Secure Firewall Management Center のコマンド ライン リファレンス

このリファレンスでは、Secure Firewall Management Center のコマンドライン インターフェイス（CLI）について説明します。

（注） Secure Firewall Threat Defense については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

Secure Firewall Management Center CLI について

SSH を使用して Management Center にログインすると、CLI にアクセスします。`expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。

注意 Cisco TAC または Firepower ユーザー マニュアルの明示的な手順による指示がない限り、Linux シェルにアクセスしないことを強くお勧めします。

⚠

注意 Linux シェルへのアクセス権があるユーザーはルート権限を取得できるため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、Linux シェル アクセスが付与されるユーザーのリストを適切に制限してください。
- 事前定義された `admin` ユーザーに加えて、Linux シェル ユーザーを確立しないでください。

この付録で説明されているコマンドを使用して Secure Firewall Management Center を表示してトラブルシューティングを行うとともに、限定された設定操作を実行できます。

Secure Firewall Management Center CLI モード

CLI には 4 つのモードが含まれています。デフォルト モードである CLI 管理には、CLI 自体の内部を移動するためのコマンドが含まれています。残りのモードには、Secure Firewall Management Center の機能の 3 つの異なる領域に対処するコマンドが含まれています。これらのモード内のコマンドは、モード名の`system`ム、`show`、または `configure` で始まります。

モードを入力すると、CLI は、現在のモードを反映するように変更を求められます。たとえば、システム コンポーネントのバージョン情報を表示するには、標準 CLI プロンプトに完全なコマンドを入力します。

```
> show version
```

これまでに `show` モードに入ったことがある場合は、show モードの CLI プロンプトで `show` キーワードを使用せずにコマンドを入力できます。

```
show> version
```

Secure Firewall Management Center CLI 管理コマンド

CLI 管理コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザーは現行の CLI セッションからログアウトします。

構文

```
exit
```

例

```
system> exit
>
```

expert

Linux シェルを起動します。

構文

```
expert
```

例

```
> expert
```

?（疑問符）

CLI コマンドと CLI パラメータの状況依存ヘルプを表示します。以下のように疑問符（?）コマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンド プロンプトで疑問符（?）を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符（?）に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックされないことに注意してください。

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

Secure Firewall Management Center CLI の show コマンド

Show コマンドは、アプライアンスの状態に関する情報を提供します。これらのコマンドはアプライアンスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。

version

製品のバージョンおよびビルドと、UUID などの情報を表示します。

構文

```
show version
```

例

```
> show version
-------------------[ fmc-austin ]-------------------
Model                     : Cisco Secure Firewall Management Center for VMware (66)
Version 7.6.0 (Build 1385)
UUID                      : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Rules update version      : 2024-05-13-001-vrt
LSP version               : lsp-rel-20240513-1955
VDB version               : 380
----------------------------------------------------
```

Secure Firewall Management Center CLI 設定コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。

password

現在の CLI ユーザーは自身のパスワードを変更できます。

⚠

注意 システム セキュリティ上の理由により、いかなるアプライアンスでも、事前定義された **admin** に加えて、Linux シェル ユーザーを確立しないことをお勧めします。

（注） `password` コマンドは、エクスポートモードではサポートされていません。Secure Firewall システムで管理ユーザーのパスワードをリセットするには、詳細をご覧ください。エキスパートモードで `password` コマンドを使用して管理者パスワードをリセットする場合は、`configure user admin password` コマンドを使用してパスワードを再設定することをお勧めします。パスワードを再設定したら、エキスパートモードに切り替え、管理者ユーザーのパスワードハッシュが /opt/cisco/config/db/sam.config ファイルおよび /etc/shadow ファイルで同じであることを確認します。

コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザーに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

構文

```
configure password
```

例

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Secure Firewall Management Center CLI システム コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

構文

```
system generate-troubleshoot option1 optionN
```

オプションが次の 1 つまたは複数の場合は、スペースで区切ります。

- `ALL`：次のすべてのオプションを実行します。
- `SNT`：Snort のパフォーマンスと設定
- `PER`: ハードウェアのパフォーマンスとログ

- SYS：システム設定、ポリシー、およびログ
- DES：検出設定、ポリシー、およびログ
- NET：インターフェイスとネットワーク関連データ
- VDB：検出、認知、VDB データ、およびログ
- UPG：データとログのアップグレード
- DBO：すべてのデータベース データ
- LOG：すべてのログ データ
- NMP：ネットワーク マップ情報

例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

expert コマンドを削除し、デバイス上の Linux シェルへアクセスします。

⚠

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

構文

```
system lockdown
```

例

```
> system lockdown
```

reboot

アプライアンスのリブート。

構文

```
system reboot
```

例

```
> system reboot
```

restart

アプライアンス アプリケーションを再起動します。

構文

```
system restart
```

例

```
> system restart
```

shutdown

アプライアンスをシャット ダウンします。

構文

```
system shutdown
```

例

```
> system shutdown
```

安全消去

ハードドライブデータを完全に消去します。

このコマンドを使用する前に、シリアルポートを使用して Management Center に接続する必要があります。このコマンドを実行すると、デバイスが再起動し、すべてのデータが完全に削除されます。プロセスが完了するまでに数時間かかることがあります。ドライブの容量が大きいほど、時間がかかります。安全な消去プロセス中の中断を防ぐために、電源を確保してください。消去が完了したら、新しいソフトウェアイメージをインストールできます。

⚠

注意 ハードドライブの消去処理では、アプライアンスのすべてのデータ（ISO イメージを含む）が失われます。

サポートされるデバイス

- Firepower Management Center 1600、2600、4600
- Firewall Management Center 1700、2700、4700

構文

```
secure-erase
```

例

```
> secure-erase
***************************** Caution *********************************

 If you run this command:
     - The management center hard drive data, including configurations
       and bootable images, will be permanently erased.
     - The device will reboot and reinitialize.

Note: Do not power off your device during this procedure.

***********************************************************************

Do you want to proceed? (Yes/No)
```

Secure Firewall Management Center CLI の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center を対象とした自動 CLI アクセス	6.5	任意（Any）	SSH を使用して Management Center にログインすると、CLI に自動的にアクセスします。CLI `expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。 （注） Management Center の CLI アクセスを有効または無効にするバージョン 6.3 の機能は廃止されます。このオプションが廃止された結果、仮想 Management Center は、**[システム（System）] > [設定（Configuration）] > [コンソールの設定（Console Configuration）]** ページを表示しなくなりました。このページは、物理 Management Center では引き続き表示されます。

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center の CLI アクセスを有効化および無効化する機能	6.3	任意（Any）	新しい/変更された画面： Management Center の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**システム**（⚙）> **[構成（Configuration）]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して Management Center にログインすると CLI にアクセスします。 • オフ：SSH を使用して Management Center にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 サポートされているプラットフォーム： Management Center
Management Center CLI	6.3	任意（Any）	導入された機能。 初期状態では、次のコマンドがサポートされています。 • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` サポートされているプラットフォーム： Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。