

firepowerシステムでの管理者ユーザのパスワードのリセット

内容

[はじめに](#)

[背景説明](#)

[Firepower脅威に対する防御：管理者パスワードのリセット](#)

[ASA Firepowerサービスモジュール：管理者パスワードのリセット](#)

[ASA 5512-XからASA 5555-X\(ソフトウェアASA Firepowerモジュール\)およびISA 3000デバイスを経由したASA 5512-XおよびASA 5506-Xでの管理者パスワードのリセット](#)

[ASA 5585-Xシリーズデバイスでの管理者パスワードのリセット\(ハードウェアASA Firepowerモジュール\)](#)

[FMCおよびNGIPSvのCLIまたはシェル管理者パスワードの変更](#)

[FMCのWebインターフェイス管理者パスワード、または7000および8000シリーズデバイスのWebインターフェイス管理者およびCLI管理者パスワードの変更](#)

[FMCまたはNGIPSvの失われたCLIまたはシェル管理者パスワードのリセット、または7000および8000シリーズデバイスの失われたWebインターフェイスまたはCLIパスワードのリセット](#)

[オプション 1デバイスを安全にリポートし、ブート時にシングルユーザモードに入ってパスワードをリセットする](#)

[オプション 2外部認証を使用してCLIにアクセスし、Firepower Management Centerのパスワードをリセットする](#)

[firepower Management Centerの失われたWebインターフェイス管理者パスワードのリセット](#)

kWh

はじめに


このドキュメントでは、Firepowerシステムの管理者アカウントのパスワードをリセットする手順について説明します。

背景説明

firepower Management Center(FMC)は、コマンドラインインターフェイス(CLI)/シェルアクセスとWebインターフェイスアクセス(使用可能な場合)に対して、異なる管理者アカウント(個別のパスワード付き)を提供します。firepowerや適応型セキュリティアプライアンス(ASA) Firepowerサービスアプライアンスなどの管理対象デバイスの管理者アカウントは、CLIアクセス、シェルアクセス、およびWebインターフェイスアクセス(使用可能な場合)で同じです。

ここでは、Firepower Management Centerについて説明します。

 注: Firepower Management Center CLIのリファレンスは、バージョン6.3以降にのみ適用さ

 れます。7000および8000シリーズのデバイスは、バージョン6.4でサポートされています。

Firepower脅威に対する防御：管理者パスワードのリセット

firepower9300および4100プラットフォーム上のFirepower Threat Defense(FTD)論理デバイスで失われた管理者パスワードをリセットするには、『[FXOS Chassis Managerを使用したFTDのパスワードの変更または回復](#)』ガイドの手順を実行します。

firepower1000/2100/3100で稼働するFTDデバイスの場合は、デバイスのイメージを再作成する必要があります。これらのプラットフォームでの再イメージ化手順については、『[Firepower脅威対策を実行するFirepower 1000/2100シリーズのCisco FXOSトラブルシューティングガイド](#)』を参照してください。


ASA 5500-XおよびIntegrated Security Appliance(ISA)3000モデルで稼働するFTDデバイスでは、デバイスのイメージを再作成する必要があります。手順については『[Cisco ASA and Firepower Threat Defense Device Reimage Guide](#)』を参照してください。

仮想FTDデバイスの場合は、新しい展開でデバイスを置き換える必要があります。

物理デバイスの再イメージ化によって設定が消去され、管理者パスワードが Admin123を参照。

アマゾンウェブサービス(AWS)でFirepower7.0+を使用するFTDvを除き、新しいFTDvデプロイメントには設定がなく、admin passwordは Admin123を参照。AWSでFirepower7.0+を使用するFTDvの場合、新しいデプロイには設定がなく、デフォルトパスワードはありません。デプロイ時に管理者パスワードを入力します。

- Firepower Device Manager で管理されている FTD デバイスのイメージを再作成する場合：
 - 最近の外部に保存されたバックアップがある場合は、再イメージ化した後でバックアップされた設定を復元できません。詳細については、ご使用のバージョンの『[CiscoFirepower脅威対策コンフィギュレーションガイドfor Firepower Device Manager](#)』を参照してください。
 - バックアップがない場合は、インターフェイス、ルーティングポリシー、DHCPおよびダイナミックドメインネームシステム(DDNS)の設定を含むデバイス設定を手動で再作成する必要があります。
- firepower Management Centerで管理されているFTDデバイス、およびバージョン6.3+が稼働しているFMCとデバイスを再イメージ化する場合、再イメージ化の前にFMCのWebインターフェイスを使用してデバイス設定をバックアップし、再イメージ化後にバックアップを復元できます。詳細については、ご使用のバージョンの『[Firepower Management Center Configuration Guide](#)』を参照してください。

