Firepower システムへのログイン

以下のトピックでは、Firepower システムにログインする方法を示します。

Firepower システム ユーザ アカウント

ユーザ名とパスワードを入力して、FMC または管理対象デバイスの Web インターフェイス、シェル、または CLI へのローカル アクセスを取得する必要があります。管理対象デバイスでは、Config レベルのアクセス権を持つ CLI ユーザは、`expert` コマンドを使用して Linux シェルにアクセスできます。FMC では、すべての CLI ユーザが `expert` コマンドを使用できます。FTD と FMC は、外部 LDAP や RADIUS サーバでユーザ クレデンシャルを保存する外部認証を使用するように設定できる場合があります。その場合、外部ユーザに対し、CLI またはシェルへのアクセスを禁止または許可することができます。

FMC CLI は、すべてのコマンドにアクセスできる単一の **admin** ユーザを提供します。FMC Web インターフェイスのユーザがアクセスできる機能は、管理者がユーザ アカウントに付与する権限によって制御されます。管理対象デバイスでは、ユーザがアクセスできる機能（CLI と Web インターフェイス用の）は、管理者がユーザ アカウントに付与する権限によって制御されます。

（注） システムはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることが保証されます。

注意 すべての FMC CLI ユーザ、および管理対象デバイスで Config レベルの CLI アクセス権を持つユーザは、Linux シェルの root 権限を取得できます。このため、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、CLI またはシェルへのアクセス権があるユーザのリストを適切に制限してください。
- 管理対象デバイスで CLI アクセス権限を付与する場合は、Config レベルの CLI アクセス権を付与された内部ユーザのリストを制限します。
- Linux シェルユーザは確立しないでください。事前定義された **admin** ユーザおよび CLI 内で **admin** ユーザが作成したユーザのみを使用します。

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

アプライアンスが異なれば、サポートするユーザアカウントのタイプは異なり、搭載される機能もさまざまです。

Firepower Management Centerについて

Firepower Management Center では、次のユーザ アカウント タイプをサポートします。

- Web インターフェイス アクセス用に事前定義された **admin** アカウント。このアカウントは管理者ロールを保有し、Web インターフェイスから管理できます。
- カスタム ユーザ アカウント。このアカウントは Web インターフェイスへのアクセスが可能で、**admin** ユーザおよび管理者権限を持つユーザが作成および管理できます。
- CLI またはシェルへのアクセス権に事前に定義されている **admin** アカウント。このアカウントはルート権限を取得できます。デフォルトでは、デバイスにログインすると、この **admin** アカウントはシェルにダイレクトアクセスできるようになります。ただし、Firepower Management Center CLI が有効になっている場合、このアカウントでログインするユーザは `expert` コマンドを使用してシェルにアクセスする必要があります。

注意 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザを確立しないことを強く推奨します。

7000 & 8000 シリーズ デバイス

7000 & 8000 シリーズ デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび管理者ロールのユーザが作成、管理できます。

7000 & 8000 シリーズは、ユーザの外部認証をサポートしています。

NGIPSv デバイス

NGIPSv デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

NGIPSv は、ユーザの外部認証をサポートしていません。

Firepower Threat Defense および Firepower Threat Defense Virtual デバイス

Firepower Threat Defense および Firepower Threat Defense Virtual デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前に定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

Firepower Threat Defense は、SSH ユーザの外部認証をサポートしています。

ASA FirePOWER デバイス

ASA FirePOWER モジュールでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

ASA FirePOWER モジュールは、ユーザの外部認証をサポートしていません。ASA CLI および ASDM を介した ASA デバイスへのアクセスについては、『*Cisco ASA Series General Operations CLI Configuration Guide*』および『*Cisco ASA Series General Operations ASDM Configuration Guide*』に記載されています。

Firepower システム ユーザ インターフェイス

アプライアンスのタイプに応じて、Web ベースの GUI、補助的な CLI、または Linux シェルを使用して Firepower アプライアンスを操作できます。Firepower Management Center 展開では、ほとんどの設定タスクを FMC の GUI から実行します。CLI または Linux シェルを使用してアプライアンスに直接アクセスすることが必要なタスクは、ごく一部のタスクのみです。Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

