用户管理

用户帐户

用户账户用于访问系统。您最多可配置48个本地用户帐户。每个用户帐户必须具有唯一的用户名和密码。

管理员账户

管理员帐户是默认用户帐户，并且无法修改或删除。此帐户是系统管理员或超级用户帐户并具有完整权限。管理员账户没有已分配的默认密码；您必须在初始系统设置中选择密码。

管理员帐户始终处于活动状态，并且不会到期。无法将管理员帐户配置为非活动状态。

本地身份验证的用户账户

本地身份验证用户账户直接通过机箱进行身份验证，并且可以由具有管理员或AAA权限的任何用户来启用或禁用。一旦本地用户账户被禁用，该用户将无法登录。已禁用本地用户账户的详细配置信息不会被数据库删除。如果重新启用已禁用的本地用户帐户，此帐户将再次以现有配置变为活动状态。

远程身份验证的用户账户

远程身份验证的用户账户是指任何通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的用户账户。默认情况下，所有远程用户最初都分配了**只读**角色。

如果用户同时持有本地用户账户和远程用户账户，则在本地用户账户中定义的角色将覆盖在远程用户账户中持有的角色。

备用身份验证方法是使用本地数据库。该备用方法是不可配置的。

有关远程身份验证指导原则以及如何配置和删除远程身份验证提供程序的详细信息，请参阅以下主题：

- 远程身份验证指导原则，第 4 页
- 配置 LDAP 提供程序
- 配置 RADIUS 提供程序
- 配置 TACACS+ 提供程序

用户账户的到期

您可以配置用户账户在预定时间过期。当到达到期时间时，系统将会禁用用户账户。

默认情况下，用户账户不会到期。

在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。

面向用户名的指导原则

用户名还用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。将登录 ID 分配到用户账户时，请考虑以下指导原则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：
  - 任何字母字符

- 任何数字
- _（下划线）
- -（连字符）
- .（圆点）

- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头，而不能以数字或特殊字符开头，例如下划线。
- 登录 ID 区分大小写。
- 无法创建全数字登录 ID。
- 创建用户帐户后，无法更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

密码的指导原则

密码对于每个本地认证的用户账户都是必需的。具有管理员或AAA权限的用户可以配置系统，以对用户密码执行密码强度检查。如果密码强度检查已启用，则每个用户必须使用强密码。

建议每个用户都使用强密码。如果对本地身份验证的用户启用密码强度检查，则 FXOS将拒绝不符合以下要求的任何密码：

- 必须包含最少 8 个字符，最多 127 个字符。

注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。有关详细信息，请参阅配置最小密码长度检查，第 15 页。

- 必须包含至少一个大写字母字符。
- 必须包含至少一个小写字母字符。
- 必须包含至少一个非字母数字（特殊）字符。
- 不得包含空格。
- 不能包含连续重复 3 次的字符，例如 aaabbb。
- 不得包含三个以任何顺序排列的连续数字或字母，例如 passwordABC 或 password321。
- 不能与用户名相同，或与用户名正好相反。
- 必须通过密码字典检查。例如，密码不可以是标准的词典单词。
- 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。

注释 无论密码强度检查是否启用，此限制均适用。

- 本地用户和管理员账户的密码不得为空。

远程身份验证指导原则

如果为支持的远程身份验证服务之一配置系统，则必须创建用于为该服务的创建提供程序，以确保 Firepower 4100/9300 机箱 能够与系统进行通信。下列指导原则影响用户授权：

远程身份验证服务中的用户账户

用户账户可能存在于 Firepower 4100/9300 机箱本地或远程身份验证服务器中。

您可以查看通过 Firepower 机箱管理器或 FXOS CLI 中的远程身份验证服务登录的用户的临时会话。

远程身份验证服务中的用户角色

如果在远程身份验证服务器中创建用户账户，则必须确保账户包括用户在 Firepower 4100/9300 机箱中工作所需的角色，并且这些角色的名称与 FXOS 中使用的名称相匹配。基于角色策略，可能不允许用户进行登录，也可能仅授予用户只读权限。

