パスワード管理

Cisco UCS パスワードに関するガイドライン

それぞれのローカル認証されたユーザ 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
.	period
/	スラッシュ
:	colon
;	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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval enable**	ローカル認証されたユーザが指定された時間の間に実行できるパスワード変更の回数を制限します。
ステップ 4	UCS-A /security/password-profile # **set change-count** *pass-change-num*	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 を指定します。 この値は、0 ～ 10 から自由に設定できます。
ステップ 5	UCS-A /security/password-profile # **set change-interval** *num-of-hours*	[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 を指定します 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

	コマンドまたはアクション	目的
		パスワード変更を実行することはできません。
ステップ 6	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、change during interval オプションをイネーブルにし、変更回数を 5 回、変更間隔を 72 時間に設定し、トランザクションをコミットします。

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

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval disable**	間隔中の変更機能をディセーブルにします。
ステップ 4	UCS-A /security/password-profile # **set no-change-interval** *min-num-hours*	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。 を指定します 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] に設定されている場合、無視されます。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、間隔中の変更オプションをディセーブルにし、変更禁止間隔を 72 時間に設定し、トランザクションをコミットする例を示します。

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

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set history-count** *num-of-passwords*	ローカル認証されたユーザが、以前に使用されたパスワードを再利用できるまでに、作成する必要がある一意のパスワードの数を指定します。 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。この値によって履歴カウントが無効化されるため、ユーザはいつでも以前のパスワードを使用できます。
ステップ 4	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set history-count 5
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

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利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が先頭で、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使用できます。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る後まで再使用できません。

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。

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使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。 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： • [Change During Interval] を無効に設定 • [No Change Interval] を 48 に設定
変更間隔内のパスワード変更許可	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。	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。 • [Change during interval] を有効に設定 • [Change count] を 1 に設定 • [Change interval] を 24 に設定

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *user-name*	指定されたユーザ アカウントに対するローカル ユーザ セキュリティ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set clear password-history yes**	指定されたユーザアカウントのパスワード履歴をクリアします。
ステップ 4	UCS-A /security/local-user # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope local-user admin
UCS-A /security/local-user # set clear password-history yes
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

失われたパスワードの復旧

amin 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 インターコネクト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 インターコネクトをシャーシ 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 インターコネクト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 インターコネクトの電源を切る必要があります。したがって、ファブリック インターコネクト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 6454 Fabric Interconnect 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 インターコネクトのリーダーシップ ロールの決定

（注） 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show cluster state**	クラスタの両方のファブリック インターコネクトの動作状態およびリーダーシップ ロールを表示します。

例

次に、クラスタの両方のファブリック インターコネクトのリーダーシップ ロールを表示する例を示します。ここでは、ファブリック インターコネクト A がプライマリ ロールで、ファブリック インターコネクト B が従属ロールです。

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

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. 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 6454 Fabric Interconnect

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 6454 Fabric Interconnect イメージのバージョンを確認します。

（注） Cisco UCS 6454 Fabric Interconnect 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 6454 Fabric Interconnectイメージをブートします。

```
loader > boot /installables/switch/Cisco UCS 6454 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らない場合があります。

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らない場合があります。

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 6454 Fabric Interconnect

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 6454 Fabric Interconnect のイメージ

（注） Cisco UCS 6454 Fabric Interconnect 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 6454 Fabric Interconnectイメージをブートします。

```
loader > boot /installables/switch/Cisco UCS 6454 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
```