



## パスワード管理

- [Cisco UCS パスワードに関するガイドライン \(1 ページ\)](#)
- [Cisco UCS ユーザ名に関するガイドライン \(3 ページ\)](#)
- [変更間隔のパスワード変更の最大回数の設定 \(4 ページ\)](#)
- [パスワードの変更禁止間隔の設定 \(5 ページ\)](#)
- [パスワード履歴カウントの設定 \(5 ページ\)](#)
- [ローカル認証されたユーザのパスワードプロファイル \(6 ページ\)](#)
- [ローカル認証されたユーザのパスワード履歴のクリア \(7 ページ\)](#)
- [失われたパスワードの復旧, on page 8](#)

## Cisco UCS 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は、パスワードが必要です。admin または aaa の権限を持つユーザは、Cisco UCS Managerを設定して、ユーザのパスワードの強度チェックを実行できます。表 1: UCS パスワードに使用可能な ASCII 文字の表 (1 ページ) に、UCS パスワードに使用可能な ASCII 文字のリストを示します。

表 1: UCS パスワードに使用可能な ASCII 文字の表

| 出力可能な ASCII 文字 | 説明         |
|----------------|------------|
| A ~ Z          | 大文字の A ~ Z |
| a ~ z          | 小文字の a ~ z |
| 0 ~ 9          | 数字の 0 ~ 9  |
| !              | 感嘆符        |
| "              | 引用符        |
| %              | パーセント記号    |
| &              | アンパサンド     |

| 出力可能な ASCII 文字 | 説明       |
|----------------|----------|
| '              | アポストロフィ  |
| (              | 左カッコ     |
| )              | 右カッコ     |
| *              | アスタリスク   |
| +              | プラス記号    |
| ,              | カンマ      |
| -              | ハイフン     |
| .              | ピリオド     |
| /              | スラッシュ    |
| :              | コロン      |
| ;              | セミコロン    |
| <              | 小なり      |
| >              | 大なり      |
| @              | アットマーク   |
| [              | 開き大カッコ   |
| \              | バックスラッシュ |
| ]              | 閉じ大カッコ   |
| ^              | キャレット    |
| _              | アンダースコア  |
| `              | アクサングラーブ |
| {              | 開き中カッコ   |
|                | 縦棒       |
| }              | 閉じ中カッコ   |
| ~              | チルダ      |

シスコでは強力なパスワードを使用することを推奨しています。そうしなかった場合、ローカル認証されたユーザに対するパスワードの強度チェックで、Cisco UCS Manager によって次の要件を満たさないパスワードが拒否されます。

- 8 ～ 80 文字を含む。
- パスワードの強度の確認が有効になっている場合はパスワード長は可変で、6 ～ 80 文字の間で設定できます。



---

(注) デフォルトは 8 文字です。

---

- 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。
- 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。

## Cisco UCS ユーザ名に関するガイドライン

ユーザ名は、Cisco UCS Manager のログイン ID としても使用されます。Cisco UCS 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、Cisco UCS Manager 内で一意である必要があります。
- ログイン ID は、英文字から始まる必要があります。アンダースコアなどの特殊文字や数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。
- すべてが数字のログイン 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。

## 変更間隔のパスワード変更の最大回数の設定

パスワードプロファイルプロパティを変更するには、admin または aaa 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

### 手順

---

**ステップ 1** [Navigation] ペインで [Admin] をクリックします。

**ステップ 2** [All] > [User Management] > [User Services] の順に展開します。

**ステップ 3** [Locally Authenticated Users] ノードをクリックします。

**ステップ 4** [Password Profile] 領域で、次の手順を実行します。

a) [Change During Interval] フィールドで、[Enable] をクリックします。

b) [Change Count] フィールドで、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を入力します。

この値は、0 ~ 10 から自由に設定できます。

c) [Change Interval] フィールドで、[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数を入力します。

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。

**ステップ 5** [Save Changes] をクリックします。

---

## パスワードの変更禁止間隔の設定

パスワードプロファイルプロパティを変更するには、**admin**または**aaa**権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、**admin**または**aaa**権限を持つユーザに適用されません。