ブラウザの要件については、『Firepower Release Notes』を参照してください。

（注） いずれのアプライアンスでも、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続が終了します。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
Firepower Management Center	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • アドミニストレーティブ タスク、管理タスク、分析タスクに使用することができます。	• 事前定義された **admin** ユーザとカスタム外部ユーザ アカウントでサポートされます。 • 有効な場合にのみアクセスできます。Firepower Management Center CLI の有効化を参照してください。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。	• 事前定義された **admin** ユーザとカスタム外部ユーザ アカウントでサポートされます。 • サポート対象ユーザのアクセスのデフォルト形式ですが、Firepower Management Center CLI が有効な場合は `expert` コマンド経由でアクセスする必要があります。Firepower Management Center CLI の有効化を参照してください。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
7000 & 8000 シリーズ デバイス	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • 初期設定、基本的な分析、および設定タスクにのみ使用することができます。	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。
Firepower Threat Defense Firepower Threat Defense Virtual	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH、シリアル、またはキーボードとモニタ接続を使用してアクセスできます。仮想デバイスでは、SSH または VM コンソール経由でアクセスできます。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
NGIPSv	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続または VM コンソールを使用してアクセスできます。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。
ASA FirePOWERモジュール	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH 接続を使用してアクセスできます。また、ASA 5585-X デバイス（ハードウェア モジュール）の場合はキーボードおよびモニタ接続を使用して、その他の ASA 5500-X シリーズ デバイス（ソフトウェア モジュール）の場合はコンソール ポートを使用してアクセスできます。 • 設定タスクおよび管理タスクに使用することができます。	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

関連トピック

社内ユーザ アカウントの追加

Web インターフェイスの考慮事項

- 組織が認証に共通アクセスカード（CAC）を使用している場合は、LDAP で認証されている外部ユーザは CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることができます。
- Web セッション時にアプライアンスのホーム ページに初めてアクセスした際に、そのアプライアンスに対する最後のログインセッションに関する情報を表示できます。最後のログインについて、次の情報を表示できます。
  - ログインの年、月、日、曜日
  - ログイン時のアプライアンスのローカル時間（24 時間表記）
  - アプライアンスにアクセスするために最後に使用されたホストとドメイン名
- デフォルトのホーム ページの上部に表示されるメニューおよびメニュー オプションは、ユーザアカウントの権限に基づきます。ただし、デフォルトホームページのリンクには、ユーザアカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。
- プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまでスクリプトの続行を許可してください。

関連トピック

ホームページの指定

セッション タイムアウト

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くと、Firepower システムが自動的にセッションからユーザをログアウトします。

管理者ロールを割り当てられたユーザは、以下の設定を使用して、アプライアンスのセッション タイムアウト間隔を変更できます。

アプライアンス	設定
Firepower Management Center	**[システム（System）] > [設定（Configuration）] > [シェル タイムアウト（Shell Timeout）]**
7000 & 8000 シリーズ デバイス	**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [シェル タイムアウト（Shell Timeout）]**

関連トピック

セッション タイムアウトの設定

Firepower Management Center Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

複数の FMC が同じ IP アドレスを共有する NAT 環境の場合

- 各 FMC が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる FMC にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレットモードまたはプライベートモードに設定します。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加の説明に従って、ユーザ アカウントを作成します。

ステップ 1 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している FMC に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザ アカウントが作成されたドメインをユーザ名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザ アカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。

  ```
  SubdomainB\username
  ```

- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の

場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッション タイムアウト （7 ページ）

7000 または 8000 シリーズ デバイスの Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよびWeb インターフェイスでの内部ユーザの追加の説明に従って、初期設定プロセスを完了し、ユーザアカウントを作成します。

ステップ 1 ブラウザで https://*hostname*/ にアクセスします。ここで、*hostname* はアクセスする管理対象デバイスのホスト名に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が 1111 で、SecurID トークンが 222222 の場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッション タイムアウト （7 ページ）

CAC クレデンシャルを使用した Firepower Management Center へのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

複数の FMC が同じ IP アドレスを共有する NAT 環境の場合

- 各 FMC が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる FMC にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレット モードまたはプライベート モードに設定します。

⚠

注意 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加の説明に従ってユーザ アカウントを作成します。
- LDAP を使用した共通アクセス カード認証の設定の説明に従って、CAC の認証と認可を設定します。

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している FMC に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

