



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 システムのユーザ アカウント](#) (1 ページ)
- [Firepower システムのユーザ インターフェイス](#) (3 ページ)
- [Web インターフェイスによる Firepower Management Center へのログイン](#) (8 ページ)
- [Web インターフェイスによる管理対象デバイスへのログイン](#) (10 ページ)
- [CAC クレデンシヤルを使用した Firepower Management Center へのログイン](#) (11 ページ)
- [CAC クレデンシヤルを使用した管理対象デバイスへのログイン](#) (12 ページ)
- [従来型デバイスでのコマンドライン インターフェイスへのログイン](#) (13 ページ)
- [Firepower Threat Defense 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](#) (14 ページ)
- [Web インターフェイスでの基本システム情報の表示](#) (15 ページ)
- [Firepower Management Center のドメインの切り替え](#) (16 ページ)
- [Firepower システム Web インターフェイスからのログアウト](#) (16 ページ)
- [コンテキスト メニュー](#) (17 ページ)

Firepower システムのユーザ アカウント

ユーザ名とパスワードを入力して、アプライアンスの 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。ユーザがログイン時にアクセスできる機能は、ユーザアカウントに許可されている権限によって制御されます。一部のアプライアンスは、外部 LDAP や RADIUS サーバでユーザ クレデンシヤ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。



(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 すべてのアプライアンスで、（外部認証または CLI expert コマンドで取得した）シェルアクセスを持つユーザには、シェルでの `sudoers` 権限がありますが、これはセキュリティリスクを示す場合があります。外部認証を確立する場合は、シェルアクセスが付与されるユーザのリストを適切に制限してください。同様に、CLI アクセス権限を付与する場合は、構成レベルのアクセス権を持つユーザのリストを制限してください。



注意 Cisco TAC の指示に従って操作する場合を除き、シェルや CLI expert モードを使用して Firepower アプライアンスにアクセスしないよう強くお勧めします。

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

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。
- シェルアクセス用に事前適宜された `admin` アカウント。このアカウントには `sudoers` 権限があります。
- 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。



注意 システムセキュリティ上の理由から、シスコは、追加のシェルユーザを Firepower Management Center で確立しないようにすることを推奨します。そのようなリスクを受け入れる場合は、外部認証を使用して、ユーザに Firepower Management Center へのシェルアクセス権を付与できます。

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。

Firepower システムは、7000 & 8000 シリーズ デバイスにログインしているユーザの外部認証は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 タイプがサポートされます。Firepower システムでは、NGIPSv デバイスにログインするユーザ用の外部認証がサポートされません。

- 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 Configuration アクセス権をもつユーザが作成、管理できます。

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。

Firepower システムは、Firepower Threat Defense デバイスにログインしているユーザの外部認証はサポートしていません。

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 Configuration アクセス権をもつユーザが作成、管理できます。

Firepower システムは、ASA FirePOWER デバイスにログインしているユーザの外部認証は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 システムのユーザインターフェイス

Firepower システムでは、グラフィカル ユーザインターフェイス、補助的なコマンドラインインターフェイス (CLI)、Linux シェルのいずれかを使用してアプライアンスにログインできます。(Web インターフェイスのブラウザ要件の詳細については、Firepower システムの該当バージョンのリリース ノートを参照してください)。



- (注) Firepower Management Center を使用して複数のデバイスを管理し、それらのデバイスからのデータを関連付けます。単一のデバイスを直接管理するのが適切な場合には、Firepower Device Manager を使用して一部の Firepower Threat Defense デバイスでポリシーやデバイス設定を管理し、Adaptive Security Device Manager (ASDM) を使用して ASA FirePOWER サービス デバイスで同じ機能を管理できます。アプライアンスの管理ツールを選択した後に、別の管理ツールに切り替えると、最新の設定は失われます。7000 & 8000 シリーズデバイスのローカル Web インターフェイスでは、限定的なシステム設定の機能を提供しますが、その機能を使用してポリシーを管理することはできません。それらのデバイスは Firepower Management Center を使用して管理する必要があります。

