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；但帐户密码必须重置。

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Firepower eXtensible Operating System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 13 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。

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
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

配置用户设置

过程

步骤 1 选择**系统 (System)** > **用户管理 (User Management)**。

步骤 2 单击**设置** (Settings) 选项卡。

步骤 3 使用必填信息填写下列字段：

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）。

名称	说明
默认身份验证 (Default Authentication) 字段	在远程登录期间，对用户进行身份验证的默认方式。这可以是以下其中一项： • **本地 (Local)** - 必须在 Firepower 机箱本地定义用户帐户。 • **Radius** - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户账户。 • **TACACS** - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户账户。 • **LDAP** - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户账户。 • **无 (None)** - 如果用户账户是 Firepower 机箱的本地账户，当用户在远程登录时，不需要密码。 **注释** 所有 **Radius**、 **TACACS** 和 **LDAP** 设置必须在平台设置下进行配置。有关详细信息，请参阅“平台设置”一章中的关于 AAA。
控制台身份验证 (Console Authentication) 字段	通过控制台端口连接到 FXOS CLI 时用于用户身份验证的方法。这可以是以下其中一项： • **本地 (Local)** - 必须在 Firepower 机箱本地定义用户帐户。 • **Radius** - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户账户。 • **TACACS** - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户账户。 • **LDAP** - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户账户。 • **无 (None)** - 如果用户账户是 Firepower 机箱的本地账户，则在用户使用控制台端口连接至 FXOS CLI 时无需密码。
远程用户设置	
远程用户角色策略	控制当用户尝试登录并且远程身份验证提供程序不向用户角色提供身份验证信息时发生的事情： • **分配默认角色 (Assign Default Role)** - 允许用户使用只读用户角色登录。 • **无登录 (No-Login)** - 不允许用户登录系统，即使用户名和密码正确也是如此。

名称	说明
本地用户设置	
密码强度检查 (Password Strength Check) 复选框	如果选中，所有本地用户密码都必须符合强密码准则（请参阅密码的指导原则，第 3 页）。默认情况下，系统会启用强密码。
历史记录计数 (History Count) 字段	用户在重新使用先前使用的密码之前必须创建的唯一密码的数量。历史记录计数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。 该值可以是介于 0 和 15 之间的任意值。 您可以将**历史记录计数 (History Count)** 字段设置为 0，这表示禁用历史记录计数，使用户随时都能够重复使用之前已使用的密码。
间隔期间更改 (Change During Interval) 字段	控制本地验证用户何时能够更改其密码。该字段可以是： • **启用 (Enable)** - 本地身份验证用户可以根据“更改间隔 (Change Interval)”和“更改计数 (Change Count)”设置更改其密码。 • **禁用 (Disable)** - 本地身份验证用户不能在为“无更改间隔 (No Change Interval)”指定的期限内更改其密码。
更改间隔 (Change Interval) 字段	在其期间执行在**更改计数 (Change Count)** 字段中指定的密码更改次数的小时数。 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。
更改计数 (Change Count) 字段	本地身份验证用户能够在“更改间隔 (Change Interval)”内更改其密码的最大次数。 该值可以是介于 0 和 10 之间的任意值。
无更改间隔 (No Change Interval) 字段	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。 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。
密码到期天数 (Passphrase Expiration Days) 字段	将到期时间设置为 1 到 9999 天。默认情况下，禁用过期。
密码到期警告期 (Passphrase Expiration Warning Period) 字段	设置到期前的天数，在用户每次登录时提醒密码到期，范围介于 0 到 9999 之间。默认时间为 14 天。

名称	说明
到期宽限期 (Expiration Grace Period) 字段	设置用户在到期后可以更改密码的天数，范围介于 0 到 9999 之间。默认值为 3 天。
密码重用间隔 (Password Reuse Interval) 字段	设置可重复使用密码的天数，范围介于 1 到 365 之间。默认值为 15 天。如果同时启用**历史记录计数**和**密码重复使用间隔**，则必须满足两个要求。例如，如果您将历史计数设置为 3，并将重复使用间隔设置为 10 天，则您只能在更改 3 次密码的 10 天后更改密码。

步骤 4 单击**保存 (Save)**。

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）。

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 将任务提交到系统配置：

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

步骤 5 （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
```

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）。

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

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

创建本地用户账户

过程

步骤 1 依次选择 **系统 (System)** > **用户管理 (User Management)**。

步骤 2 单击**本地用户 (Local Users)** 选项卡。

步骤 3 单击**添加用户 (Add User)**，可打开**添加用户 (Add User)** 对话框。

步骤 4 使用关于用户的必填信息，填写下列字段：

名称	说明
用户名 (User Name) 字段	登录此账户时使用的账户名称。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）。 保存用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。
名字 (First Name) 字段	用户的名字。该字段最多包含 32 个字符。
姓氏 (Last Name) 字段	用户的姓氏。该字段最多包含 32 个字符。

名称	说明
邮件 (Email) 字段	用户的邮件地址。
电话号码 (Phone Number) 字段	用户的电话号码。
密码 (Password) 字段	与此账户关联的密码。如果启用了密码强度检查，则用户的密码必须为强密码，Firepower eXtensible Operating System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。
确认密码 (Confirm Password) 字段	第二次用于确认目的的密码。
账户状态 (Account Status) 字段	如果状态设置为**活动 (Active)**，用户可以登录使用此登录 ID 和密码登录 Firepower 机箱管理器和 FXOS CLI。
用户角色 列表	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）。 所有用户均默认分配了“只读 (Read-Only)”角色，并且此角色无法取消选择。要分配多个角色，请按住**Ctrl**键并单击所需角色。 **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。
账户到期复选框	如果选中，在**到期日期 (Expiration Date)** 字段中指定的日期过后，此账户将到期且无法使用。 **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。
到期日期 (Expiry Date) 字段	账户到期日期。日期格式应为 yyyy-mm-dd。 单击此字段末尾的日历图标，查看您可以用来选择到期日期的日历。

步骤 5 单击 **Add**。

删除本地用户账户

过程

步骤 1 依次选择 **系统 (System)** > **用户管理 (User Management)**。

步骤 2 单击**本地用户 (Local Users)** 选项卡。

步骤 3 在与您想要删除的用户账户对应的行中，单击**删除 (Delete)**。

步骤 4 在**确认 (Confirm)** 对话框中，单击**是 (Yes)**。

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 依次选择 **系统 (System)** > **用户管理 (User Management)**。

步骤 2 单击**本地用户 (Local Users)** 选项卡。

步骤 3 在您要激活或停用的用户账户所在的行中，单击**编辑 (Edit)**（铅笔图标）。

步骤 4 在**编辑用户 (Edit User)** 对话框中，执行以下操作之一：

- 要激活用户账户，请单击**账户状态 (Account Status)** 字段中的**活动 (Active)** 单选按钮。请注意，当您重新激活用户帐户时，必须重置帐户密码。
- 要停用用户账户，请单击**账户状态 (Account Status)** 字段中的**非活动 (Inactive)** 单选按钮。

管理员用户账户始终设置为活动。不能修改。

步骤 5 单击**保存 (Save)**。

步骤 6 将任务提交到系统配置：

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

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 #
```