Management Center 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。

ユーザーアカウント

ユーザー名とパスワードを入力して、Firewall Management Center または管理対象デバイスの Web インターフェイスまたは 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 ユーザーは、`expert` コマンドを使用して Linux シェルにアクセスできます。Firewall Management Center では、すべての CLI ユーザーが `expert` コマンドを使用できます。Firewall Threat Defense と Firewall Management Center は、外部 LDAP や RADIUS サーバーでユーザーログイン情報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、外部ユーザーに対し、CLI へのアクセスを禁止または許可することができます。Firewall Management Center は、認証および承認のために、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する任意の SSO プロバイダーを使用したシングルサインオン（SSO）をサポートするように設定できます。

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

（注） システムはユーザーアカウントに基づいてユーザーアクティビティを監査します。ユーザーが正しいアカウントでシステムにログインすることを確認してください。

注意 すべての Firewall Management Center CLI ユーザー、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ーは、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 へのアクセス権があるユーザー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 シェルユーザーは確立しないでください。事前定義された **admin** ユーザーおよび CLI 内で **admin** ユーザーが作成したユーザーのみを使用します。

注意 Cisco TAC または Cisco Secure Firewall の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ー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。

Secure Firewall Management Centerについて

Secure Firewall Management Center では、次のユーザー 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 ユーザー 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** ユーザーおよび管理者権限を持つユーザーが作成および管理できます。
- CLI アクセスのために事前定義された **admin** アカウント。このアカウントでログインするユーザーは、`expert` コマンドを使用して Linux シェルにアクセスできます。

  CLI の **admin** アカウントと Web インターフェイスの **admin** アカウントのパスワードは初期設定時に同期されますが、それ以降、必要に応じて 2 つの **admin** アカウントに個別のパスワードを設定することができます。

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 ユーザーを確立しないことを強く推奨します。

Secure Firewall Threat Defense および Secure Firewall Threat Defense Virtual デバイス

Secure Firewall Threat Defense および Secure Firewall Threat Defense Virtual デバイスでは、次のユーザー 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 ユーザー アカウント。このアカウントは、**admin** ユーザーおよび Config アクセス権をもつユーザーが作成、管理できます。

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

システム ユーザー 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 シェルを使用してアプライアンスを操作できます。Secure Firewall Management Center 展開では、ほとんどの設定タスクを Firewall Management Center 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、『Cisco Secure Firewall Release Notes』を参照してください。

（注） すべてのアプライアンスでは、SSH を介した CLI 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。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
Secure Firewall Management Center	• 事前定義された **admin** ユーザーとカスタム ユーザー 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** ユーザーとカスタム外部ユーザー 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ー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** ユーザーでサポートされます。 • Secure Firewall Management Center CLI から `expert` コマンドを使用してアクセスする必要があります。 • SSH 接続、シリアル接続、またはキーボードおよびモニター接続を使用してアクセス可能です。 • Cisco TAC または Firewall Management Center 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。
Secure Firewall Threat Defense Secure Firewall Threat Defense Virtual	—	• 事前定義された **admin** ユーザーとカスタム ユーザー 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ー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** ユーザーとカスタム ユーザー アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザーが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または Firewall Management Center 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

内部ユーザーの追加または編集

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ーは 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。
- 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、システムが自動的にセッションからユーザーをログアウトします。

（注） SSO ユーザーの場合、Firewall Management Center セッションがタイムアウトすると、表示は IdP インターフェイスに一時的にリダイレクトされ、次に Firewall Management Center ログインページにリダイレクトされます。SSO セッションが他の場所から終了していない限り、ログインページの [シングルサインオン（Single Sign-On）] リンクをクリックするだけで、ログイン資格情報を提供しなくても、誰でも Firewall Management Center にアクセスできます。Firewall Management Center のセキュリティを確保し、他の人が SSO アカウントを使用して Firewall Management Center にアクセスするのを防ぐために、Firewall Management Center ログインセッションを無人のままにせず、Firewall Management Center からログアウトするときに IdP で SSO フェデレーションからログアウトすることをお勧めします。

管理者ロールを割り当てられたユーザーは、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。

[システム（System）] > [設定（Configuration）] > [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
SAML シングルサインオンの設定

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

（注） このタスクは、LDAP または RADIUS サーバーによって認証された内部ユーザーと外部ユーザーに適用されます。SSO ログインについては、SSO を使用した Firewall Management Center Web インターフェイスへのログイン （7 ページ）を参照してください。

ユーザー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ー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、または別のユーザーとしてログインするように求められます。

複数の Firewall Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Firewall Management Center 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 Firewall Management Center 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ーとしてログインし、アカウントの特権を変更します。
- 「内部ユーザーの追加または編集」の説明に従って、ユーザ アカウントを作成します。

手順

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 Firewall Management Center に対応します。

ステップ 2 [ユーザー名（Username）] および [パスワード（Password）] フィールドに、ユーザー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。

- ユーザー名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザーアカウントが作成されたサブドメインをユーザー名の前に付加します。グローバル ドメインを指定する必要はありません。たとえばユーザー アカウントを SubdomainA で作成した場合、次の形式でユーザー名を入力します。

```
SubdomainA\username
```