使用可能なローカル アクセス タイプはアプライアンスのタイプによって異なります。

表 1: アプライアンス別のローカル アクセス

アプライアンス	グラフィカル ユーザ インターフェイス	CLI アクセス	Linux シェルへのアクセス
Firepower Management Center	<ul style="list-style-type: none"> • Firepower Web インターフェイス • 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 • 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 	none	<ul style="list-style-type: none"> • 事前定義された admin ユーザでサポートされます • シリアルまたは キーボードを使用してアクセス可能であり、接続をモニタできます • 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

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
7000 & 8000 シリーズ デバイス	<ul style="list-style-type: none"> • Firepower Web インターフェイス • 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使用することができます 	<ul style="list-style-type: none"> • 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 • 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 	<ul style="list-style-type: none"> • 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 • Configuration 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 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
NGIPSv デバイス	none	<ul style="list-style-type: none"> • 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 • 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 	<ul style="list-style-type: none"> • 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 • Configuration 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 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

アプライアンス	グラフィカル ユーザ インターフェイス	CLI アクセス	Linux シェルへのアクセス
Firepower Threat Defense および Firepower Threat Defense Virtual デバイス	<ul style="list-style-type: none"> • Firepower Device Manager、次で動作する Firepower Threat Defense でサポートされます。 <ul style="list-style-type: none"> • ASA 5506-X • ASA 5506H-X • ASA 5506W-X • ASA 5508-X • ASA 5516-X • ASA 5512-X • ASA 5515-X • ASA 5525-X • ASA 5545-X • ASA 5555-X • 事前定義された <code>admin</code> ユーザでサポートされます • 初期設定、設定、およびシステム モニタリング に使用することができます 	<ul style="list-style-type: none"> • 事前定義された <code>admin</code> 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 • 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 	<ul style="list-style-type: none"> • 事前定義された <code>admin</code> 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 • Configuration アクセス権を持つ CLI ユーザが <code>expert</code> コマンドを使用してアクセスできます • 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

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
ASA FirePOWER サービス デバイス	<ul style="list-style-type: none"> Adaptive Security Device Manager (ASDM) 初回アクセスやカスタム 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使用することができます 	<ul style="list-style-type: none"> 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 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 	none



(注) ASDM を使用した ASA FirePOWER モジュールの管理の詳細については、『*Cisco ASA Series General Operations Configuration Guide*』参照してください。

Web インターフェイスに関する考慮事項

- 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、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。
 - ログインの曜日、月、日、年
 - 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](#)

セッションのタイムアウト (Session Timeout)

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](#)

WebインターフェイスによるFirepowerManagementCenter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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

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、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。
- [Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000](#)または[Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500](#)、および[ユーザアカウントの作成](#)の説明に従って、初期セットアップ手順を完了し、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://hostname/` にアクセスします。ここで、`hostname` は Firepower Management Center 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。
- 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

[セッションのタイムアウト \(Session Timeout\)](#) (8 ページ)

Web インターフェイスによる管理対象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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シリーズ	該当なし	任意 (Any)

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、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 [ユーザ アカウントの作成](#) の説明に従って、初期セットアップ手順を完了し、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://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、111122222 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

[セッションのタイムアウト \(Session Timeout\)](#) (8 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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

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。
- [Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000](#) または [Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500](#)、および [ユーザアカウントの作成](#) の説明に従って、初期セットアップ手順を完了し、ユーザアカウントを作成します。
- [CAC 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://hostname/` にアクセスします。ここで、`hostname` は Firepower Management Center 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

[CAC 認証](#)

[セッションのタイムアウト \(Session Timeout\)](#) (8 ページ)

CAC クレデンシヤルを使用した管理対象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	サポートされるド メイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シ リーズ	該当なし	任意 (Any)

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。
- デバイスに該当する Firepower クイック スタート ガイドおよび [ユーザ アカウントの作成](#) の説明に従って、初期セットアップ手順を完了し、ユーザ アカウントを作成します。
- [CAC 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://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