 注：バージョン6.0.1 ~ 6.2.3を実行している場合は、FTD設定をバックアップできません。バージョン6.3.0 ~ 6.6.0を実行する場合、FTDコンテナインスタンスでは、FMC Webインターフェイスからのバックアップと復元はサポートされません。再イメージ化した後でFirepowerマネジメントセンターから共有ポリシーを適用できますが、デバイス固有の設定(インターフェイス、ルーティングポリシー、DHCPおよびDDNS設定など)は手動で行う必要があります。

ASAFirepowerサービスモジュール：管理者パスワードのリセット

ASAFirepowerモジュールCLIのadmin passwordは、ASA一般操作CLIのsessionコマンドを使用してリセットできます。ASA CLIのパスワードを紛失した場合は、ご使用のASAバージョンの『[CLIブック1: Cisco ASAシリーズ一般操作CLIコンフィギュレーションガイド](#)』で説明されているように回復できます。

ASA 5512-XからASA 5555-X(ソフトウェアASAFirepowerモジュール)およびISA 3000デバイスを経由したASA 5512-XおよびASA 5506-Xでの管理者パスワードのリセット

ASAFirepowerソフトウェアモジュールまたはISA 3000デバイスのadminユーザをデフォルトパスワードにリセットするには、ASAプロンプトで次のコマンドを入力します。

```
session sfr do password-reset
```

詳細については、ご使用のASAバージョンの『[Cisco ASAシリーズCLIブック2: Cisco ASAシリーズファイアウォールCLIコンフィギュレーションガイド](#)』を参照してください。

ASA 5585-Xシリーズデバイスでの管理者パスワードのリセット(ハードウェアASAFirepowerモジュール)

ASA FirePOWER ハードウェアモジュールの admin ユーザーのパスワードをデフォルトにリセットするには、ASA プロンプトで次のコマンドを入力します。

```
session 1 do password-reset
```

詳細については、ご使用のASAバージョンの『[Cisco ASAシリーズCLIブック2: Cisco ASAシリーズファイアウォールCLIコンフィギュレーションガイド](#)』を参照してください。

FMCおよびNGIPSvのCLIまたはシェル管理者パスワードの変更

これらの管理者アカウントの既知のパスワードをリセットするには、次の手順を使用します。

- Firepower Management Center: CLIまたはシェルへのアクセスに使用されるadmin password。
- Next Generation Information Preservation System(NGIPSv)virtual: CLIへのアクセスに使用されるadminパスワード。

手順：

1. SSHまたはコンソールを使用して、アプライアンスの管理者アカウントにログインします。
 - firepower Management Centerの場合：
 - firepower Management CenterがFirepowerバージョン6.2以下を実行している場合、ログインするとLinuxシェルに直接アクセスできます。

- firepower Management CenterがFirepowerバージョン6.3または6.4を実行していて、Firepower Management Center CLIが有効になっていない場合、ログインするとLinuxシェルに直接アクセスできます。
 - firepower Management CenterがFirepowerバージョン6.3または6.4を実行しており、Firepower Management CLIが有効になっている場合は、ログインするとFirepower Management Center CLIにアクセスできます。expertコマンドを入力して、Linuxシェルにアクセスします。
 - firepower Management CenterでFirepowerバージョン6.5+が稼働している場合、ログインするとFirepower Management CenterのCLIにアクセスできます。expertコマンドを入力して、Linuxシェルにアクセスします。
 - 管理対象デバイスの場合、ログインするとデバイスのCLIにアクセスできます。expertコマンドを入力して、Linuxシェルにアクセスします。
2. シェルプロンプトで、次のコマンドを入力します。 `sudo passwd admin`.
 3. プロンプトが表示されたら、現在の admin パスワードを入力して権限をルートアクセスに昇格させます。
 4. プロンプトに応じて、新しい admin パスワードを 2 回入力します。



注：システムに「BAD PASSWORD」というメッセージが表示されます。これは情報としての意味しかありません。このメッセージが表示されたとしても、システムはユーザーが指定したパスワードを適用します。とはいえ、セキュリティ上の理由から、より複雑なパスワードを設定することを推奨します。