LDAP を使用した共通アクセス カード認証の設定
セッション タイムアウト （7 ページ）

CAC クレデンシャルを使用した 7000 または 8000 シリーズ デバイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	任意

ユーザは単一のアクティブなセッションに制限されます。

注意 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加の説明に従って、ユーザ アカウントを作成します。
- LDAP を使用した共通アクセス カード認証の設定の説明に従って、CAC の認証と認可を設定します。

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアクセスするアプライアンスのホスト名に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。
ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。
ステップ 5 [続行（Continue）] をクリックします。

関連トピック

LDAP を使用した共通アクセス カード認証の設定
セッション タイムアウト （7 ページ）

FMC コマンドライン インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

管理CLI ユーザと特定のカスタム外部ユーザは、FMC CLI/シェルにログインできます。

注意 Cisco TAC または FMC マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

admin ユーザとして初期設定プロセスを完了します。を参照してください。最初のログイン

ステップ 1 **admin** ユーザ名とパスワードを使用して、SSH またはコンソールポート経由で FMC に接続します。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。ログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 2 CLI アクセスが有効になっている場合は、利用可能な CLI コマンドのいずれかをします。

7000/8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスの CLI へのログイン

基本的な CLI 設定へのアクセスを最低限保有していれば、従来の管理対象デバイスに直接ログインできます。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- 最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。
- **configure user add** コマンドを使用して、CLI にログインできる追加のユーザ アカウントを作成します。
- 7000 & 8000 シリーズ デバイスでは、Web インターフェイスでの内部ユーザの追加の説明に従って、Web インターフェイスでユーザ アカウントを作成します。

ステップ 1 デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用します。

専用の ASA FirePOWER コンソールポートをもつ ASA 5585-X デバイスを除いて、コンソールを介してアクセスされる ASA FirePOWER デバイスは、デフォルトのオペレーティングシステム CLI に設定されます。これには、Firepower CLI にアクセスするための追加の手順（**session sfr**）が必要です。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。ログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 2 CLI プロンプトで、コマンド ライン アクセスのレベルで許可されている任意のコマンドを使用します。

FTD デバイスのコマンドライン インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	FTD	該当なし	CLI の基本設定

FTD 管理対象デバイスのコマンドライン インターフェイスに直接ログインできます。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。**configure user add** コマンドを使用して、CLI にログインできる追加のユーザ アカウントを作成します。

ステップ 1 コンソール ポートまたは SSH を使用して、FTD CLI に接続します。

FTD デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。特定のデータ インターフェイスへの SSH 接続を許可する方法については、セキュア シェルの設定を参照してください。

デバイスのコンソール ポートに直接接続できます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

コンソール ポートでアクセスする最初の CLI は、デバイス タイプによって異なります。

- ASA シリーズ デバイス：コンソール ポートの CLI は通常の FTD CLI です。
- Firepower シリーズ デバイス：コンソール ポートの CLI は FXOS です。**connect ftd** コマンドを使用して FTD CLI にアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには FTD CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 2 **admin** のユーザ名とパスワードでログインします。

ステップ 3 CLI プロンプト（>）で、コマンド ライン アクセス レベルで許可されている任意のコマンドを使用します。

ステップ 4 （オプション）診断 CLI にアクセスします。

system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の **show** コマンドや、ASA 5506W-X ワイヤレス アクセス ポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。

この CLI には 2 つのサブモード、ユーザ EXEC モードと特権 EXEC モードがあります。特権 EXEC モードではより多くのコマンドが利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a**、**d** を入力します。

Firepower システム Web インターフェイスからのログアウト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	任意	任意	任意

Firepower システムの Web インターフェイスをアクティブに使用しなくなった場合、シスコでは、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトすることで Web セッションを終了し、別のユーザが自分の資格情報を使用してインターフェイスを使用できないようにします。

ユーザ名の下にあるドロップダウンリストから、[Logout] を選択します。

関連トピック

セッション タイムアウト （7 ページ）

Firepower システムへのログイン履歴

機能	バージョン	詳細
SSH ログイン失敗の制限数	6.3	ユーザが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。

機能	バージョン	詳細
のCLIアクセスを有効化および無効化する機能 FMC	6.3	新しい/変更された画面： FMC 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：**[System]** > **[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 FMC 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 FMC 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。 サポートされるプラットフォーム FMC