[CAC 認証](#)

[セッションのタイムアウト \(Session Timeout\)](#) (8 ページ)

従来型デバイスで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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	従来型 (Classic)	該当なし	CLI の基本設定

従来型管理対象デバイス（7000 & 8000 シリーズ、NGIPSv、および ASA FirePOWER）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。

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。

- 7000 & 8000 シリーズ デバイスで、[ユーザアカウントの作成](#)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。
- すべてのデバイスで、CLIにログインできる追加のユーザアカウントを **configure user add** コマンドを使用して作成します。

手順

ステップ 1 SSHを使用して、管理インターフェイスのホスト名またはIPアドレスに接続します。または、コンソールポートに接続することもできます。

ステップ 2 「log in as:」 コマンドプロンプトに対してユーザ名を入力し、Enter を押します。

ステップ 3 「Password:」 プロンプトに対してパスワードを入力し、Enter を押します。

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。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 4 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。

Firepower Threat Defense 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	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	該当なし	CLI の基本設定

Firepower Threat Defense 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。

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。

手順

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

Firepower Threat Defense 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 Firepower Threat Defense 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。Firepower Threat Defense CLI には、**connect ftd** コマンドを使用してアクセスできます。FXOS CLI はシャレ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 Firepower Threat Defense 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 管理者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。

Web インターフェイスでの基本システム情報の表示

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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

[バージョン情報 (About)] ページには、Firepower システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

手順

ステップ1 ページ上部のツールバーから [ヘルプ (Help)] をクリックします。

ステップ2 [バージョン情報 (About)] を選択します。

Firepower Management Center のドメインの切り替え

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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

マルチドメイン導入環境では、ユーザロール権限によって、ユーザがアクセスできるドメインと、そのドメイン内でのユーザの権限が決まります。単一のユーザアカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバルドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイスセッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザロールに応じて定められたメニューオプション。

手順

アクセスするドメインは、ユーザ名の下にあるドロップダウンリストから選択します。

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	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

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。

手順

ユーザ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。

関連トピック

[セッションのタイムアウト \(Session Timeout\)](#) (8 ページ)

コンテキストメニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキストメニューを表示できます。コンテキストメニューは、Firepower システム内の他の機能にアクセスするためのショートカットとして使用できます。コンテキストメニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IPアドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホストプロファイル情報を含む）が表示されます。
- SHA-256 ハッシュ値のホットスポットでは、ファイルの SHA-256 ハッシュ値をクリーンリストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。

Firepower システム コンテキストメニューをサポートしていないページや場所では、ブラウザの通常のコンテキストメニューが表示されます。

ポリシー エディタ

多くのポリシーエディタには、各ルールのホットスポットが含まれています。新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、ルールの編集などを行うことができます。

侵入ルール エディタ

侵入ルールエディタには、各侵入ルールのホットスポットが含まれています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。

イベント ビューア

イベント ページ（ドリルダウン ページとテーブル ビュー）には、各イベント、IP アドレス、URL、DNS クエリ、特定のファイルの SHA-256 ハッシュ値のホットスポットが含ま

れています。ほとんどのイベント タイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベント ビューですべて表示できない場合、テキスト全体を表示する。

接続イベントの表示中は、デフォルトのセキュリティインテリジェンスのホワイトリストとブラックリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。
- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。
- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルールエディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止オプションを設定する。
- ルールのドキュメンテーションを表示する。

侵入イベントの packets ビュー

侵入イベントの packets ビューには、IP アドレスのホットスポットが含まれています。packets ビューでは、左クリックによるコンテキスト メニューを使用します。

ダッシュボード

多くのダッシュボードウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれています。ダッシュボードウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブルビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールを表示できます。

Context Explorer でも左クリックのコンテキストメニューを使用します。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。

関連トピック

[セキュリティインテリジェンスのリストとフィード](#)