5. Type `exit` をクリックしてシェルを終了します。
6. 管理対象デバイスまたはCLIが有効になっているFirepowerManagement Centerで、次のように入力します `exit` CLIを終了します。

FMCのWebインターフェイス管理者パスワード、または7000および8000シリーズデバイスのWebインターフェイス管理者およびCLI管理者パスワードの変更

これらの管理者アカウントの既知のパスワードをリセットするには、次の手順を使用します。

- Firepower管理センター：Webインターフェイスへのアクセスに使用されるadmin password。
- 7000および8000シリーズデバイス：WebインターフェイスおよびCLIへのアクセスに使用されるadmin password。

手順：


1. 管理者アクセス権を持つユーザとしてアプライアンスのWebインターフェイスにログインします。
2. 選択 `System > Users` をクリックし、`Edit` アイコンをクリックします。
3. の値を入力します。 `Password` と `Confirm Password` フィールド。
値は同じであり、ユーザに設定されたパスワードオプションに準拠している必要があります。
-

4. クリック Saveを参照。

FMCまたはNGIPSvの失われたCLIまたはシェル管理者パスワードのリセット、または7000および8000シリーズデバイスの失われたWebインターフェイスまたはCLIパスワードのリセット

これらの管理者アカウントの失われたパスワードをリセットするには、次の手順を使用します。

- Firepower Management Center:CLIまたはシェルへのアクセスに使用されるadmin password。
- 7000および8000シリーズデバイス：WebインターフェイスおよびCLIへのアクセスに使用されるadmin password。
- NGIPSv:CLIへのアクセスに使用されるadminパスワード。

 注：これらの管理者アカウントの失われたパスワードをリセットするには、アプライアンスとのコンソールまたはSSH接続を確立する必要があります(外部Firepowerが設定されたUser Management Centerの場合は、SSH接続を使用できます)。さらに、admin ログイン情報を紛失したアプライアンスを再起動する必要もあります。使用可能なデバイスアクセスのタイプに応じて、次のようなさまざまな方法でリブートを開始できます。

- Management CenterのFirepowerには、管理者アクセス権を持つWebインタフェース・ユーザーのログイン資格証明、またはCLI/シェル・アクセス権を持つ外部認証ユーザーのログイン資格証明が必要です。
 - 7000または8000シリーズのデバイスでは、次のいずれかのアクセス方法でログイン認証情報が必要です：管理者アクセス権を持つWebインターフェイスユーザー、設定アクセス権を持つCLIユーザー、または管理対象FirepowerManagement Centerの管理者アクセス権を持つユーザー。
 - NGIPSvの場合、構成アクセス権を持つCLIユーザーまたは管理対象Firepower管理センターの管理者アクセス権を持つユーザーのログイン資格情報が必要です。
 - Firepower Management Center、7000および8000シリーズ・デバイス、NGIPSvデバイスの場合、コンソール接続（物理またはリモート）があれば、ログイン・クレデンシャルなしでこのタスクを実行できます。
- これらの方法でデバイスにアクセスできない場合は、次の手順で管理者パスワードをリセットできません。Cisco TACにお問い合わせください。

オプション 1デバイスを安全にリブートし、ブート時にシングルユーザモードに入ってパスワードをリセットする

1. admin パスワードを紛失したデバイスのアプライアンスコンソールへの接続を開きます。
 - 7000シリーズデバイス、8000シリーズデバイス、およびFirepower Management Centerの場合は、キーボード/モニタまたはシリアル接続を使用します。
 - 仮想アプライアンスの場合は、仮想プラットフォームが提供するコンソールを使用します。詳細については、『[Cisco Firepower Management Center Virtual Getting Started Guide](#)』または『[Cisco Firepower NGIPSv Quick Start Guide for VMware](#)』を参照してください。
 - あるいは、Firepower・マネジメント・センター、7000および8000シリーズ、および仮想

アプライアンスの場合、リモートのキーボード・ビデオ/マウス(KVM)を使用してアプライアンスとのコンソール接続を確立すれば、そのインターフェイスにアクセスできます。