远程身份验证提供程序中的用户属性

对于 RADIUS 和 TACAS+ 配置，您必须在用户用于登录 Firepower 机箱管理器或 FXOS CLI 的每个远程身份验证提供程序中为 Firepower 4100/9300 机箱配置一个用户属性。此用户属性存储分配给各用户的角色和区域设置信息。

用户登录后，FXOS 执行以下操作：

1. 查询远程身份验证服务。
2. 验证用户。
3. 如果对用户进行了验证，则检查分配给该用户的角色和区域设置。

下表包含 FXOS 支持的远程身份验证提供程序的用户属性要求比较：

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
LDAP	可选	您可以选择执行以下操作之一： • 请不要扩展 LDAP 方案，配置符合要求的现有的未使用属性。 • 扩展 LDAP 方案，使用唯一名称（例如，CiscoAVPair）创建自定义属性。	思科 LDAP 实施需要 unicode 类型属性。 如果选择创建 CiscoAVPair 自定义属性，请使用以下属性 ID：1.3.6.1.4.1.9.287247.1 以下部分提供示例 OID。
RADIUS	可选	您可以选择执行以下操作之一： • 请不要扩展 RADIUS 方案，并使用符合要求的现有的未使用属性。 • 扩展 RADIUS 方案，使用唯一名称（例如，cisco-avpair）创建自定义属性。	思科 RADIUS 实施的供应商 ID 为 009，属性的供应商 ID 为 001。 以下语法示例显示，如果选择创建 cisco-avpair 属性，如何指定多个用户角色和区域：`shell:roles="admin,aaa" shell:locales="L1,abc"`。使用逗号“,”作为分隔多个值的分隔符。
TACACS+	必要	必须扩展方案，并使用名称 cisco-av-pair 创建自定义属性。	cisco-av-pair 名称是为 TACACS+ 提供程序提供属性 ID 的字符串。 以下语法示例显示如何在创建 cisco-av-pair 属性时指定多个用户角色和区域：`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。在 cisco-av-pair 属性语法中使用星号 (*) 将区域标记为可选项，以避免使用相同身份验证配置文件的其他思科设备的身份验证失败。使用空格作为分隔符来分隔多个值。

LDAP 用户属性的示例 OID

以下是自定义 CiscoAVPair 属性的示例 OID：

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
```

```
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

用户角色

系统包含以下用户角色：

管理员

完成对整个系统的读写访问。默认情况，下会向默认管理员账户分配此角色，并且不能对其进行更改。

只读

对系统配置进行只读访问，但无权修改系统状态。

运营

对NTP配置、用于智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。

AAA 管理员

对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。

本地身份验证用户的密码配置文件

密码配置文件包含所有本地身份验证用户的密码历史记录和密码更改时间间隔属性。不能为每个本地身份验证的用户指定其他密码配置文件。

密码历史记录计数

借助密码历史记录计数，您可以阻止本地身份验证的用户反复使用同一密码。配置此属性后，Firepower机箱最多可以存储本地身份验证的用户先前使用的 15 个密码。密码存储的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。

用户必须创建和使用在密码历史记录计数中配置的密码数量，然后才能重新使用密码。例如，如果您将密码历史记录计数设置为 8，本地身份验证用户无法重新使用第一个密码，直至第九个密码过期为止。

