Firepower システム ユーザ管理

次のトピックでは、管理アクセス権を持つユーザが Firepower システム内のユーザ アカウントを管理する方法について説明します。

ユーザの役割

Firepowerシステムでは、ユーザのロールに基づいてユーザ特権を割り当てることができます。たとえば、アナリストに対して Security Analyst や Discovery Admin などの事前定義ロールを付与し、Firepower システムを管理するセキュリティ管理者に対して Administrator ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成することもできます。

管理対象デバイスのプラットフォーム設定ポリシーでは、そのデバイスからの外部で認証されたすべてのユーザのデフォルト アクセス ロールを設定します。外部認証ユーザの初回ログイン後に、[ユーザ管理（User Management）] ページでそのユーザのアクセス権を追加または削除できます。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。内部認証ユーザは手動で作成されるため、内部認証ユーザの作成時にアクセス権を設定します。

LDAP グループを使用したアクセス権の管理を設定した場合、ユーザのアクセス権はLDAP グループのそのメンバーシップに基づきます。属しているグループの中で最も高いレベルのアクセスを持つグループのデフォルトアクセス権が付与されます。ユーザがどのグループにも属していない場合にグループアクセスを設定していた場合、ユーザには、LDAPサーバの認証オブジェクトで設定されているデフォルト ユーザ アクセス権が付与されます。グループ アクセスを設定すると、それらの設定によってプラットフォーム設定ポリシーのデフォルトアクセス設定がオーバーライドされます。

同様に、RADIUS 認証オブジェクトの特定のユーザ ロール リストにユーザを割り当てると、1 つ以上のロールが相互に矛盾しない限り、割り当てられたすべてのロールがそのユーザに付与されます。2 つの相互に矛盾するロールのリストにユーザが含まれている場合、最も高いレベルのアクセスを持つロールが付与されます。ユーザがどのリストにも属しておらず、認証オブジェクトでデフォルト アクセス ロールを設定している場合、そのユーザにはそのデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセスを設定すると、それらの設定によってプラットフォーム設定ポリシーのデフォルトアクセス設定がオーバーライドされます。

マルチドメイン展開では、複数のドメインでユーザ ロールを割り当てることができます。たとえば、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、サブドメインでは管理者権限を割り当てることができます。

定義済みのユーザ ロール

Firepower System では、組織のニーズを満たすために、アクセス権限セットの範囲を提供する 10 の定義済みのユーザ ロールを含みます。7000 および 8000 シリーズ デバイスは、10 の定義済みユーザ ロールのうちの 3 つ（管理者、メンテナンス ユーザ、セキュリティ アナリスト）のみにアクセスする点にご注意ください。

定義済みユーザ ロールは編集できませんが、カスタム ユーザ ロールの基準として、アクセス特権セットを使用できます。また、別のユーザ ロールに対して段階的に増やすように設定できません。

次の表では、利用可能な定義済みのロールを簡単に説明します。

アクセス管理者（Access Admin）

[ポリシー（Policies）] メニューでアクセス制御ポリシー機能や関連する機能へのアクセスが可能です。アクセス管理者は、ポリシーを展開できません。

管理者（Administrator）

解析およびレポート機能、ルールおよびポリシー コンフィギュレーション機能、システム管理機能、すべてのメンテナンス機能へのアクセスが可能です。管理者は、ポリシーを含むデバイスへの設定変更も展開できます。管理者は、すべてのメニュー オプションにアクセスします。侵害された場合には、これらのセッションには高いセキュリティ リスクが存在するため、ログイン セッションがタイムアウトする可能性があります。

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

検出管理者（Discovery Admin）

[ポリシー（Policies）] メニューのネットワーク検出機能、アプリケーション検出機能、相関機能にアクセス可能です。検出管理者は、ポリシーを展開できません。

外部データベースのユーザ（External Database User）

JDBC SSL 接続に対応しているアプリケーションを用いて、Firepower System データベースに対して読取り専用のアクセスが可能です。Firepower システム アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースへの

アクセスを有効にする必要があります。Web インターフェイスでは、外部データベースユーザは、[ヘルプ（Help）] メニューのオンライン ヘルプ関連のオプションのみにアクセスできます。このロールの機能は、web インターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

侵入管理者（Intrusion Admin）

[ポリシー（Policies）] メニューと [オブジェクト（Objects）] メニューの侵入ポリシー機能、侵入ルール機能、ネットワーク分析ポリシー機能のすべてにアクセスが可能です。侵入管理者は、ポリシーを展開できません。

メンテナンス ユーザ（Maintenance User）

監視機能やメインテナンス機能へのアクセスが可能です。メンテナンス ユーザは、[ヘルス（Health）] メニューや [システム（System）] メニューのメンテナンス関連オプションにアクセスできます。

ネットワーク管理者（Network Admin）

[ポリシー（Policies）] メニューのアクセス制御機能、SSL インスペクション機能、DNS ポリシー機能、アイデンティティ ポリシー機能、および [デバイス（Devices）] メニューのデバイス設定機能へのアクセスが可能です。ネットワーク管理者は、デバイスへの設定の変更を展開できます。

セキュリティ アナリスト（Security Analyst）

セキュリティ イベント分析機能へのアクセスと [概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのヘルス イベントに対する読み取り専用のアクセスが可能です。

セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）

[概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのセキュリティ イベント分析機能とヘルス イベント機能への読み取り専用アクセスを提供します。

セキュリティ承認者（Security Approver）

[ポリシー（Policies）] メニューのアクセス制御ポリシーや関連のあるポリシー、ネットワーク検出ポリシーへの制限付きのアクセスが可能です。セキュリティ承認者はこれらのポリシーを表示し、展開できますが、ポリシーを変更することはできません。

外部認証ユーザは、他のロールを割当てられていない場合、LDAP または RADIUS 認証オブジェクトの設定やプラットフォーム設定に基づいて、最低限のアクセス権を有します。追加の権利を外部ユーザに割り当てることはできますが、最低限のアクセス権を削除するまたは変更するには、以下のタスクを実施する必要があります。