2. admin パスワードを紛失したデバイスを再起動します。次の選択肢があります。

• Firepower Management Center の場合：

A. 管理者アクセス権を持つユーザーとして Firepower Management Center の Web インターフェイスにログインします。

B. ご使用のバージョンの『[Firepower Management Center Configuration Guide](#)』の説明に従って、[Firepower Management Center を再起動します。](#)

• 7000または8000シリーズのデバイスまたはNGIPSvで、管理対象Firepower管理センターで管理者アクセス権を持つWebインターフェイスユーザのクレデンシャルを持っている場合：

a.管理者アクセス権を持つユーザーとして、管理対象Firepower管理センターのWebインターフェイスにログインします。

B. ご使用のバージョンの『[Firepower Management Center Configuration Guide](#)』の説明に従って、[管理対象デバイスをシャットダウンして再起動します。](#)

• 7000 または 8000 シリーズ デバイスで、管理者アクセス権を含む Web インターフェイス ユーザーのログイン情報がある場合：

A. 管理者アクセス権を持つユーザーとしてデバイスの Web インターフェイスにログインします。


B. ご使用のバージョンの『[Firepower Management Center Configuration Guide](#)』の説明に従って、[デバイスを再起動します。](#)


• 7000 または 8000 シリーズ デバイスまたは NGIPSv で、設定アクセス権を持つ CLI ユーザーのログイン情報がある場合：

a. CLI設定アクセス権を持つユーザ名で、シェルによってアプライアンスにログインします。

B. プロンプトで、system reboot コマンドを入力します。


• Firepower Management Center、7000および8000シリーズ、およびコンソール付き仮想アプライアンスの場合は、CTRL-ALT-DELを参照。(リモートKVMを使用する場合、KVMインターフェイスは次の送信手段を提供します。CTRL-ALT-DEL KVM自体に干渉することなくデバイスに接続できます)。

 注:Firepower Management Centerまたは管理対象デバイスをリブートすると、アプライアンスからログアウトされ、完了までに最大1時間かかる可能性のあるデータベースチェックが実行されます。

 注意：電源ボタンを使用してアプライアンスをシャットダウンしたり、電源ケーブルを抜いたりしないでください。システムデータベースが破損する可能性があります。Webインターフェイスを使用してアプライアンスを完全にシャットダウンします。