默认情况下，密码历史记录设置为0。该值禁用历史记录计数，允许用户随时重新使用以前的密码。

如有必要，可以清除本地身份验证的用户的密码历史记录计数并支持重复使用先前的密码。

密码更改间隔

通过密码更改间隔，可以限制本地身份验证的用户在特定小时数内能够进行的密码更改次数。下表介绍密码更改间隔的两个配置选项。

间隔配置	说明	示例
不允许密码更改 (No password change allowed)	此选项不允许在密码更改后的指定小时数内更改本地身份验证的用户的密码。 可以指定介于 1 和 745 小时之间的无更改间隔。默认情况下，无更改间隔为 24 小时。	例如，要在本地身份验证用户更改其密码后 48 小时内阻止更改密码，请进行以下设置： • 将在间隔期间更改设置为禁用 • 将无更改间隔设置为 48
更改间隔内允许密码更改 (Password changes allowed within change interval)	此选项指定本地身份验证的用户的密码在预定义间隔内可以更改的最大次数。 可以指定介于 1 和 745 小时之间的更改间隔，以及介于 0 和 10 之间的最大密码更改次数。默认情况下，允许本地身份验证的用户在 48 小时间隔内最多更改 2 次密码。	例如，要在本地身份验证用户更改其密码后 24 小时内最多允许一次密码更改，请进行以下设置： • 将在间隔期间更改设置为启用 • 将更改计数设置为 1 • 将更改间隔设置为 24

选择默认身份验证服务

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入默认授权安全模式：

Firepower-chassis /security # **scope default-auth**

步骤 3 指定默认身份验证：

Firepower-chassis /security/default-auth # **set realm** *auth-type*

其中 *auth-type* 为以下关键字之一：

- **ldap**- 指定 LDAP 身份验证
- **local**- 指定本地身份验证
- **none**- 允许本地用户登录，无需指定密码
- **radius**- 指定 RADIUS 身份验证

- **tacacs**- 指定 TACACS+ 身份验证

注释　如果默认身份验证和控制台身份验证都设置为使用相同的远程身份验证协议（RADIUS、TACACS+ 或 LDAP），不更新这些用户设置就无法更改该服务器配置的某些方面（例如，删除该服务器或更改其分配顺序）。

步骤 4 （可选） 指定相关联的提供程序组，如果有：

Firepower-chassis /security/default-auth # **set auth-server-group** *auth-serv-group-name*

步骤 5 （可选） 为本域中的用户指定刷新请求的最大时间间隔：

Firepower-chassis /security/default-auth # **set refresh-period** *seconds*

指定一个介于 0 和 600 之间的整数。默认值为 600 秒。

如果超过此时间限制，则 FXOS 会认为 Web 会话处于非活动状态，但不终止此会话。

步骤 6 （可选） 指定自上次刷新请求后至 FXOS 认为 Web 会话已结束前的最长时间间隔：

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

指定一个介于 0 和 600 之间的整数。默认值为 600 秒。

注释　如果为 RADIUS 或 TACACS+ 领域设置双因素身份验证，请考虑延长 **session-refresh** 和 **session-timeout** 期限，避免远程用户太过频繁地重新进行身份验证。

步骤 7 （可选） 将领域的身份验证方式设置为双因素身份验证：

Firepower-chassis /security/default-auth # **set use-2-factor yes**

注释　双因素身份验证仅适用于 RADIUS 和 TACACS+ 领域。

步骤 8 将任务提交到系统配置：

commit-buffer

示例

以下示例将默认身份验证设置为 RADIUS，将默认身份验证提供程序组设置为 provider 1，启用双因素身份验证，将刷新期限设置为 300 秒（5 分钟），将会话超时期限设置为 540 秒（9 分钟），并且启用双因素身份验证。然后，提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 300
Firepower-chassis /security/default-auth* # set session-timeout 540
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

配置会话超时

您可以使用 FXOS CLI 来指定 Firepower 4100/9300 机箱在关闭用户会话之前允许用户不活动的时间段。您可以为控制台会话以及 HTTPS、SSH 和 Telnet 会话配置不同的设置。

超时值最大可设置为 3600 秒（60 分钟）。默认值为 600 秒。要禁用此设置，请将会话超时值设置为 0。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入默认授权安全模式：

Firepower-chassis /security # **scope default-auth**

步骤 3 设置 HTTPS、SSH 和 Telnet 会话的空闲超时：

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

步骤 4 （可选）设置控制台会话的空闲超时：

Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*

步骤 5 将任务提交到系统配置：

Firepower-chassis /security/default-auth # **commit-buffer**

步骤 6 （可选）查看会话和绝对会话超时设置：

Firepower-chassis /security/default-auth # **show detail**

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

配置绝对会话超时

Firepower 4100/9300 机箱具有绝对会话超时设置，即系统会在绝对会话超时期限已过后关闭用户会话，而不考虑会话是否在使用。此绝对超时功能具全局性，适用于所有形式的访问（包括串行控制台、SSH 和 HTTPS）。

