ユーザ管理

ユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。最大 48 のローカル ユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

管理者アカウント

管理者アカウントはデフォルト ユーザ アカウントであり、変更や削除はできません。このアカウントは、システム管理者またはスーパーユーザアカウントであり、すべての権限が与えられています。管理者アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザアカウントは、シャーシを通じて直接認証され、管理者権限または AAA 権限があれば誰でも有効化または無効化できます。ローカル ユーザ アカウントを無効にすると、ユーザはログインできません。データベースは無効化されたローカル ユーザ アカウントの設定の詳細を削除しません。無効なローカルユーザアカウントを再度有効にすると、アカウントは既存の設定で再びアクティブになりますが、アカウントのパスワードは再設定する必要があります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ を通じて認証されたユーザ アカウントのことです。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

リモート認証のガイドラインの詳細や、リモート認証プロバイダーの設定および削除方法については、次のトピックを参照してください。

- リモート認証のガイドライン （4 ページ）
- LDAP プロバイダーの設定
- RADIUS プロバイダーの設定
- TACACS+ プロバイダーの設定

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。有効期限の時間になると、ユーザ アカウントは無効になります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。

ユーザ名に関するガイドライン

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID としても使用されます。ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。

- 任意の英字
- 任意の数字
- _（アンダースコア）
- -（ダッシュ）
- .（ドット）

- ログイン ID は一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字から始めることはできません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワードに関するガイドライン

ローカル認証された各ユーザ アカウントにパスワードが必要です。admin または AAA 権限を持つユーザについては、ユーザ パスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証されたユーザのパスワード強度チェックを有効にすると、Firepower eXtensible Operating System は次の要件を満たしていないパスワードを拒否します。

- 少なくとも 8 文字を含み、最大 127 文字であること

（注） コモンクライテリア要件に準拠するために、オプションでシステムの最小文字数 15 文字の長さのパスワードを設定できます。詳細については、最小パスワード長チェックの設定 （16 ページ）を参照してください。

- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字（特殊文字）を少なくとも 1 文字含む。
- スペースを含まない。

- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。

（注） この制限は、パスワードの強度チェックが有効になっているかどうかにかかわらず適用されます。

- ローカル ユーザ アカウントおよび admin アカウントの場合は空白にしない。

リモート認証のガイドライン

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Firepower 4100/9300 シャーシがそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Firepower 4100/9300 シャーシ にローカルに存在するか、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションを、Firepower Chassis Manager または FXOS CLI から表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Firepower 4100/9300 シャーシで作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を FXOS で使用される名前と一致させることが必要です。ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

リモート認証プロバイダーのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Firepower Chassis Manager または FXOS CLI へのログインに使用する各リモート認証プロバイダーに Firepower 4100/9300 シャーシ 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