### 手順

**ステップ 1** [Navigation] ペインで [Admin] をクリックします。

**ステップ 2** [All] > [User Management] > [User Services]の順に展開します。

**ステップ 3** [Locally Authenticated Users] ノードをクリックします。

**ステップ 4** [Password Profile] 領域で、次の手順を実行します。

- a) [Change During Interval] フィールドで、**[Enable]** をクリックします。
- b) [No Change Interval] フィールドで、ローカル認証されたユーザが、新しく作成されたパスワードを変更する前に待機する時間の最小数。を入力します。

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] に設定されている場合、無視されます。

**ステップ 5** [Save Changes] をクリックします。

## パスワード履歴カウントの設定

パスワードプロファイルプロパティを変更するには、**admin**または**aaa**権限を持っている必要があります。

### 手順

**ステップ 1** [Navigation] ペインで [Admin] をクリックします。

**ステップ 2** [All] > [User Management] > [User Services]の順に展開します。

**ステップ 3** [Locally Authenticated Users] ノードをクリックします。

**ステップ 4** [Password Profile] 領域で、ローカル認証されたユーザが、以前 [History Count] フィールドで使用したパスワードを再使用できるようになる前に、作成する必要がある一意のパスワードの数をに入力します。

この値は、0 ~ 15 から自由に設定できます。

デフォルトでは、[History Count] フィールドは 0 に設定されます。これにより、履歴カウントが無効になるため、ユーザはいつでも以前に使用していたパスワードを再利用できます。

ステップ 5 [Save Changes] をクリックします。

## 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、Cisco UCS Manager の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。



(注) パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

### 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同じパスワードを再使用しないようにすることができます。パスワード履歴カウントを設定すると、Cisco UCS Manager は過去に使用されたパスワードを最大 15 個まで保存します。パスワード履歴カウントには最新のパスワードを先頭に、パスワードが新しい順に保存されます。そのため、履歴カウントがしきい値に達したときには、最も古いパスワードを再利用できます。

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と、ユーザはパスワードを再利用できます。たとえば、パスワード履歴カウントを 8 に設定した場合、ユーザは 9 番目のパスワードが期限切れになる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、履歴のカウントを無効にし、ユーザはいつでも前のパスワードを使用できます。

ローカル認証されたユーザのパスワード履歴カウントをクリアして、以前のパスワードを再利用可能にすることができます。

### 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の回数を制限します。次の表で、パスワード変更間隔の 2 つの間隔設定オプションについて説明します。

| 間隔の設定   | 説明   | 例   |
|---|--|---|
| [No password change allowed]                      | パスワードの変更に後、指定された時間の間は、ローカル認証されたユーザのパスワードを変更することはできません。<br><br>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。  | パスワード変更後 48 時間以内にユーザがパスワードを変更するのを防ぐため：<br><br><ul style="list-style-type: none"> <li>• [Change During Interval] を無効に設定</li> <li>• [No Change Interval] を 48 に設定</li> </ul>  |
| [Password changes allowed within change interval] | 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。<br><br>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。 | パスワード変更後 24 時間以内に最大 1 回のパスワード変更を許可するには、次のような設定を行います。<br><br><ul style="list-style-type: none"> <li>• [Change during interval] を有効に設定</li> <li>• [Change count] を 1 に設定</li> <li>• [Change interval] を 24 に設定</li> </ul> |

## 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 [Navigation] ペインで [Admin] をクリックします。
  - ステップ 2 [All] > [User Management] > [User Services] > [Locally Authenticated Users] の順に展開します。
  - ステップ 3 パスワード履歴をクリアするユーザをクリックします。
  - ステップ 4 [Actions] 領域で、[Clear Password History] をクリックします。
  - ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
-