您可以为串行控制台会话单独配置绝对会话超时。这允许针对调试需求禁用串行控制台绝对会话超时，同时保持其他访问形式的超时。

绝对超时值默认为 3600 秒（60 分钟），可使用 FXOS CLI 进行更改。要禁用此设置，请将绝对会话超时值设为 0。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入默认授权安全模式：

Firepower-chassis /security # **scope default-auth**

步骤 3 设置绝对会话超时：

Firepower-chassis /security/default-auth # **set absolute-session-timeout** *seconds*

步骤 4 （可选）设置单独的控制台绝对会话超时：

Firepower-chassis /security/default-auth # **set con-absolute-session-timeout** *seconds*

步骤 5 将任务提交到系统配置：

Firepower-chassis /security/default-auth # **commit-buffer**

步骤 6 （可选）查看会话和绝对会话超时设置：

Firepower-chassis /security/default-auth # **show detail**

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

为远程用户配置角色策略

默认情况下，向使用 LDAP、RADIUS 或 TACACS 协议从远程服务器登录 Firepower 机箱管理器或 FXOS CLI 的所有用户授予只读权限。出于安全原因，有必要限制匹配已建立的用户角色的那些用户的访问权限。

您可以通过以下方式为远程用户配置角色策略：

assign-default-role

当用户尝试登录并且远程身份验证提供程序不能为用户角色提供身份验证信息时，允许用户使用只读用户角色登录。

此为默认行为。

no-login

当用户尝试登录并且远程身份验证提供程序不为用户角色提供身份验证信息时，拒绝访问。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 指定是否应根据用户角色限制对 Firepower 机箱管理器 和 FXOS CLI 的用户访问：

Firepower-chassis /security # **set remote-user default-role** {**assign-default-role** | **no-login**}

步骤 3 将任务提交到系统配置：

Firepower-chassis /security # **commit-buffer**

示例

以下示例为远程用户设置角色策略，提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # set remote-user default-role no-login
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

为本地身份验证的用户启用密码强度检查

如果启用密码强度检查，则 FXOS不允许用户选择不符合强密码准则的密码（请参阅密码的指导原则，第 3 页）。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 指定密码强度检查已启用还是已禁用：

Firepower-chassis /security # **set enforce-strong-password** {**yes** | **no**}

示例

以下示例启用密码强度检查：

```
Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

设置最大尝试登录次数

您可配置在将用户您可配置允许用户尝试登录的最大失败次数，如果超过该次数，用户会被Firepower 4100/9300机箱锁定一段指定的时间长度之前允许用户尝试登录的最大失败次数。锁定一段指定的时间长度。如果用户超过设置的最大尝试登录次数，用户会被系统锁定。系统不会显示表明用户被锁定的通知。在这种情况下，用户必须等待一段指定的时间长度，然后才能尝试登录。

执行以下步骤，以配置最大登录尝试次数。

注释

- 在超过最大尝试登录次数后，所有类型的用户账户（包括管理员账户）均被锁定。
- 默认的最大尝试登录失败次数为 0。在超过最大尝试登录次数后，用户被系统锁定的默认时间长度为 30 分钟（1800 秒）。
- 有关查看用户锁定状态和清除用户锁定状态的步骤，请参阅查看和清除用户锁定状态，第 13 页。

这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 设置最大尝试登录失败次数。

set max-login-attempts *num_attempts*

num_attempts 值可以是 0 到 10 之间的任何整数。

步骤 3 指定在达到最大尝试登录次数后用户应被系统锁定的时间长度（以秒为单位）：

set user-account-unlock-time

unlock_time

步骤 4 提交配置：

commit-buffer

查看和清除用户锁定状态

对于超过 Maximum Number of Login Attempts CLI 设置中指定的最大失败登录尝试次数之后被 Firepower 4100/9300 机箱锁定的用户，管理员用户可查看和清除其锁定状态。有关详细信息，请参阅设置最大尝试登录次数，第 12 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 显示相关用户的用户信息（包括锁定状态）：

Firepower-chassis /security # **show local-user** *user* **detail**

示例：