- ユーザを認証オブジェクトの 1 つのリストから別のリストに移動させるか、外部認証サーバのユーザの属性値またはグループ メンバーシップを変更します。
- プラットフォームの設定を更新します。
- ユーザ管理ページを使用して、ユーザ アカウントからのアクセスを削除します。

関連トピック

ユーザ アカウントの権限 （5 ページ）

カスタム ユーザ ロール

事前定義ユーザ ロールの他に、特定の分野に特化したアクセス権限を含むカスタム ユーザ ロールを作成できます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。事前定義ユーザ ロールと同様に、カスタム ロールは外部認証ユーザのデフォルト ロールとして使用できます。事前定義ロールとは異なり、カスタム ロールは変更、削除できます。

選択可能なアクセス許可は階層構造になっており、Firepower システムのメニュー レイアウトに基づいています。アクセス許可にサブページが含まれているか、または単純なページアクセスよりも詳細なアクセス許可が含まれている場合、このアクセス許可は拡張可能です。その場合、親のアクセス許可によって、ページ ビュー アクセス、およびそのページの関連機能への詳細な子のアクセス権が付与されます。「管理（Manage）」という単語が含まれているアクセス許可は、他のユーザが作成する情報を編集および削除できる権限を付与します。

ヒント メニュー構造に含まれていないページまたは機能の権限は、親または関連ページにより付与されます。たとえば、侵入ポリシーの変更（Modify Intrusion Policy）権限があれば、ネットワーク分析ポリシーの変更もできます。

カスタム ユーザ ロールに制限付き検索を適用できます。これにより、イベント ビューアでユーザに対して表示されるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニュー ベースのアクセス許可の下で [制限付き検索（Restricted Search）] ドロップダウン メニューからその検索を選択します。

Firepower Management Center でカスタム ユーザ ロールを設定するときには、すべてのメニューベースのアクセス許可を付与できます。管理対象デバイスでカスタム ユーザ ロールを設定するときには、デバイス機能に関連する一部のアクセス許可だけを使用できます。

[システム許可（System Permissions）] で選択できるオプションでは、外部データベースに対してクエリを実行したり、対象ユーザ ロールのアクセス許可にエスカレーションしたりすることができるユーザ ロールを作成できます。

オプションで、新しいカスタム ユーザ ロールを作成する代わりに、別のアプライアンスからカスタム ユーザ ロールをエクスポートし、ご使用のアプライアンスにインポートできます。インポートしたロールは、適用する前に、ニーズに合わせて編集できます。

関連トピック

ユーザ アカウントの権限 （5 ページ）
外部データベース アクセスの設定

例：カスタム ユーザ ロールとアクセス制御

アクセス制御関連機能のカスタム ユーザ ロールを作成して、Firepower システムのユーザのアクセス制御および関連付けられたポリシーの表示、変更権限の有無を指定できます。

次の表に、作成可能なカスタム ロールと例として挙げたロールでそれぞれ与えられるユーザ権限を示します。表にはそれぞれのカスタム ロールに必要な権限が記載されています。この例では、ポリシー承認者（Policy Approver）はアクセス コントロール ポリシーと侵入ポリシーの表示が可能です（変更はできません）。また、ポリシー承認者は設定の変更をデバイスに展開することもできます。

表 *1*：アクセス制御のカスタム ロールの例

カスタム ロールの権限	例：アクセス コントロール編集者（**Access Control Editor**）	例：侵入およびネットワーク分析編集者（**Intrusion & Network Analysis Editor**）	例：ポリシー承認者（**Policy Approver**）
アクセス制御	Yes	No	Yes
アクセス コントロール ポリシー（Access Control Policy）	Yes	No	Yes
アクセス制御ポリシーの変更（Modify Access Control Policy）	Yes	No	No
侵入ポリシー（Intrusion Policy）	No	Yes	Yes
侵入ポリシーの変更（Modify Intrusion Policy）	No	Yes	No
設定をデバイスに展開	No	No	Yes

ユーザ アカウントの権限

ここでは、Firepower システムでの設定可能なユーザ アクセス許可と、それらのアクセス許可にアクセスできる事前定義ユーザ ロールの一覧を示します。管理対象デバイスでは使用できないアクセス許可があります。Firepower Management Center でのみ使用可能なアクセス許可には、そのようにマークが付いています。

[概要（Overview）] メニュー

次の表は、[概要（Overview）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin、

および External Database User の各ロールには、[概要（Overview）] メニューでのアクセス許可がありません。

表 2 : [概要（*Overview*）] メニュー

権限	管理	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（**RO**）
ダッシュボード	Yes	Yes	Yes	Yes
ダッシュボードの管理	Yes	No	No	No
[アプライアンス情報（Appliance Information）] ウィジェット	Yes	Yes	Yes	Yes
[アプライアンス ステータス（Appliance Status）] ウィジェット（*Management Center* のみ）	Yes	Yes	Yes	Yes
[コリレーション イベント（Correlation Events）] ウィジェット	Yes	No	Yes	Yes
[現行インターフェイス ステータス（Current Interface Status）] ウィジェット	Yes	Yes	Yes	Yes
[現行セッション（Current Sessions）] ウィジェット	Yes	No	No	No
[カスタム分析（Custom Analysis）] ウィジェット（*Management Center* のみ）	Yes	No	Yes	Yes
[ディスク使用率（Disk Usage）] ウィジェット	Yes	Yes	Yes	Yes
[インターフェイス トラフィック（Interface Traffic）] ウィジェット	Yes	Yes	Yes	Yes

権限	管理	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
[侵入イベント（Intrusion Events）] ウィジェット（*Management Center* のみ）	Yes	No	Yes	Yes
[ネットワーク コリレーション（Network Correlation）] ウィジェット（*Management Center* のみ）	Yes	No	Yes	Yes
[製品ライセンス（Product Licensing）] ウィジェット（*Management Center* のみ）	Yes	Yes	No	No
[製品の更新（Product Updates）] ウィジェット	Yes	Yes	No	No
[RSS フィード（RSS Feed）] ウィジェット	Yes	Yes	Yes	Yes
[システムの負荷（System Load）] ウィジェット	Yes	Yes	Yes	Yes
[システム時刻（System Time）] ウィジェット	Yes	Yes	Yes	Yes
[ホワイトリスト イベント（White List Events）] ウィジェット（*Management Center* のみ）	Yes	No	Yes	Yes
[レポート（Reporting）]（*Management Center* のみ）	Yes	No	Yes	Yes