ユーザがログインすると、FXOS は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表は、FXOS でサポートしているリモート認証プロバイダーのユーザ属性要件を比較したものです。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	オプション	次のいずれかを実行するように選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 次の項で、サンプル OID を示します。
RADIUS	オプション	次のいずれかを実行するように選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用します。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成します。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
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
```

ユーザの役割

システムには、次のユーザ ロールが用意されています。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトのadminアカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

読み取り専用

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

操作

NTPの設定、Smart LicensingのためのSmart Call Homeの設定、システム ログ（syslogサーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

AAA アドミニストレータ

ユーザ、ロール、およびAAA設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

ローカル認証されたユーザのパスワード プロファイル

パスワードのプロファイルには、ローカル認証されたユーザすべてのパスワード履歴やパスワード変更間隔プロパティが含まれます。ローカル認証されたユーザのそれぞれに異なるパスワード プロファイルを指定することはできません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。このプロパティが設定されている場合、Firepowerシャーシは、ローカル認証されたユーザがこれまでに使用した最大15個のパスワードを保存します。パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になる前に、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用する必要があります。たとえば、パスワード履歴カウントを8に設定した場合、ローカル認証されたユーザは9番目のパスワードが期限切れになった後まで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は0に設定されます。この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザについてパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更回数を制限することができます。次の表で、パスワード変更間隔の2つの設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更禁止	このオプションを設定すると、ローカル認証されたユーザは、パスワードを変更してから指定された時間内はパスワードを変更できなくなります。 1 ～ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが48時間の間パスワードを変更できないようにする場合、次のように設定します。 • [間隔中の変更（Change During Interval）] を無効にする • [変更禁止間隔（No Change Interval）] を 48 に設定する
変更間隔内のパスワード変更許可	このオプションは、ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。デフォルトでは、ローカル認証されたユーザに対して、48時間間隔内で最大2回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に最大 1 回そのパスワードを変更できるようにするには、次のように設定します。 • [間隔中の変更（Change During Interval）] を有効にする • [変更カウント（Change Count）] を 1 に設定する • [変更間隔（Change Interval）] を 24 に設定する

ユーザ設定の設定

手順

ステップ 1 **[システム（System）]** > **[ユーザ管理（User Management）]** を選択します。

ステップ 2 [設定（Settings）] タブをクリックします。

ステップ 3 次のフィールドに必要な情報を入力します。

（注） デフォルトの認証とコンソール認証の両方が同じリモート認証プロトコル（RADIUS、TACACS+、または LDAP）を使用するように設定されている場合、そのサーバの設定の特定の側面を変更することは（たとえば、サーバの削除や、割り当ての順序の変更）、これらのユーザ設定を更新することなしではできません。

名前	説明
[Default Authentication] フィールド	リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。 • [Local]：ユーザ アカウントは、Firepower シャーシでローカルに定義する必要があります。 • [Radius]：ユーザ アカウントは、Firepower シャーシに指定された RADIUS サーバで定義する必要があります。 • [TACACS]：ユーザ アカウントは、Firepower シャーシに指定された TACACS+ サーバで定義する必要があります。 • [LDAP]：ユーザ アカウントは、Firepower シャーシに指定された LDAP/MS-AD サーバで定義する必要があります。 • [None]：ユーザ アカウントが Firepower シャーシに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。 （注） [Radius]、[TACACS]、および [LDAP] のすべての設定は、[Platform Settings] で設定する必要があります。詳細については、「プラットフォームの設定」の章の「AAA について」を参照してください。

名前	説明