3.アプライアンスのコンソール画面で、再起動プロセスを確認し、再起動するアプライアンスの

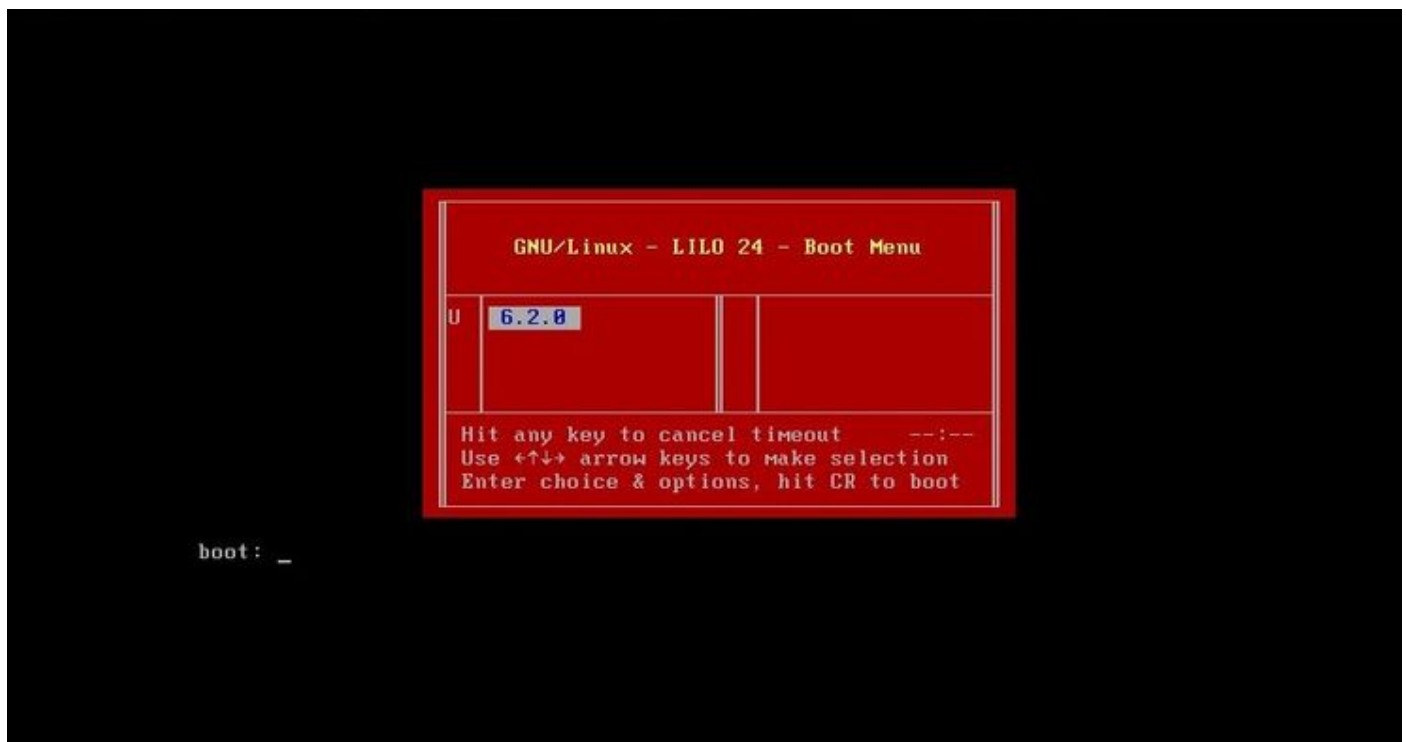
種類に応じて次の手順を実行します。

 注：システムでデータベースチェックが行われている場合は、次のメッセージが表示されま
す。 The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish.

• Firepower Management Center モデル 750、1500、2000、3500、または4000 の場合、または
Firepower 7000 または 8000 シリーズ デバイスまたは NGIPSv の場合は、再起動プロセスを中断
します。

A. アプライアンスが起動したら、キーボードの任意のキーを押して LILO ブートメニューでカウ
ントダウンをキャンセルします。

B. LILO ブートメニューに表示されるバージョン番号をメモします。この例では、バージョン番
号は6.2.0です。



c. boot : プロンプトで、version singleコマンドを入力します。ここで、versionはバージョン番号
です (たとえば、6.2.0 single)。システムでUnited Capabilities Approved Products
List(UCAPL)コンプライアンスが有効になっている場合は、パスワードを入力するように求められ
ます。パスワードを入力します Sourcefireを参照。

• Management CenterのFirepower・ モデル1000、1600、2500、2600、4500、4600の場合：
ブートメニューが表示されたら、 Option 4, Cisco Firepower Management Console Password Restore Modeを参照。

4.新しい管理者パスワードを割り当てます。デバイスに適した手順を使用してください。

• Firepower Management CenterまたはNGIPSvの新しいCLIおよびシェル管理パスワードの場
合：

a.ポンド記号(#)で終わるOSプロンプトが表示されたら、次のコマンドを入力します。

```
passwd admin
```

b.プロンプトが表示されたら、新しい管理者パスワードを入力します(2回)。

注：システムに「BAD PASSWORD」というメッセージが表示されます。これは情報としての意味しかありません。このメッセージが表示されたとしても、システムはユーザーが指定したパスワードを適用します。ただし、セキュリティ上の理由から、より複雑なパスワードを使用することを推奨します。

- ・ 7000および8000シリーズデバイスの新しいWebおよびCLI管理パスワードの場合：

シャープ記号(#)で終わるOSプロンプトで、次のコマンドを入力します。

```
usertool.pl -p 'admin password'
```

ここで、passwordは新しいadminパスワードです。

5.ログイン試行の失敗回数が多すぎるために管理者アカウントがロックされている場合は、アカウントのロックを解除する必要があります。使用しているデバイスに適した手順を使用します。

- ・ Firepower Management CenterまたはNGIPSvでCLIおよびシェルの管理者アカウントのロックを解除するには、OSプロンプトで次のコマンドを入力します。プロンプトの末尾にシャープ記号(#)が付きます：

```
pam_tally --user admin --reset
```

- ・ 7000および8000シリーズデバイスでWebとCLIの両方の管理者アカウントのロックを解除するには、OSプロンプトで次のコマンドを入力します。プロンプトの末尾にシャープ記号(#)が付いています。

```
usertool.pl -u admin
```