```
Local User user:
 First Name:
 Last Name:
 Email:
 Phone:
 Expiration: Never
 Password:
 User lock status: Locked
 Account status: Active
 User Roles:
 Name: read-only
 User SSH public key:
```

步骤 3 （可选）清除用户锁定状态：

Firepower-chassis /security # **scope local-user** *user*

Firepower-chassis /security/local-user # **clear lock-status**

配置更改间隔的最大密码更改次数

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 限制本地身份验证用户在给定小时数内更改密码的次数。

Firepower-chassis /security/password-profile # **set change-during-interval enable**

步骤 4 指定本地身份验证用户在更改间隔内可以更改其密码的最大次数：

Firepower-chassis /security/password-profile # **set change-count** *pass-change-num*

该值可以是介于 0 和 10 之间的任意值。

步骤 5 指定最大小时数，在该时间段内，密码更改次数为**更改计数 (Change Count)** 字段中所指定的值。

Firepower-chassis /security/password-profile # **set change-interval** *num-of-hours*

该值可以是 1 至 745（小时）的任意值。

例如，如果该字段设置为 48，**更改计数 (Change Count)** 字段设置为 2，那么本地身份验证用户在 48 小时内执行的密码更改不能超过 2 次。

步骤 6 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例启用“间隔期间更改 (change during interval)”选项，将更改计数设置为 5，将更改间隔设置为 72 小时，并且提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Firepower-chassis /security/password-profile* # set change-count 5
Firepower-chassis /security/password-profile* # set change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

配置最小密码长度检查

如果启用最小密码长度检查，则必须使用指定的最小数目的字符创建密码。例如，如果将 *min_length* 选项设为 15，则用户必须使用 15 个或更多字符创建密码。此选项是在系统上用于实施通用标准认证合规性的众多选项之一。有关详细信息，请参阅安全认证合规性。

执行以下步骤，以配置最小密码长度检查。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 指定最小密码长度：

set min-password-length *min_length*

步骤 3 提交配置：

commit-buffer

为密码配置无更改间隔

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 禁用在间隔内更改功能：

Firepower-chassis /security/password-profile # **set change-during-interval disable**

步骤 4 指定本地身份验证用户在更改新建密码之前必须等待的最少小时数：

Firepower-chassis /security/password-profile # **set no-change-interval** *min-num-hours*

该值可以是 1 至 745（小时）的任意值。

如果未将**间隔期间更改 (Change During Interval)** 属性设置为**禁用 (Disable)**，该时间间隔将被忽略。

步骤 5 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例禁用“间隔期间更改 (change during interval)”选项，将无更改间隔设置为 72 小时，提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

配置密码历史记录计数

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 指定本地身份验证用户必须创建的唯一密码数量，在此之前，用户可以重新使用以前用过的密码：

Firepower-chassis /security/password-profile # **set history-count** *num-of-passwords*

该值可以是从 0 至 15 的任意值。

默认情况下，**历史计数 (History Count)** 字段设置为 0，这表示禁用历史计数，使用户随时都能够重复使用之前已使用的密码。

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例配置密码历史记录计数并且提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set history-count 5
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

创建本地用户账户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 创建用户账户：

Firepower-chassis /security # **create local-user** *local-user-name*

其中，*local-user-name* 是登录此账户时要使用的账户名称。此名称必须唯一，并满足用户帐户名称的准则和限制（请参阅面向用户名的指导原则，第 2 页）。

创建用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

步骤 3 指定本地用户账户已启用还是已禁用：

Firepower-chassis /security/local-user # **set account-status** {**active**| **inactive**}

步骤 4 设置用户账户的密码：

Firepower-chassis /security/local-user # **set password**

输入密码：*password*

确认密码：*password*

如果启用了密码强度检查，则用户的密码必须为强密码，FXOS会拒绝任何不满足强度检查要求的密码（请参阅密码的指导原则，第 3 页）。