[Console Authentication] フィールド	コンソール ポート経由で FXOS CLI に接続するときにユーザが認証される方法。次のいずれかになります。 • [Local]：ユーザ アカウントは、Firepower シャーシでローカルに定義する必要があります。 • [Radius]：ユーザ アカウントは、Firepower シャーシに指定された RADIUS サーバで定義する必要があります。 • [TACACS]：ユーザ アカウントは、Firepower シャーシに指定された TACACS+ サーバで定義する必要があります。 • [LDAP]：ユーザ アカウントは、Firepower シャーシに指定された LDAP/MS-AD サーバで定義する必要があります。 • [なし（None）]：ユーザ アカウントが Firepower シャーシにローカルである場合、ユーザがコンソール ポートを使用して FXOS CLI に接続するときにはパスワードは不要です。
リモート ユーザの設定	
リモート ユーザのロール ポリシー	ユーザがログインを試みたときに、リモート認証プロバイダーが認証情報を含むユーザ ロールを提供しない場合の動作を制御します。 • [デフォルト ロールの割り当て（Assign Default Role）]：ユーザは、読み取り専用ユーザ ロールでログインできます。 • [ログイン禁止（No-Login）]：ユーザ名とパスワードが正しい場合でも、ユーザはシステムにログインできません。
ローカル ユーザ設定	
[パスワード強度チェック（Password Strength Check）] チェックボックス	オンにすると、すべてのローカル ユーザ パスワードは、強力なパスワードのガイドラインに準拠しなければならなくなります（パスワードに関するガイドライン （3 ページ）を参照）。デフォルトでは、強力なパスワードチェックが有効になっています。

名前	説明
[History Count] フィールド	以前に使用したパスワードが再使用可能になるまでにユーザが作成する必要がある、一意のパスワードの数。履歴カウントは、最も新しいパスワードを先頭に時系列とは逆の順番で表示され、履歴カウントのしきい値に到達すると、最も古いパスワードのみが使用可能になります。 この値は、0 ～ 15 から自由に設定できます。 [History Count] フィールドを 0 に設定して履歴カウントをディセーブルにすると、ユーザは以前のパスワードをいつでも再使用できます。
[Change During Interval] フィールド	ローカル認証されたユーザがパスワードを変更できるタイミングを制御します。ここに表示される値は次のとおりです。 • [Enable]：ローカル認証されたユーザは、[Change Interval] および [Change Count] の設定に基づいてパスワードを変更できます。 • [Disable]：ローカル認証されたユーザは、[No Change Interval] に指定された期間はパスワードを変更できません。
[Change Interval] フィールド	[Change Count] フィールドで指定したパスワード変更回数が適用される時間数。 この値は、1 ～ 745 時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。
[Change Count] フィールド	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数。 この値は、0 ～ 10 から自由に設定できます。
[No Change Interval] フィールド	ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。 この値は、1 ～ 745 時間の範囲で自由に設定できます。 この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合は無視されます。
[Passphrase Expiration Days] フィールド	有効期限を 1 ~ 9999 日の間で設定します。デフォルトでは、有効期限は無効になっています。

名前	説明
[Passphrase Expiration Warning Period] フィールド	ログイン時にパスワードの有効期限をユーザに警告するのは、有効期限の何日前かを 0 ~ 9999 の間で設定します。デフォルトは、14 日です。
[Expiration Grace Period] フィールド	有効期限の何日後までにユーザがパスワードを変更する必要があるかを 0 ~ 9999 の間で設定します。デフォルトは 3 日です。
[Password Reuse Interval] フィールド	パスワードの再利用が可能になるまでの日数を 1 ~ 365 の間で設定します。デフォルトは 15 日です。[History Count] と [Password Reuse Interval] の両方を有効にする場合は、両方の要件を満たしている必要があります。たとえば、履歴カウントを 3 に設定し、再利用間隔を 10 日に設定すると、パスワードを変更できるのは 10 日間経過した後で、パスワードを 3 回変更した場合に限られます。

ステップ 4 [**保存（Save**）] をクリックします。

セッション タイムアウトの設定

FXOS CLI を使用することにより、ユーザ アクティビティなしで経過可能な時間を指定できます。この時間が経過した後、Firepower 4100/9300 シャーシはユーザセッションを閉じます。コンソール セッションと、HTTPS、SSH、および Telnet セッションとで、異なる設定を行うことができます。

タイムアウトとして 3600 秒（60 分）以下の値を設定できます。デフォルト値は 600 秒です。この設定を無効にするには、セッション タイムアウト値を 0 に設定します。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 デフォルト認証セキュリティ モードを開始します。

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

ステップ 3 HTTPS、SSH、および Telnet セッションのアイドル タイムアウトを設定します。

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

ステップ 4 （任意）コンソール セッションのアイドル タイムアウトを設定します。

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

ステップ 5 トランザクションをシステム設定にコミットします。

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

ステップ 6 （任意）セッションおよび絶対セッション タイムアウトの設定を表示します。

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

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
```