権限	管理	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
[レポートの管理テンプレート（Manage Report Templates）]（*Management Center* のみ）	Yes	No	Yes	Yes
要約	Yes	No	Yes	Yes
[侵入イベント統計（Intrusion Event Statistics）]（*Management Center* のみ）	Yes	No	Yes	Yes
侵入イベント パフォーマンス（Intrusion Event Performance）	Yes	No	No	No
[侵入イベント グラフ（Intrusion Event Graphs）]（*Management Center* のみ）	Yes	No	Yes	Yes
[検出統計情報（Discovery Statistics）]（*Management Center* のみ）	Yes	No	Yes	Yes
[ディスカバリ パフォーマンス（Discovery Performance）]（*Management Center* のみ）	Yes	No	No	No
[接続の概要（Connection Summary）]（*Management Center* のみ）	Yes	No	Yes	Yes

[分析（Analysis）] メニュー

次の表に、[分析（Analysis）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、そのユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。異なる見出しの下に複数回出現する権限は、最初に出現する表にのみ示されています。ただし、サブメニューの見出しを示す場合を除きます。Security Approver、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[分析（Analysis）] メニューに対する権限はありません。[分析（Analysis）] メニューは Firepower Management Center でのみ使用可能です。

表 *3 : [分析（Analysis）] メニュー*

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
コンテキスト エクスプローラ（Context Explorer）	Yes	No	No	Yes	Yes
接続イベント	Yes	No	No	Yes	Yes
接続イベントの変更（Modify Connection Events）	Yes	No	No	Yes	No
接続サマリー イベント（Connection Summary Events）	Yes	No	No	Yes	Yes
接続サマリー イベントの変更（Modify Connection Summary Events）	Yes	No	No	Yes	No
セキュリティ インテリジェンス イベント	Yes	No	No	Yes	Yes
セキュリティ インテリジェンス イベントの変更（Modify Security Intelligence Events）	Yes	No	No	Yes	No
侵入（Intrusion）	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
侵入イベント	Yes	No	No	Yes	Yes
侵入イベントの変更（Modify Intrusion Events）	Yes	No	No	Yes	No
ローカル ルールの表示（View Local Rules）	Yes	No	No	Yes	Yes
確認済みイベント（Reviewed Events）	Yes	No	No	Yes	Yes
クリップボード（Clipboard）	Yes	No	No	Yes	Yes
[インシデント（Incidents）]	Yes	No	No	Yes	Yes
インシデントの変更（Modify Incidents）	Yes	No	No	Yes	No
ファイル（Files）	Yes	No	No	Yes	Yes
マルウェア イベント	Yes	No	No	Yes	Yes
マルウェア イベントの変更（Modify Malware Events）	Yes	No	No	Yes	No
ファイル イベント	Yes	No	No	Yes	Yes
ファイル イベントの変更（Modify File Events）	Yes	No	No	Yes	No
キャプチャ ファイル（Captured Files）	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
キャプチャ ファイル（Captured Files）の編集（Modify Captured Files）	Yes	No	No	Yes	No
File Trajectory	Yes	No	No	Yes	Yes
ファイルのダウンロード（File Download）	Yes	No	No	Yes	Yes
ダイナミック ファイル分析（Dynamic File Analysis）	Yes	No	No	Yes	No
Hosts	Yes	No	No	Yes	Yes
ネットワーク マップ（Network Map）	Yes	No	No	Yes	Yes
Hosts	Yes	No	No	Yes	Yes
ホストの変更（Modify Hosts）	Yes	No	No	Yes	No
Indications of Compromise	Yes	No	No	Yes	Yes
侵害の兆候の変更（Modify Indications of Compromise）	Yes	No	No	Yes	No
サーバ	Yes	No	No	Yes	Yes
サーバの変更（Modify Servers）	Yes	No	No	Yes	No
脆弱性（Vulnerabilities）	Yes	No	No	Yes	Yes
脆弱性の変更（Modify Vulnerabilities）	Yes	No	No	Yes	No

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
ホスト属性（Host Attributes）	Yes	No	No	Yes	Yes
ホスト属性の変更（Modify Host Attributes）	Yes	No	No	Yes	No
アプリケーション	Yes	No	No	Yes	Yes
アプリケーション詳細（Application Details）	Yes	No	No	Yes	Yes
アプリケーションの詳細の変更（Modify Application Details）	Yes	No	No	Yes	No
ホスト属性の管理（Host Attribute Management）	Yes	No	No	No	No
検出イベント（Discovery Events）	Yes	No	No	Yes	Yes
検出イベントの変更（Modify Discovery Events）	Yes	No	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザアクティビティ（User Activity）	Yes	Yes	No	Yes	Yes
ユーザアクティビティイベントの変更（Modify User Activity Events）	Yes	Yes	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザの変更（Modify Users）	Yes	Yes	No	Yes	No

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
脆弱性（Vulnerabilities）	Yes	No	No	Yes	Yes
サードパーティの脆弱性（Third-party Vulnerabilities）	Yes	No	No	Yes	Yes
サードパーティの脆弱性の変更（Modify Third-party Vulnerabilities）	Yes	No	No	Yes	No
相関（Correlation）	Yes	Yes	No	Yes	Yes
相関イベント（Correlation Events）	Yes	Yes	No	Yes	Yes
相関イベントの変更（Modify Correlation Events）	Yes	Yes	No	Yes	No
ホワイトリストイベント（White List Events）	Yes	Yes	No	Yes	Yes
ホワイトリストイベントの変更（Modify White List Events）	Yes	Yes	No	Yes	No
ホワイトリスト違反（White List Violations）	Yes	Yes	No	Yes	Yes
修復ステータス（Remediation Status）	Yes	Yes	No	No	No
修復ステータスの変更（Modify Remediation Status）	Yes	Yes	No	No	No