6.ポンド記号(#)で終わるOSプロンプトで、`reboot` コマンドを使用して、アップグレードを実行します。

7.再起動プロセスの完了を許可します。

オプション 2外部認証を使用してCLIにアクセスし、Firepower Management Centerのパスワードをリセットする

管理者アクセス権を持つアカウントでFMC Webインターフェイスにアクセスできる状況になっている場合は、`External Authentication` CLIにアクセスするための機能です。この方法を使用すると、FMCのCLIにログインし、Linuxシェルにアクセスし、`root`に昇格し、CLI/shell管理パスワードを手動でリセットできます。このオプションの場合、再起動は必要ありません。このオプションを使用するには、管理パスワードをリセットするFirepowerManagement Centerで外部認証 (SSHアクセス付き) が正しく設定されている必要があります。(手順については、ご使用のバージョンの『[Firepower Management Center Configuration Guide](#)』を参照してください)。これが設定されたら、次の手順を実行します。

1. SSHまたはコンソールを使用してCLI/shellアクセスを持つ外部認証されたアカウントを使用して、Firepower Management Centerにログインします。

- ・ FMCがバージョン6.2以下を実行している場合は、Linuxシェルに直接アクセスできます。
 - ・ FMCがバージョン6.3または6.4を実行していて、FMC CLIが有効になっていない場合は、Linuxシェルに直接アクセスできます。
 - ・ FMCがバージョン6.3または6.4を実行していて、Firepower Management Center CLIが有効になっている場合、Firepower Management Center CLIにアクセスできます。config コマンドを入力します `expert` コマンドを使用してLinuxシェルにアクセスします。
 - ・ FMCでバージョン6.5+が稼働している場合、Firepower Management CenterのCLIにアクセスできます。config コマンドを入力します `expert` コマンドを使用してLinuxシェルにアクセスします。
2. ドル記号(\$)が付いたシェルプロンプトで次のコマンドを入力して、管理者ユーザのCLIパスワードをリセットします。

```
sudo passwd admin
```

3. ユーティリティは `Password` プロンプトで、現在ログインしているユーザー名のパスワードを入力します。
4. パスワード入力を求めるプロンプトが表示されたら、新しい `admin` パスワードを入力します (2回)。



注：システムで「BAD PASSWORD」メッセージが表示される場合、このメッセージは情報としての意味しかありません。入力したパスワードは、このメッセージが表示されても適用されます。とはいえ、セキュリティ上の理由から、より複雑なパスワードを設定することを推奨します。

5. ログイン試行の失敗回数が多すぎるためにadminアカウントがロックアウトされた場合は、アカウントをロック解除し、`pam_tally` コマンドを入力し、プロンプトが表示されたらパスワードを入力します。

```
sudo pam_tally --user --reset
```

6. Type `exit` をクリックしてシェルを終了します。
7. CLIが有効になっているFirepower Management Centerで、次のように入力します `exit` CLIを終了します。

firepower Management Centerの失われたWebインターフェイス管理者パスワードのリセット

firepower Management Center Webインターフェイスへのアクセスに使用する管理者アカウントのパスワードを変更するには、次の手順を使用します。

手順：

1. SSHまたはコンソールでCLI管理アカウントを使用してアプライアンスにログインします。
2. Linuxシェルにアクセスします。
 - ・ FMCがバージョン6.2以下を実行している場合、ログインするとLinuxシェルに直接アクセスできます。
 - ・ FMCがバージョン6.3または6.4を実行していて、Firepower Management Center CLIが有効になっていない場合、ログインするとLinuxシェルに直接アクセスできます。
 - ・ FMCがバージョン6.3または6.4を実行しており、Firepower Management CenterのCLIが

有効になっている場合、ログインするとFirepower Management CenterのCLIにアクセスできます。config コマンドを入力します expert コマンドを使用してLinuxシェルにアクセスします。

・ FMCでバージョン6.5+が稼働している場合、ログインするとFirepower Management CenterのCLIにアクセスできます。config コマンドを入力します expert コマンドを使用してLinuxシェルにアクセスします。

3. シェルプロンプトで次のコマンドを入力して、Webインターフェイス管理者ユーザのパスワードをリセットします。

```
sudo usertool.pl -p 'admin password'
```

ここで、passwordはWebインターフェイス管理ユーザの新しいパスワードです。

4. ユーティリティは Password プロンプトで、現在ログインしているユーザー名のパスワードを入力します。
5. ログイン試行の失敗回数が多すぎるためにWeb管理者アカウントがロックアウトされた場合は、アカウントのロックを解除する必要があります。を実行します。 usertool コマンドを入力し、プロンプトが表示されたらCLI管理パスワードを入力します。

```
sudo usertool.pl -u admin
```

6. Type exit をクリックしてシェルを終了します。
7. CLIが有効になっているFirepower Management Centerで、次のように入力します exit CLIを終了します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。