絶対セッション タイムアウトの設定

Firepower 4100/9300 シャーシには絶対セッション タイムアウト設定があり、セッションの使用状況に関係なく、絶対セッション タイムアウト期間が経過するとユーザ セッションは閉じられます。この絶対タイムアウト機能は、シリアル コンソール、SSH、HTTPS を含むすべての形式のアクセスに対してグローバルに適用されます。

シリアル コンソール セッションの絶対セッション タイムアウトを個別に設定できます。これにより、デバッグ ニーズに応えるシリアル コンソール絶対セッション タイムアウトは無効にしながら、他の形式のアクセスのタイムアウトは維持することができます。

絶対タイムアウト値のデフォルトは 3600 秒（60 分）であり、FXOS CLI を使用して変更できます。この設定を無効にするには、絶対セッション タイムアウト値を 0 に設定します。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 デフォルト認証セキュリティ モードを開始します。

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

ステップ 3 絶対セッション タイムアウトを設定します。

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

ステップ 4 （任意）別個のコンソール セッション タイムアウトを設定します。

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

ステップ 5 トランザクションをシステム設定にコミットします。

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

ステップ 6 （任意）セッションおよび絶対セッション タイムアウトの設定を表示します。

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

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
```

ログイン試行の最大回数の設定

ロックアウト前にユーザに許可されるログイン試行の最大回数を指定します。この回数を超えると、指定した時間だけ Firepower 4100/9300 シャーシからロックアウトされることになります。ユーザは、設定した最大回数を超えてログインを試行すると、システムからロックされます。ユーザがロックアウトされたことを示す通知は表示されません。これが起きると、ユーザは次にログインを試行できるようになるまで、指定された時間だけ待機する必要があります。

ログイン試行の最大数を設定するには、次の手順を実行します。

（注）

- どのタイプのユーザアカウントであっても（管理者を含む）、ログイン試行の最大数を超えてログインを試行すると、システムからロックアウトされます。
- 失敗できるログイン試行のデフォルトの最大回数は 0 です。ユーザがログイン試行の最大数を超えたときにシステムからロックアウトされるデフォルトの時間は、30 分（1800 秒）です。
- ユーザのロックアウトのステータスを表示し、ユーザのロックアウト状態をクリアする手順については、ユーザ ロックアウト ステータスの表示およびクリア （15 ページ）を参照してください。

このオプションは、システムのコモンクライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定コンプライアンスを参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 失敗できるログイン試行の最高回数を設定します。

set max-login-attempts *num_attempts*

num_attempts の値は、0 ～ 10 の範囲内の任意の整数です。

ステップ 3 ログイン試行の最高回数に達した後、ユーザがシステムからロック アウトされる時間（秒単位）を指定します。

set user-account-unlock-time

unlock_time

ステップ 4 設定をコミットします。

commit-buffer

ユーザ ロックアウト ステータスの表示およびクリア

管理者ユーザは、失敗の回数が [最大ログイン試行回数（Maximum Number of Login Attempts）] CLI 設定で指定されたログイン最大試行回数を超えた後、Firepower 4100/9300 シャーシからロックアウトされているユーザのロックアウト ステータスを表示およびクリアできます。詳細については、ログイン試行の最大回数の設定 （14 ページ）を参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 該当するユーザのユーザ情報（ロックアウト ステータスを含む）を次のように表示します。

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

例：

```
□□□□ □□□□□□□□□
 □□
 □□
 □□□□□□□
 □□□□
 □□□□□□□□
Password:
□□□ □□□□ □□□□□□□□□□
```