親ドメインが SubdomainA である SubdomainB にユーザーが追加された場合は、次の形式でユーザー名を入力します。

```
SubdomainA\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。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 （5 ページ）

SSO を使用した Firewall Management Center Web インターフェイスへのログイン

Firewall Management Center は、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する SSO プロバイダーで導入された、シングルサインオン（SSO）フェデレーションに参加するように設定できます。アイデンティティ プロバイダー（IdP）で SSO ユーザーアカウントを確立し、アカウント名に電子メールアドレスを使用する必要があります。ユーザー名が電子メールアドレスでない場合、または SSO ログインに失敗する場合は、システム管理者にお問い合わせください。

（注） Firewall Management Center は、SSO アカウントの CAC クレデンシャルを使用したログインをサポートしていません。

ユーザー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ー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、または別のユーザーとしてログインするように求められます。

複数の Firewall Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Firewall Management Center 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 Firewall Management Center 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

- Firewall Management Center を SSO アクセス用に設定します。SAML シングルサインオンの設定を参照してください。
- Web インターフェイスにアクセスできない場合は、システム管理者に問い合わせて、SSO IdP でアカウントを設定してください。

手順

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 Firewall Management Center に対応します。

（注）
SSO ユーザーは、常に SSO アクセス用に特別に設定されたログイン URL を使用して、Firewall Management Center にアクセスする必要があります。この情報については、管理者にお問い合わせください。

ステップ 2 [シングルサインオン（Single Sign-On）] リンクをクリックします。

ステップ 3 システムは、次の 2 つの方法のいずれかで応答します。

- SSO フェデレーションにすでにログインしている場合は、Firewall Management Center のデフォルトのホームページが表示されます。
- SSO フェデレーションにまだログインしていない場合は、Firewall Management Center によりブラウザが IdP のログインページにリダイレクトされます。IdP でログインプロセスを完了すると、Firewall Management Center のデフォルトのホームページが表示されます。

関連トピック

セッション タイムアウト （5 ページ）
SAML シングルサインオンの設定

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

ユーザー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ー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、または別のユーザーとしてログインするように求められます。

複数の Firewall Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Firewall Management Center 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 Firewall Management Center 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ーとしてログインし、アカウントの特権を変更します。
- 「内部ユーザーの追加または編集」の説明に従ってユーザー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。

手順

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 Firewall Management Center 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 [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 （5 ページ）
Firewall Management Center の SSO ガイドライン

Firewall Management Center コマンドライン インターフェイスへのログイン

admin CLI ユーザーと特定のカスタム外部ユーザーは、Firewall Management Center CLI にログインできます。

注意 Cisco TAC または Firewall Management Center 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 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 ユーザーとして初期設定プロセスを完了します。「最初のログイン」を参照してください。

手順

ステップ 1 **admin** ユーザー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 Firewall Management Center 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 利用可能な CLI コマンドのいずれかを使用します。

最後のログインの表示

権限のないユーザがクレデンシャルを使用して Secure Firewall Management Center にサインインしていることが疑われる場合は、クレデンシャルが最後にログインに使用された日付、時刻、および IP アドレスを確認できます。

手順

ステップ 1 Secure Firewall Management Center にサインインします。

ステップ 2 ブラウザ ウィンドウの右上隅で、サインインに使用したユーザー ID を探します。

ステップ 3 ユーザー名をクリックします。

ステップ 4 前回のログインに関する情報が、表示されるメニューの下部に表示されます。

Firepower システム Web インターフェイスからのログアウト

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、別のユーザー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。

（注） Firewall Management Center で SSO セッションからログアウトしている場合は、ログアウトするときにブラウザで組織の SSO IdP にリダイレクトされます。Firewall Management Center のセキュリティを確保し、他の人が SSO アカウントを使用して Firewall Management Center にアクセスするのを防ぐために、IdP で SSO フェデレーションからログアウトすることをお勧めします。

手順

ステップ 1 ユーザー名の下にあるドロップダウンリストから、[ログアウト（Logout）] を選択します。

ステップ 2 Firewall Management Center で SSO セッションからログアウトしている場合は、組織の SSO IdP にリダイレクトされます。Firewall Management Center のセキュリティを確保するために、IdP でログアウトします。

関連トピック

セッション タイムアウト （5 ページ）

Management Center へのログイン履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオン（SSO）のサポートが追加されました。	6.7	いずれか	サードパーティの SAML 2.0 準拠アイデンティティ プロバイダー（IdP）で設定されたユーザーがログインページの新しい [シングルサインオン（Single Sign-On）] リンクを使用して Firewall Management Center にログインする機能が追加されました。 新規/変更された画面： ログイン画面

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Secure Firewall Management Center に最後にサインインした時刻に関する情報を表示します。	6.5	任意（Any）	最後にログインした日付、時刻、および IP アドレスを表示します。 新規/変更されたメニュー： ウィンドウの右上の、ログインに使用したユーザー名を表示するメニュー。 サポートされているプラットフォーム： Firewall Management Center
次を対象とした自動 CLI アクセス Firewall Management Center	6.5	任意（Any）	SSH を使用して Firewall 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） Firewall 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 Firewall 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 Firewall Management Center では引き続き表示されます。
SSH ログイン失敗の制限数	6.3	任意（Any）	ユーザーが 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。
Firewall 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： Firewall 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（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）]** ページの **[CLIアクセスの有効化（Enable CLI Access）]**。 • オン： SSH を使用して Firewall 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 Firewall 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： Firewall 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。