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
カスタム（Custom）	Yes	No	No	Yes	Yes
カスタム ワークフロー（Custom Workflows）	Yes	No	No	Yes	Yes
カスタム ワークフローの管理（Manage Custom Workflows）	Yes	No	No	Yes	Yes
カスタム テーブル（Custom Tables）	Yes	No	No	Yes	Yes
カスタム テーブルの管理（Manage Custom Tables）	Yes	No	No	Yes	Yes
検索（Search）	Yes	No	Yes	Yes	Yes
検索の管理（Manage Search）	Yes	No	No	No	No
ブックマーク（Bookmarks）	Yes	No	No	Yes	Yes
ブックマークの管理（Manage Bookmarks）	Yes	No	No	Yes	Yes
アプリケーション統計（Application Statistics）	Yes	No	No	Yes	Yes
地理位置情報の統計（Geolocation Statistics）	Yes	No	No	Yes	Yes
ユーザ統計（User Statistics）	Yes	No	No	Yes	Yes
URL カテゴリ統計（URL Category Statistics）	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
URL レピュテーション統計（URL Reputation Statistics）	Yes	No	No	Yes	Yes
レコードタイプ別 DNS クエリ（DNS Queries by Record Types）	Yes	No	No	Yes	Yes
SSL 統計（SSL Statistics）	Yes	No	No	Yes	Yes
アプリケーション別侵入イベント統計（Intrusion Event Statistics by Application）	Yes	No	No	Yes	Yes
ユーザ別侵入イベント統計（Intrusion Event Statistics by User）	Yes	No	No	Yes	Yes
セキュリティ インテリジェンス カテゴリ統計（Security Intelligence Category Statistics）	Yes	No	No	Yes	Yes
性質別ファイル ストレージ統計（File Storage Statistics by Disposition）	Yes	No	No	Yes	Yes
タイプ別ファイル ストレージ統計（File Storage Statistics by Type）	Yes	No	No	Yes	Yes
ダイナミック ファイル分析統計（Dynamic File Analysis Statistics）	Yes	No	No	Yes	Yes

ポリシー メニュー

次の表には、ポリシー メニューのそれぞれのオプションへのアクセスに必要なユーザ ロールの権限や、ユーザ ロールがポリシー メニューのサブパーミッションにアクセス可能であるかを順番に示します。外部データベース ユーザ、メンテナンス ユーザ、セキュリティ アナリスト、セキュリティ アナリスト（読取り専用）ロールには、ポリシー メニューの権限はありません。ポリシー メニューは、Firepower Management Center でのみ利用可能です。

侵入ポリシーおよび「侵入ポリシーの変更」の権限により、ネットワーク アナリシス ポリシーの作成および変更が可能になる点にご注意ください。

表 *4:* ポリシー メニュー

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
アクセス制御	Yes	Yes	No	No	Yes	Yes
アクセス コントロール ポリシー（Access Control Policy）	Yes	Yes	No	No	Yes	Yes
アクセス制御ポリシーの変更（Modify Access Control Policy）	Yes	Yes	No	No	Yes	No
管理者ルールの変更（Modify Administrator Rules）	Yes	Yes	No	No	Yes	No
ルート ルールの変更（Modify Root Rules）	Yes	Yes	No	No	Yes	No
侵入ポリシー（Intrusion Policy）	No	Yes	No	Yes	No	Yes
侵入ポリシーの変更（Modify Intrusion Policy）	No	Yes	No	Yes	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
マルウェア & ファイル ポリシー（Malware & File Policy）	Yes	Yes	No	No	No	Yes
マルウェア & ファイル ポリシーの変更（Modify Malware & File Policy）	Yes	Yes	No	No	No	No
DNS ポリシー（DNS Policy）	Yes	Yes	No	No	Yes	Yes
DNS ポリシーの変更（Modify DNS Policy）	Yes	Yes	No	No	Yes	No
アイデンティティ ポリシー（Identity Policy）	Yes	Yes	No	No	Yes	No
アイデンティティ ポリシーの変更（Modify Identity Policy）	Yes	Yes	No	No	Yes	No
管理者ルールの変更（Modify Administrator Rules）	Yes	Yes	No	No	Yes	No
ルート ルールの変更（Modify Root Rules）	Yes	Yes	No	No	Yes	No
SSL ポリシー（SSL Policy）	Yes	Yes	No	No	Yes	Yes
SSL ポリシーの変更（Modify SSL Policy）	Yes	Yes	No	No	Yes	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
管理者ルールの変更（Modify Administrator Rules）	Yes	Yes	No	No	Yes	No
ルート ルールの変更（Modify Root Rules）	Yes	Yes	No	No	Yes	No
プレフィルタ ポリシー（Prefilter Policy）	Yes	Yes	No	No	Yes	Yes
プレフィルタ ポリシーの変更（odify Prefilter Policy）	Yes	Yes	No	No	Yes	No
ネットワーク ディスカバリ（Network Discovery）	No	Yes	Yes	No	No	Yes
カスタム フィンガープリント（Custom Fingerprinting）	No	Yes	Yes	No	No	No
カスタム フィンガープリントの変更（Modify Custom Fingerprinting）	No	Yes	Yes	No	No	No
カスタム トポロジ（Custom Topology）	No	Yes	Yes	No	No	No
カスタム トポロジの変更（Modify Custom Topology）	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
ネットワーク検出の変更（Modify Network Discovery）	No	Yes	Yes	No	No	No
アプリケーション ディテクタ（Application Detectors）	No	Yes	Yes	No	No	No
アプリケーション ディテクタの変更（Modify Application Detectors）	No	Yes	Yes	No	No	No
ユーザ サードパーティ マッピング（User 3rd Party Mappings）	No	Yes	Yes	No	No	No
ユーザ サードパーティ マッピングの変更（Modify User 3rd Party Mappings）	No	Yes	No	No	No	No
カスタム製品のマッピング（Custom Product Mappings）	No	Yes	Yes	No	No	No
カスタム製品マッピングの変更（Modify Custom Product Mappings）	No	Yes	No	No	No	No
相関（Correlation）	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
ポリシーの管理（Policy Management）	No	Yes	No	No	No	No
ポリシーの管理の変更（Modify Policy Management）	No	Yes	Yes	No	No	No
ルールの管理（Rule Management）	No	Yes	No	No	No	No
ルールの管理の変更（Modify Rule Management）	No	Yes	Yes	No	No	No
ホワイト リスト（White List）	No	Yes	No	No	No	No
ホワイトリストの変更（Modify White List）	No	Yes	Yes	No	No	No
トラフィック プロファイル（Traffic Profiles）	No	Yes	No	No	No	No
トラフィック プロファイルの変更（Modify Traffic Profiles）	No	Yes	Yes	No	No	No
アクション（Actions）	No	Yes	Yes	No	No	Yes
アラート（Alerts）	No	Yes	Yes	No	No	Yes
影響度フラグ アラート（Impact Flag Alerts）	No	Yes	Yes	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
影響度フラグアラートの変更（Modify Impact Flag Alerts）	No	Yes	Yes	No	No	No
検出イベントアラート（Discovery Event Alerts）	No	Yes	Yes	No	No	No
検出イベントアラートの変更（Modify Discovery Event Alerts）	No	Yes	Yes	No	No	No
E メール	No	Yes	No	Yes	No	No
E メールの変更（Modify Email）	No	Yes	No	Yes	No	No
アラートの変更（Modify Alerts）	No	Yes	Yes	No	No	No
スキャナ（Scanners）	No	Yes	Yes	No	No	No
スキャン結果（Scan Results）	No	Yes	Yes	No	No	No
スキャン結果の変更（Modify Scan Results）	No	Yes	Yes	No	No	No
スキャナの変更（Modify Scanners）	No	Yes	Yes	No	No	No
グループ（Groups）	No	Yes	No	No	No	No
グループの変更（Modify Groups）	No	Yes	Yes	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
モジュール（Modules）	No	Yes	No	No	No	No
モジュールの変更（Modify Modules）	No	Yes	Yes	No	No	No
インスタンス（Instances）	No	Yes	No	No	No	No
インスタンスの変更（Modify Instances）	No	Yes	Yes	No	No	No