```
□□□□□ □□□□□□□□□□□□
□□□ □□□□
□□□□□□□□□□
□□□ SSH □□□□□
```

ステップ 3 （任意）ユーザのロックアウト ステータスをクリアします。

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

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

最小パスワード長チェックの設定

最小パスワード長チェックを有効にした場合は、指定した最小文字を使用するパスワードを作成する必要があります。たとえば、*min_length* オプションを 15 に設定した場合、パスワードは 15 文字以上を使用して作成する必要があります。このオプションは、システムのコモン クライテリア認定への準拠のための数の 1 つです。詳細については、セキュリティ認定コンプライアンスを参照してください。

最小パスワード長チェックを設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 パスワードの最小の長さを指定します。

set min-password-length *min_length*

ステップ 3 設定をコミットします。

commit-buffer

ローカル ユーザ アカウントの作成

手順

ステップ 1 [System] > [User Management] > を選択します。

ステップ 2 [Local Users] タブをクリックします。

ステップ 3 [ユーザの追加（Add User）] をクリックして [ユーザの追加（Add User）] ダイアログボックスを開きます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明
[User Name] フィールド	このアカウントにログインするときに使用されるアカウント名。この名前は、固有であり、ユーザ アカウント名のガイドラインと制限を満たしている必要があります（ユーザ名に関するガイドライン （2 ページ）を参照）。 ユーザを保存した後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone Number] フィールド	ユーザの電話番号。
[Password] フィールド	このアカウントに関連付けられているパスワード。パスワード強度チェックを有効にした場合は、ユーザ パスワードを強固なものにする必要があります。Firepower eXtensible Operating System は強度チェック要件を満たしていないパスワードを拒否します（パスワードに関するガイドライン （3 ページ）を参照）。 （注） パスワードには次の記号を含めることはできません。$（ドル記号）、?（疑問符）、=（等号）。この制限は、パスワードの強度チェックが有効になっているかどうかにかかわらず適用されます。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Status] フィールド	ステータスが [アクティブ（Active）] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Firepower Chassis Manager と FXOS CLI にログインできます。

名前	説明
[User Role] リスト	ユーザ アカウントに割り当てる権限を表すロール（ユーザの役割 （6 ページ）を参照）。 すべてのユーザはデフォルトでは読み取り専用ロールが割り当てられます。このロールは選択解除できません。複数のロールを割り当てるには、**Ctrl** を押したまま、目的のロールをクリックします。 （注） ユーザロールを削除すると、そのユーザの現在のセッション ID が取り消されます。つまり、すべてのユーザ'のアクティブセッション（CLI と Web の両方）がただちに終了します。
[Account Expires] チェックボックス	オンにすると、このアカウントは期限切れになり、[Expiration Date] フィールドに指定した日付以降に使用できなくなります。 （注） ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。
[Expiry Date] フィールド	アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。 このフィールドの終端にあるカレンダー アイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 5 [Add] をクリックします。

ローカル ユーザ アカウントの削除

手順

ステップ 1 [System] > [User Management] > を選択します。
ステップ 2 [Local Users] タブをクリックします。
ステップ 3 削除するユーザ アカウントの行で、[削除（Delete）] をクリックします。
ステップ 4 [確認（Confirm）] ダイアログボックスで、[はい（Yes）] をクリックします。

ローカルユーザアカウントのアクティブ化または非アクティブ化

ローカルユーザアカウントをアクティブ化または非アクティブ化できるのは、admin権限またはAAA権限を持つユーザのみです。

手順

ステップ1 [System] > [User Management] > を選択します。

ステップ2 [Local Users] タブをクリックします。

ステップ3 アクティブ化または非アクティブ化するユーザ アカウントの行で、[編集（Edit）]（鉛筆アイコン）をクリックします。

ステップ4 [ユーザの編集（Edit User）] ダイアログボックスで、次のいずれかの手順を実行します。

- ユーザ アカウントをアクティブ化するには、[Account Status] フィールドの [Active] オプション ボタンをクリックします。ユーザアカウントを再アクティブ化する際、アカウントのパスワードをリセットする必要があるので注意してください。
- ユーザ アカウントを非アクティブ化するには、[Account Status] フィールドの [Inactive] オプション ボタンをクリックします。

admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。

ステップ5 [保存（Save）] をクリックします。

ステップ6 トランザクションをシステム設定にコミットします。

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

ローカル認証されたユーザのパスワード履歴のクリア

手順

ステップ1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ2 指定したユーザ アカウントに対してローカル ユーザ セキュリティ モードを開始します。

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

ステップ3 指定したユーザ アカウントのパスワード履歴をクリアします。

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

ステップ 4 トランザクションをシステム設定にコミットします。

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

例

次に、パスワード履歴を消去し、トランザクションを確定する例を示します。

```
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 #
```