User Management

User Accounts

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 個のローカル 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、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。 admin 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、シャーシによって直接認証され、admin 権限か AAA 権限を持つユーザが有効または無効にできます。 ローカル ユーザ アカウントが無効になっている場合、ユーザはログインできません。無効化されたローカル ユーザ アカウントの設定の詳細はデータベースから削除されません。 無効ローカル ユーザ アカウントを再度有効にすると、アカ

ウントはユーザ名とパスワードを含め、既存のコンフィギュレーションで再びアクティブになります。

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+ で認証されたユーザ アカウントです。

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。

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 アカウントはディセーブルになります。

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日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。 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は開始できません。
- 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 権限または AAA 権限を持つユーザは、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化した場合、Firepower eXtensible Operating System は次の要件を満たしていないパスワードをすべて拒否します。

- 8 ～ 80 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- password123 のような 3 つの連続する数字を含まない。
- 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、パスワードには辞書に記載されている標準的な単語に基づいたもの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）。
- 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。

デフォルト ユーザ ロール

システムには、次のデフォルトのユーザ 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。

Read-Only

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。

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 プロファイルには、ローカル認証されたすべてのユーザ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。

Password History Count

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以前に使用したパスワードを最大 15 個まで保存します。 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最初のパスワードを 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
パスワード変更不許可	このオプションでは、ローカル認証されたユーザは、パスワードの変更後、指定された時間内にはパスワードを変更できません。 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。 • [Change During Interval] をディセーブルに • [No Change Interval] を 48 に

間隔の設定	説明	例
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 1 回まで変更できるようにする場合、次のように設定します。 • [Change During Interval] をイネーブルに • [Change Count] を 1 に • [Change Interval] を 24 に

ユーザ設定

手順

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

ステップ 2 [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。

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。
リモート ユーザ設定	

名前	説明
[Remote User Role Policy]	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。 • [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。 • [No-Login]：ユーザ名とパスワードが正しくても、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	
[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、次のパスワード セキュリティ要件に準拠する必要があります。 • 8 ～ 80 文字を含む。 • 次の少なくとも 3 種類を含む。 ◦小文字 ◦大文字 ◦数字 ◦特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • password123 のような 3 つの連続する数字を含まない。 • 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、パスワードには辞書に記載されている標準的な単語に基づいたもの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）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

名前	説明
[History Count] フィールド	自分が以前に使用したパスワードを再使用する前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 時間から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、無視されます。

ステップ 4 [Save（保存）] をクリックします。

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 [Add User] をクリックして [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。このアカウントは固有であるとともに、ユーザアカウントに関する次のガイドラインと制約事項を満たしている必要があります。 • 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は開始できません。 • 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。 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。

名前	説明
[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化した場合は、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 は次の要件を満たしていないパスワードを拒否します。 • 8 ～ 80 文字を含む。 • 次の少なくとも 3 種類を含む。 ◦ 小文字 ◦ 大文字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • password123 のような 3 つの連続する数字を含まない。 • 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、パスワードには辞書に記載されている標準的な単語に基づいたもの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）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[Account Status] フィールド	ステータスが [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 および FXOS CLI にログインできます。
[User Role] ドロップダウン 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。 **Admin** 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。 **Read-Only** 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。
[Account Expires] チェックボックス	オンにすると、このアカウントは [Expiration Date] フィールドで指定した日付に期限切れになり、それ以降は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、アカウントの有効期限を使用可能な最も遅い日付に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、[Delete] をクリックします。
ステップ 4 [Confirm] ダイアログボックスで、[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、[Edit]（鉛筆アイコン）をクリックします。
ステップ 4 [Edit User] ダイアログボックスで、次のいずれかを実行します。

- 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 [Save（保存）] をクリックします。