# 失われたパスワードの復旧

## admin アカウントのパスワードの復旧

admin アカウントは、システムアドミニストレータまたはスーパーユーザのアカウントです。アドミニストレータが admin アカウントのパスワードを失うと、重大なセキュリティ上の問題が発生する可能性があります。admin アカウントのパスワードを回復させる手順では、すべてのファブリックインターコネクต์に電源を再投入する必要があり、データ伝送が一時的に停止します。

admin アカウントのパスワードを復旧する場合、実際にはそのアカウントのパスワードを変更します。admin アカウントに対応する元のパスワードを取得することはできません。

admin 以外のすべてのローカル アカウントのパスワードは、Cisco UCS Manager からリセットできます。ただし、aaa または admin 権限を持つアカウントを使用して Cisco UCS Manager にログインする必要があります。



**注意** Cisco UCS Mini の場合、この手順で Cisco UCS ドメインに含まれるすべてのファブリック インターコネクต์をシャーシスロットから取り出す必要があります。したがって、ファブリック インターコネクต์がそれぞれのシャーシスロットに戻されるまでは、Cisco UCS ドメインでのデータ送信が全面的に停止します。

他の Cisco UCS については、この手順ですべてのファブリック インターコネクต์の電源を切る必要があります。したがって、ファブリック インターコネクต์が再起動されるまでは、Cisco UCS ドメイン内のデータ送信が全面的に停止します。



(注) Cisco UCS 6400 シリーズ ファブリック インターコネクต์ 別のカーネルとシステム イメージを持っていません。1 つの統一されたイメージがあります。

## ファブリック インターコネクットのリーダーシップ ロールの決定



**重要** 管理者パスワードがわからなくなった場合にクラスタ内のファブリック インターコネクットの権限を判別するには、両方のファブリック インターコネクットの IP アドレスから Cisco UCS Manager GUI を開きます。従属ファブリック インターコネクットは失敗し、次のメッセージが表示されます。

```
UCSM GUI is not available on secondary node.
```



## 手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。
- ステップ 3 ロールを識別するファブリック インターコネクットをクリックします。
- ステップ 4 [Work] ペインで、[General] タブをクリックします。
- ステップ 5 [General] タブで、[High Availability Details] バーの下矢印をクリックしてこの領域を展開します。
- ステップ 6 [Leadership] フィールドを表示して、このファブリック インターコネクットがプライマリ ファブリック インターコネクットか、従属ファブリック インターコネクットかを決定します。

## ファブリック インターコネクットのファームウェアバージョンの確認

次の手順を使用して、Cisco UCS ドメインのすべてのファブリック インターコネクットのファームウェアバージョンを確認できます。ファブリック インターコネクットの [Installed Firmware] タブを使用すると、単一のファブリック インターコネクットのファームウェアを確認できます。

## 手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2 [Equipment] タブで [Equipment] ノードをクリックします。
- ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ 4 [Installed Firmware] タブで、次に示す各ファブリック インターコネクットのファームウェアバージョンが、アップデートしたファームウェアのバージョンと一致していることを確認します。
  - カーネル バージョン
  - システム バージョン

## 6200 および 6300 FI シリーズのスタンドアロン構成での admin アカウントパスワードの復旧

この手順により、ファブリック インターコネクットで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

### 始める前に

1. ファブリック インターコネクットのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次のファームウェアの実行中のバージョンを確認します。
  - ファブリック インターコネクットのファームウェア カーネルバージョン
  - ファームウェア システム バージョン



**ヒント** この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザアカウントを使用してログインします。

### 手順

- ステップ 1** コンソール ポートに接続します。
- ステップ 2** ファブリック インターコネクットの電源を次のように再投入します。
- a) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクットの電源をオフにします。
  - b) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクットの電源をオンにします。
- ステップ 3** コンソールで次のいずれかのキーの組み合わせを押して、起動時に loader プロンプトを表示させます。

- **Ctrl+l**
- **Ctrl+Shift+r**

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

- ステップ 4** ファブリック インターコネクットのカーネル ファームウェア バージョンをブートします。

```
loader >  
boot /installables/switch/  
kernel_firmware_version
```

例 :

```
loader > boot  
/installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

```
loader > boot  
/installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