[デバイス（Devices）] メニュー

[Devices（デバイス）] メニューの表には、[デバイス（Devices）] メニューの各オプションとそのサブ権限にアクセスするために必要なユーザ ロール特権を順に示します。検出管理者、外部データベースユーザ、侵入管理者、メンテナンスユーザ、セキュリティアナリスト、セキュリティ アナリスト（読取り専用）ロールには、ポリシー メニューの権限はありません。[デバイス（Devices）] メニューは Firepower Management Center でのみ使用可能です。

表 5 : [デバイス（*Devices*）] メニュー

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
デバイス管理	No	Yes	Yes	Yes
デバイスの変更（Modify Devices）	No	Yes	Yes	No
NAT	Yes	Yes	Yes	Yes
NAT リスト（NAT List）	Yes	Yes	Yes	Yes
NAT ポリシーの変更（Modify NAT Policy）	Yes	Yes	Yes	No
VPN	No	Yes	Yes	Yes
VPN の変更（Modify VPN）	No	Yes	Yes	No
QoS	Yes	Yes	Yes	No
QoS ポリシーの変更（Modify QoS Policy）	Yes	Yes	Yes	No
デバイス管理	No	Yes	Yes	No

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
デバイスの変更（Modify Devices）	No	Yes	Yes	No

[オブジェクト マネージャ（Object Manager）] メニュー

[オブジェクト マネージャ（Object Manager）] メニューの表には、[オブジェクト マネージャ（Object Manager）] メニューの各オプションとそのサブ権限にアクセスするために必要なユーザ ロール特権を順に示します。Discovery Admin、Security Approver、Maintenance User、External Database User、Security Analyst、および Security Analyst（読み取り専用）の各ロールには、[オブジェクト マネージャ（Object Manager）] メニューでのアクセス許可がありません。[オブジェクト マネージャ（Object Manager）] メニューは Firepower Management Center でのみ使用可能です。

表 *6 : [*オブジェクト マネージャ（***Object Manager***）*]* メニュー

メニュー	アクセス管理者	管理者	侵入管理者	ネットワーク管理者
[オブジェクト マネージャ（Object Manager）]	Yes	Yes	No	Yes
[ルール エディタ（Rule Editor）]	No	Yes	Yes	No
[ルール エディタの変更（Modify Rule Editor）]	No	Yes	Yes	No
NAT リスト（NAT List）	Yes	Yes	No	Yes
[オブジェクト マネージャの変更（Modify Object Manager）]	No	Yes	No	No

Cisco AMP

Cisco AMP 権限は、Administrator ユーザ ロールのみに対して使用可能です。この権限は、Firepower Management Center でのみ使用可能です。

デバイスへの設定の展開

デバイスに設定を展開する権限は、Administrator、Network Admin、および Security Approver のロールで使用できます。この権限は、Firepower Management Center でのみ使用可能です。

[システム（System）] メニュー

次の表は、[システム（System）] メニューの各オプションにアクセスするために必要なユーザロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。外部データベース ユーザ ロールには、[システム（System）] メニューへのアクセス許可が与えられません。

