9999:

```
> configure user maxfailedlogins admin 9999

>
```

第5步：使用show user命令验证配置：

```
> 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
```

提示：确保您有另一个具有config权限的用户，以防管理员用户被锁定！

解锁锁定的管理员用户

假设您设置maxfailedlogins 3，在3次失败尝试后，管理员帐户被锁定：

```
> 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
```

在这种情况下，您必须使用其他用户登录并手动解锁管理员用户：

```
> 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
```

由设备管理器(FDM)管理的防火墙

FDM当前不支持CC或UCAPL合规性模式。

相关增强:CSCws76567增强版：在Firepower设备管理器上添加CC/UCAPL支持

如果此功能非常关键，建议与您的客户经理讨论相关增强请求(称为CSCws76567)的优先级。

设置Web GUI访问的最大失败登录尝试次数

与CLI登录类似，此功能仅在启用CC或UCAPL合规性模式时可用：

设置Web GUI访问的最大失败登录尝试次数

与CLI登录类似，此功能仅在启用CC或UCAPL合规性模式时可用：

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

参考

- 安全认证合规性特征

由于CC或UCAPL模式不能在FDM管理的设备上使用，因此无法设置网络GUI访问的最大登录尝试失败次数(请参阅增强功能CSCws76567)。

原因

- 对于FMC管理的设备，此选项仅在启用CC或UCAPL合规性模式时可用。
- 对于FDM管理的设备，已提交增强请求(CSCws76567)，以解决此功能差距并在防火墙设备管理器中添加对通用标准(CC)和UCAPL合规性的支持。

相关内容

- 思科技术支持和下载
- 思科漏洞ID CSCws76567

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。