- ステップ 5** config ターミナル モードを入力します。

```
Fabric (boot) #  
config terminal
```

**ステップ 6** admin パスワードをリセットします。

```
Fabric (boot) (config) #  
admin-password  
password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

**ステップ 7** config ターミナル モードを終了し、ブート プロンプトに戻ります。

**ステップ 8** ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric (boot) #  
load /installables/switch/  
system_firmware_version
```

例 :

```
Fabric (boot) # load  
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

```
Fabric (boot) # load  
/installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

**ステップ 9** システム イメージがロードされたら、Cisco UCS Manager にログインします。

**ステップ 10** Cisco UCS Manager で新しいパスワードを同期します。

```
UCS-B # scope security  
UCS-B/security # set password  
Enter new password: New_password  
Confirm new password: New_password  
UCS-B/security* # commit-buffer
```

## スタンドアロン構成の Admin アカウント パスワードの復旧 Cisco UCS 6400 シリーズ ファブリック インターコネクト

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

始める前に

1. ファブリック インターコネクトのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。

2. 実行中の Cisco UCS 6400 シリーズ ファブリック インターコネクト イメージのバージョンを確認します。



(注) Cisco UCS 6400 シリーズ ファブリック インターコネクト 別のカーネルとシステム イメージを持っていません。1つの統一されたイメージがあります。



ヒント この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザアカウントを使用してログインします。

### 手順

**ステップ 1** コンソール ポートに接続します。

**ステップ 2** UCS-A(local-mgmt)# **reboot**

これにより、ファブリック インターコネクトがリブートします。

ファブリック インターコネクトの電源再投入を行うこともできます。

**ステップ 3** リブートしたら、コンソールで **Ctrl+c** キーを押して loader プロンプトを表示させます。  
**Ctrl+c**

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

**ステップ 4** loader プロンプトで、次のコマンドを実行します。

```
loader > cmdline recoverymode=1
```

**ステップ 5** ファブリック インターコネクトで Cisco UCS 6400 シリーズ ファブリック インターコネクト イメージをブートします。

```
loader > boot /installables/switch/Cisco UCS 6400 FI Image
```

例：

```
loader > boot  
/installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin
```

**ステップ 6** config ターミナル モードを開始します。

```
switch(boot)# config terminal
```

**ステップ 7** admin パスワードをリセットします。

```
switch(boot) (config)# admin-password New_password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

**ステップ 8** config ターミナル モードを終了して FI をリブートします。

```
switch(boot) (config) # exit  
switch(boot) # exit
```

**ステップ 9** ログインプロンプトが表示されるまで待ってから、新しいパスワードを使用してログインします。

```
Cisco UCS 6400 Series Fabric Interconnect  
login: admin  
Password:New_password
```

**ステップ 10** Cisco UCS Manager で新しいパスワードを同期します。

```
UCS-A # scope security  
UCS-A/security # set password  
Enter new password: New_password  
Confirm new password: New_password  
UCS-A/security* # commit-buffer
```

---

## 6200 および 6300 FI シリーズのクラスタ構成での Admin アカウントパスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

### 始める前に

1. ファブリック インターコネクトのコンソールポートのいずれか1つを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。
  - ファブリック インターコネクトのファームウェア カーネル バージョン
  - ファームウェア システム バージョン
  - プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト



**ヒント** この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザアカウントを使用してログインします。

## 手順

**ステップ 1** 下位のファブリック インターコネクットのコンソール ポートに接続します。

**ステップ 2** 従属ファブリック インターコネクットの場合は、次の手順を実行します。

- a) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクットの電源をオフにします。
- b) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクットの電源をオンにします。
- c) コンソールで次のいずれかのキーの組み合わせを押して、起動時に loader プロンプトを表示させます。

- **Ctrl+l**

- **Ctrl+Shift+r**

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければなりません場合があります。

**ステップ 3** プライマリ ファブリック インターコネクットの電源を次のように再投入します。

- a) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクットの電源をオフにします。
- b) Cisco UCS Mini の場合、ファブリック インターコネクットをシャーシスロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクットの電源をオンにします。

**ステップ 4** コンソールで次のいずれかのキーの組み合わせを押して、起動時に loader プロンプトを表示させます。

- **Ctrl+l**

- **Ctrl+Shift+r**

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければなりません場合があります。

**ステップ 5** プライマリ ファブリック インターコネクットのカーネルファームウェアバージョンをブートします。