表 *7*: *[システム（System）]* メニュー

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
設定（Configuration）	No	Yes	No	No	No	No	No	No	No
ドメイン（Domains）	No	Yes	No	No	No	No	No	No	No
統合	No	Yes	No	No	No	Yes	Yes	No	No
Cisco CSI	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデンティティ レルム（Identity Realms）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデンティティ レルムを変更（Modify Identity Realms）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
アイデンティティ ソース（Identity Sources）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデンティティ ソースを変更（Modify Identity Sources）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	No	No	No
eStreamer	No	Yes	No	No	No	No	No	No	No
ホスト入力クライアント（Host Input Client）（*Management Center* のみ）	No	Yes	No	No	No	No	No	No	No
スマート ソフトウェア サテライト（Smart Software Satellite）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	Yes	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
スマートソフトウェア サテライトを変更（Modify Smart Software Satellite）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	No	No	No
ユーザ管理（User Management）	No	Yes	No	No	No	No	No	No	No
Users	No	Yes	No	No	No	No	No	No	No
ユーザの役割	No	Yes	No	No	No	No	No	No	No
外部認証（External Authentication）（*Management Center* のみ）	No	Yes	Yes	No	No	No	No	No	No
変更点	No	Yes	No	No	No	No	No	No	No
ルール更新（Rule Updates）（*Management Center* のみ）	No	Yes	No	Yes	No	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
ルール更新のインポート ログ（Rule Update Import Log）（*Management Center* のみ）	No	Yes	No	No	No	No	No	No	No
ライセンス	No	Yes	No	No	No	No	No	No	No
スマート ライセンス（Smart Licences）	No	Yes	No	No	No	No	No	No	No
スマート ライセンスの変更（Modify Smart Licenses）	No	Yes	No	No	No	No	No	No	No
クラシック ライセンス（Classic Licenses）	No	Yes	No	No	No	No	No	No	No
正常性（Health）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
正常性ポリシー（Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポリシーを変更（Modify Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポリシーを適用（Apply Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
ヘルス イベント（Health Events）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
ヘルス イベントを変更（Modify Health Events）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
モニタリング（Monitoring）	No	Yes	No	No	Yes	Yes	Yes	Yes	No
監査（Audit）	No	Yes	No	No	Yes	No	No	No	No
監査ログを変更（Modify Audit Log）	No	Yes	No	No	Yes	No	No	No	No
Syslog	No	Yes	No	No	Yes	No	No	No	No
統計情報（Statistics）	No	Yes	No	No	Yes	No	No	No	No
ツール	No	Yes	No	No	Yes	No	No	Yes	No
バックアップ管理（Backup Management）	No	Yes	No	No	Yes	No	No	No	No
バックアップを復元（Restore Backup）	No	Yes	No	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンス ユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティ アナリスト	セキュリティ アナリスト（RO）
スケジューリング（Scheduling）	No	Yes	No	No	Yes	No	No	No	No
その他のユーザのスケジュール済みタスクを削除（Delete Other Users' Scheduled Tasks）	No	Yes	No	No	No	No	No	No	No
インポート/エクスポート（Import/Export）	No	Yes	No	No	No	No	No	No	No
ディスカバリ データの消去（Discovery Data Purge）（*Management Center* のみ）	No	Yes	No	No	No	No	No	Yes	No
whois（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes

[REST VDI] メニュー

[REST VDI] メニュー テーブルには、REST VDI メニューのそれぞれのオプションにアクセスするのに必要なユーザ ロールの特権とその中のサブパーミッションを順番に列挙します。検出

管理者、外部データベース ユーザ、侵入管理者、メンテナンス ユーザ、セキュリティ アナリスト、セキュリティ アナリスト（読取り専用）ロールには、ポリシー メニューの権限はありません。[デバイス（Devices）] メニューはFirepower Management Centerでのみ使用可能です。

表 *8 : REST VDI* メニュー

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
REST VDI	Yes	Yes	Yes	Yes
REST VDI の変更	Yes	Yes	Yes	No

[ヘルプ（Help）] メニュー

[ヘルプ（Help）] メニューとその権限には、すべてのユーザ ロールがアクセスできます。[ヘルプ（Help）] メニュー オプションを制限することはできません。

ユーザ ロールの管理

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）	任意（Any）	任意（Any）	任意（Any）	Admin

Firepowerシステムの各ユーザは、ユーザ アクセス ロール（1 つまたは複数）に関連付けられています。これに該当するユーザ ロールには、システムのメニューなどのオプションへのアクセスを決定する権限が割り当てられます。たとえばアナリストは、ネットワークのセキュリティを分析するためにイベント データへのアクセスが必要ですが、Firepower システム自体の管理機能へのアクセスが必要になることはありません。アナリストにはSecurity Analystのアクセス権を付与し、Firepower システムを管理する 1 人以上のユーザに対して Administrator ロールを予約しておくことができます。

Firepowerシステムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。これらの事前定義のユーザ ロールには、事前設定されたアクセス権限のセットが含まれています。

より詳細なアクセス権限を使用して、カスタムのユーザ ロールを作成することもできます。

また、あるユーザ ロールがイベント ビューアで表示できるデータを制限するために、そのロールに制限付きの検索を適用することもできます。制限付きアクセスを使用してカスタム ロールを作成するには、[権限に基づくメニュー（Menu Based Permissions）] リストから制限するテーブルを選択し、次に [制限付き検索（Restrictive Search）] ドロップダウンリストからプライベート保存検索を選択します。

事前定義のユーザ ロールは削除できませんが、不要になったカスタム ロールは削除できます。カスタム ロールを完全に削除することなく無効にするには、削除する代わりに非アクティブ化します。自分のユーザ ロール、またはプラットフォーム設定ポリシーでデフォルト ユーザ ロールとして設定されているロールは削除できない点に注意してください。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 ユーザ ロールを管理します。

- アクティブ化：事前定義されたユーザ ロールをアクティブ化または非アクティブ化します。詳細については、ユーザ ロールのアクティブおよび非アクティブの設定 （32 ページ）を参照してください。
- 作成：カスタム ユーザ ロールを作成します。詳細については、次を参照してください。カスタム ユーザ ロールの作成 （33 ページ）
- コピー：新しいカスタム ユーザ ロールを作成するために、既存のユーザ ロールをコピーします。詳細については、ユーザ ロールのコピー （34 ページ）を参照してください。
- 編集：カスタム ユーザ ロールを編集します。詳細については、カスタム ユーザ ロールの編集 （35 ページ）を参照してください。
- 削除：削除するカスタム ロールの横にある削除アイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- （注） 削除されたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [ユーザ設定（User Preferences）] メニューにアクセスできますが、Firepower システムにはアクセスできなくなります。