注释 密码不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。无论密码强度检查是否启用，此限制均适用。

步骤 5 （可选） 指定用户的名字：

Firepower-chassis /security/local-user # **set firstname** *first-name*

步骤 6 （可选） 指定用户的姓氏：

Firepower-chassis /security/local-user # **set lastname** *last-name*

步骤 7 （可选） 指定用户账户到期日期： *month* 参数是月份名称的前三个字母。

Firepower-chassis /security/local-user # **set expiration** *month day-of-month year*

注释 在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。

步骤 8 （可选） 指定用户邮件地址。

Firepower-chassis /security/local-user # **set email** *email-addr*

步骤 9 （可选） 指定用户电话号码。

Firepower-chassis /security/local-user # **set phone** *phone-num*

步骤 10 （可选） 指定用于无密码访问的 SSH 密钥。

Firepower-chassis /security/local-user # **set sshkey** *ssh-key*

步骤 11 所有用户均默认分配了 *read-only* 角色，并且此角色无法删除。对于要指定给用户的每个额外角色：

Firepower-chassis /security/local-user # **create role** *role-name*

其中，*role-name* 是代表要分配给用户账户的权限的角色（请参阅用户角色，第 6 页）。

注释 用户角色和权限的更改在用户下一次登录之后才会生效。如果在向用户账户分配新角色或从中删除现有角色时用户已登录，则活动会话将继续使用上一个角色和权限。

步骤 12 从用户删除分配的角色：

Firepower-chassis /security/local-user # **delete role** *role-name*

所有用户均默认分配了 *read-only* 角色，并且此角色无法删除。

注释 删除用户角色时，系统会撤销该用户的当前会话 ID，这意味着用户的所有活动会话（包括 CLI 和 Web）都将立即终止。

步骤 13 提交任务。

Firepower-chassis security/local-user # **commit-buffer**

示例

以下示例创建名为 kikipopo 的用户账户，启用用户账户，将密码设置为 foo12345，分配管理员用户角色，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # create role admin
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

以下示例创建名为 lincey 的用户账户，启用用户账户，设置 OpenSSH 密钥以进行无密码访问，分配 aaa 和运营用户角色，并且提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
```

```
Firepower-chassis /security/local-user* # create role aaa
Firepower-chassis /security/local-user* # create role operations
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

以下示例创建名为 jforlenz 的用户账户，启用用户账户，设置 Secure SSH 密钥以进行无密码访问，并且提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

删除本地用户账户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 删除本地用户账户：

Firepower-chassis /security # **delete local-user** *local-user-name*

步骤 3 将任务提交到系统配置：

Firepower-chassis /security # **commit-buffer**

示例

以下示例删除 foo 用户账户，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

激活或停用本地用户账户

您必须是拥有管理员或 AAA 权限的用户，才能激活或停用本地用户账户。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 针对您要激活或停用的用户，进入本地用户安全模式：

Firepower-chassis /security # **scope local-user** *local-user-name*

步骤 3 指定本地用户账户是活动还是非活动状态：

Firepower-chassis /security/local-user # **set account-status** {**active** | **inactive**}

注释 管理员用户账户始终设置为活动。不能修改。

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/local-user # **commit-buffer**

示例

以下示例启用一个名为 accounting 的本地用户帐户：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope local-user accounting
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

清除本地身份验证的用户的密码历史记录

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入已指定用户账户的本地用户安全模式：

Firepower-chassis /security # **scope local-user** *user-name*

步骤 3 清除已指定用户账户的密码历史记录：

Firepower-chassis /security/local-user # **clear password-history**

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/local-user # **commit-buffer**

示例

以下示例将清除密码历史记录并提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```