```
loader > boot /installables/switch/  
kernel_firmware_version
```

例 :

```
loader > boot  
/installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

```
loader > boot  
/installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

**ステップ 6** config ターミナル モードを入力します。

```
Fabric(boot)# config terminal
```

**ステップ 7** admin パスワードをリセットします。

```
Fabric(boot) (config) # admin-password password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

**ステップ 8** config ターミナル モードを終了し、ブート プロンプトに戻ります。

**ステップ 9** プライマリ ファブリック インターコネクットのシステム ファームウェア バージョンをブートします。

```
Fabric(boot) # load /installables/switch/  
system_firmware_version
```

例 :

```
Fabric(boot) # load  
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

```
Fabric(boot) # load  
/installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

**ステップ 10** システム イメージがロードされたら、Cisco UCS Manager にログインします。

**ステップ 11** 従属ファブリック インターコネクットのコンソールで、次の手順を実行してシステムを起動します。

a) 従属ファブリック インターコネクットのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/  
kernel_firmware_version
```

b) 従属ファブリック インターコネクットのシステム ファームウェア バージョンをブートします。

```
Fabric(boot) # load /installables/switch/  
system_firmware_version
```

**ステップ 12** Cisco UCS Manager と他の FI で新しいパスワードを同期します。

```
UCS-B # scope security  
UCS-B/security # set password  
Enter new password: New_password  
Confirm new password: New_password  
UCS-B/security* # commit-buffer
```

## クラスタ構成での Admin アカウント パスワードの復旧 Cisco UCS 6400 シリーズ ファブリック インターコネクト

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

### 始める前に

1. ファブリック インターコネクトのコンソールポートのいずれか1つを、コンピュータターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。

- Cisco UCS 6400 シリーズ ファブリック インターコネクト のイメージ



(注) Cisco UCS 6400 シリーズファブリック インターコネクト別のカーネルとシステム イメージを持っていません。1つの統一されたイメージがあります。

- プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト



**ヒント** この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザアカウントを使用してログインします。

### 手順

**ステップ 1** 下位のファブリック インターコネクトのコンソール ポートに接続します。

**ステップ 2** UCS-B(local-mgmt) # **reboot**

これにより、従属ファブリック インターコネクトがリブートします。

従属ファブリック インターコネクトの電源再投入を行うこともできます。

**ステップ 3** リブートしたら、コンソールで **Ctrl+c** キーを押して loader プロンプトを表示させます。  
**Ctrl+c**

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

**ステップ 4** loader プロンプトで、次のコマンドを実行します。



```
loader > cmdline recoverymode=1
```

- ステップ 5** ファブリック インターコネクトでCisco UCS 6400 シリーズ ファブリック インターコネクトイメージをブートします。

```
loader > boot /installables/switch/Cisco UCS 6400 Series FI Image
```

例 :

```
loader > boot  
/installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin
```

- ステップ 6** config ターミナル モードを開始します。

```
switch(boot)# config terminal
```

- ステップ 7** admin パスワードをリセットします。

```
switch(boot) (config)# admin-password New_password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

- ステップ 8** config ターミナル モードを終了して FI をリブートします。

```
switch(boot) (config)# exit  
switch(boot)# exit
```

- ステップ 9** ログインプロンプトが表示されるまで待ってから、新しいパスワードを使用してログインします。

```
Cisco UCS 6400 Series Fabric Interconnect  
login: admin  
Password:New_password
```

- ステップ 10** Cisco UCS Manager と他の FI で新しいパスワードを同期します。

```
UCS-B # scope security  
UCS-B/security # set password  
Enter new password: New_password  
Confirm new password: New_password  
UCS-B/security* # commit-buffer
```