ユーザ ロールのアクティブおよび非アクティブの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。

⚠

注意 非アクティブにされたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [User Preferences] メニューにアクセスできますが、Firepower System にはアクセスできません。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログイン セッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザは Web インターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。

カスタム ユーザ ロールの作成

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）	任意（Any）	任意（Any）	任意（Any）	Admin

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 [ユーザ ロールの作成（Create User Role）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、新しいユーザ ロールの名前を入力します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 オプションで、[説明（Description）] を追加します。

ステップ 6 新しいロールのメニューベースのアクセス許可を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセ

ス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすると、その事前定義ロールに関連付けられているアクセス許可が事前選択されます。

ステップ 7 必要に応じて、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにして、新規ロールのデータベース アクセス権限を設定します。

ステップ 8 エスカレーションに使用するカスタム ユーザ ロールの設定 （37 ページ）の説明に従って、必要に応じて Firepower Management Center で、新規ユーザ ロールのエスカレーション アクセス許可を設定します。

ステップ 9 [保存（Save）] をクリックします。

ユーザ ロールのコピー

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）	任意（Any）	任意（Any）	任意（Any）	Admin

新しいカスタム ロールのベースとして使用する既存のロールをコピーできます。これにより、ユーザ ロール エディタで既存のロールの権限が事前に選択されるので、あるロールをモデルとして別のロールを作成できます。

事前定義されたユーザ ロールや先祖ドメインから継承されるカスタム ユーザ ロールなど、既存のロールをコピーできます。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 コピーするユーザ ロールの横にあるコピー アイコン（  ）をクリックします。

ステップ 4 新しい名前を入力します。

システムは、元のユーザ ロールの名前と `(copy)` サフィックスを組み合わせた新しいユーザ ロールのデフォルト名を作成します。

ステップ 5 [説明（Description）] ボックスに新しい説明を入力します。

上書きしないことを選択した場合、システムは元のユーザ ロールの説明を保持します。

ステップ 6 オプションで、元のユーザ ロールから継承されたメニュー ベースの権限を変更します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセ

ス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。

ステップ 7 オプションで、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにすることで、新しいロールのデータベース アクセス権限を設定します。

ステップ 8 オプションで、エスカレーションに使用するカスタム ユーザ ロールの設定 （37 ページ）の説明に従って、新しいユーザ ロールのエスカレーション権限を設定します。

ステップ 9 [保存（Save）] をクリックします。

カスタム ユーザ ロールの編集

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）	任意（Any）	任意（Any）	任意（Any）	Admin

事前定義ユーザ ロールは編集できません。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 変更するカスタム ユーザ ロールの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [名前（Name）] フィールドと [説明（Description）] フィールドを変更します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 ユーザ ロールのメニューベースのアクセス許可を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。

ステップ 6 必要に応じて、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにすることにより、ロールのデータベース アクセス権限を設定します。

ステップ 7 必要に応じて、エスカレーションに使用するカスタム ユーザ ロールの設定 （37 ページ）の説明に従って Firepower Management Center で、ユーザ ロールにエスカレーション アクセス許可を設定します。

ステップ 8 [保存（Save）] をクリックします。

ユーザ ロールのエスカレーション

カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、別のターゲット ユーザ ロールの特権を一時的に取得できます。これにより、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況をさらに注意深く追跡することができます。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために Administrator ロールにエスカレーションする場合があります。この機能は、ユーザが各自のパスワードを使用したり、指定された別のユーザのパスワードを使用したりできるように設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーション パスワードを容易に管理できます。

エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけであることに注意してください。カスタム ユーザ ロールまたは事前定義ユーザ ロールを使用できます。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

エスカレーション ターゲット ロールの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、他のロールからのエスカレーション先となるロールです（エスカレーションが可能な場合）。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザ ロール（User Roles）] をクリックします。

ステップ 3 [アクセス許可エスカレーションの設定（Configure Permission Escalation）] をクリックします。

ステップ 4 ドロップダウン リストからユーザ ロールを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

（注） エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーションに使用するカスタム ユーザ ロールの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーションユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーションユーザが影響を受けます。このことにより、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

手順

ステップ 1 カスタム ユーザ ロールの作成 （33 ページ）の説明に従って、カスタム ユーザ ロールの設定を開始します。

ステップ 2 [システム権限（System Permissions）] で、[このロールをエスカレーションする：（Set this role to escalate to:）] チェックボックスをオンにします。

現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。

ステップ 3 このロールがエスカレーションするときに使用するパスワードを選択します。次の2つの対処法があります。

- このロールが割り当てられているユーザがエスカレーション時に各自のパスワードを使用できるようにするには、[割り当てられているユーザのパスワードで認証（Authenticate with the assigned user's password）] を選択します。
- このロールが割り当てられているユーザが、別のユーザのパスワードを使用するようにするには、[指定されたユーザのパスワードで認証（Authenticate with the specified user's password）] を選択し、そのユーザ名を入力します。

（注） 別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

ステップ 4 [保存（Save）] をクリックします。
これで、このロールが割り当てられているユーザはターゲット ユーザ ロールにエスカレーションできます。

ユーザ ロールのエスカレーション

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）	任意（Any）	Management Center	任意（Any）	任意（Any）

エスカレーション対象のアクセス許可が含まれているカスタム ユーザ ロールが割り当てられているユーザは、いつでもターゲット ロールのアクセス許可にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。

始める前に

- 管理者が、エスカレーション ターゲット ロールの設定 （36 ページ）またはエスカレーションに使用するカスタム ユーザ ロールの設定 （37 ページ）に従って、エスカレーション ターゲット ロールまたはカスタム ユーザ ロールをエスカレーション用に設定済みであることを確認してください。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[アクセス許可のエスカレーション（Escalate Permissions）] を選択します。

ステップ 2 認証パスワードを入力します。

ステップ 3 [エスカレート（Escalate）]をクリックします。これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

（注） エスカレーションはログイン セッションの残り期間にわたって保持されます。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

ユーザ アカウント

Firepower Management Center デバイスまたは Firepower 7000 および 8000 シリーズ デバイス上の管理者アカウント、およびオプションのカスタムのユーザ アカウントを使用すれば、ユーザはこれらのデバイスにログインすることができます。内部認証ユーザについては、アカウント

を手動で作成する必要があります。外部認証ユーザについては、アカウントが自動的に作成されます。

Firepower Threat Defense の場合、個別の CLI ユーザを作成できます。これらのユーザは、SSH を通じてデバイスにアクセスして、追加のトラブルシューティングとシステムのモニタリングを行うことができます。ただし、これらのユーザは CLI で作成する必要があり、Firepower Management Center で作成することはできません。

関連トピック

Firepower システムのユーザ アカウント
Firepower システムのユーザ インターフェイス

ユーザ アカウントの管理

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）	任意（Any）	任意（Any）	任意（Any）	Admin

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 ユーザ アカウントを管理します。

- アクティブ化/非アクティブ化：ユーザの横にあるスライダをクリックすると、非アクティブ化されたユーザの場合は再アクティブ化され、アクティブなユーザ アカウントの場合は削除せずに無効化されます。アクティブ化/非アクティブ化できるのは内部で認証されたユーザのみです。
- 作成：新しいユーザ アカウントを作成します（ユーザ アカウントの作成 （40 ページ）を参照）。
- 編集：既存のユーザ アカウントを編集します（ユーザ アカウントの編集 （41 ページ）を参照）。
- 削除：ユーザを削除する場合は、削除アイコン（）をクリックします。admin アカウント以外のユーザ アカウントはシステムからいつでも削除できます。admin アカウントは削除できません。

関連トピック

Lights-Out 管理のユーザ アクセス設定
定義済みのユーザ ロール （2 ページ）
カスタム ユーザ ロール （4 ページ）

ユーザ アカウントの作成

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）	任意（Any）	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin

新しいユーザアカウントをセットアップするときに、そのアカウントでアクセスできるシステムの部分を制御できます。ユーザ アカウントの作成時に、ユーザ アカウントのパスワードの有効期限と強度を設定できます。7000 または 8000 シリーズデバイスのローカル アカウントの場合、ユーザに付与するコマンド ライン アクセスのレベルも設定できます。

マルチドメイン型展開では、Admin アクセス権限があるドメインでユーザ アカウントを作成できます。また、上位のドメインでアカウントを作成し、それよりも低いアクセス権のみをユーザに割り当てることもできます。たとえば、単一ユーザを2つのドメインの管理者にし、先祖のドメインへのアクセスは拒否することができます。このタイプのユーザアカウントは、アクセス権が割り当てられているサブドメインに切り替えることによってのみ変更することができます。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [ユーザの作成（Create User）] をクリックします。

ステップ 3 [ユーザ名（User Name）] に入力します。

ステップ 4 ログイン オプションを変更します（ユーザ アカウント ログイン オプション （43 ページ）を参照）。

ステップ 5 [パスワード（Password）] と [パスワードの確認（Confirm Password）] に値を入力します。

入力する値は、以前に設定したパスワード オプションに基づいている必要があります。

ステップ 6 7000 または 8000 シリーズ デバイスでユーザ アカウントを作成する場合、コマンド ラインのアクセス レベル （45 ページ）の説明に従って、適切なレベルの [コマンドライン インターフェイス アクセス（Command-Line Interface Access）] を割り当てます。

ステップ 7 次のようにして、ユーザ ロールを割り当てます。

- ユーザに割り当てるユーザ ロールの横のチェックボックスをオンまたはオフにします。
- マルチドメイン展開では、子孫ドメインを持つドメインにユーザアカウントを追加する場合、ユーザ ロールのチェック ボックスの代わりに表示される [ドメインの追加（Add Domains）] ボタンをクリックします。複数のドメインでのユーザ ロールの割り当て （42 ページ）の手順に従って進みます。

（注） ユーザ ロールによって、ユーザのアクセス権が決定します。詳細については、ユーザ ロールの管理 （31 ページ）を参照してください。

ステップ 8 [Save] をクリックします。

ユーザ アカウントの編集

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）	任意（Any）	任意（Any）	任意（Any）	Admin

システムにユーザ アカウントを追加したら、アクセス権限、アカウント オプション、パスワードをいつでも変更できます。パスワード管理オプションは、外部ディレクトリ サーバに対して認証されるユーザには適用されないことに注意してください。これらの設定は外部サーバで管理します。ただし、外部認証されるアカウントを含め、すべてのアカウントのアクセス権を設定する必要があります。

（注） 外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの Firepower システム ユーザ管理ページでは、最小アクセス権を削除することができません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] カラムに、[外部 - ローカルで変更済み（External - Locally Modified）] というステータスが表示されます。

ユーザの認証を外部認証から内部認証に変更した場合は、ユーザの新しいパスワードを指定する必要があります。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 変更するユーザの横にある編集アイコン（  ）をクリックします。

ステップ 3 ユーザ アカウントの作成 （40 ページ）の説明に従って設定を変更します。

ステップ 4 [保存（Save）] をクリックします。

複数のドメインでのユーザ ロールの割り当て

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）	任意（Any）	任意（Any）	任意（Any）	Admin

マルチドメイン展開では、先祖や子孫のドメインにユーザ ロールを割り当てることができます。たとえば、グローバル ドメインでユーザに読み取り専用権限を割り当てながら、子孫ドメインに管理者権限を割り当てることもできます。

手順

ステップ 1 ユーザ アカウント エディタで、[ドメインの追加（Add Domain）] をクリックします。
ステップ 2 [ドメイン（Domain）] ドロップダウン リストからドメインを選択します。
ステップ 3 ユーザを割り当てるユーザ ロールをオンにします。
ステップ 4 [保存（Save）] をクリックします。

内部認証から外部認証へのユーザの変換

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）	任意（Any）	任意（Any）	任意（Any）	Admin

（注） 内部認証から外部認証にユーザを変換するとき、ユーザ アカウントに設定されているアクセス許可が保持されます。既存のアクセス許可は、関連する認証オブジェクト グループまたはプラットフォーム設定ポリシーで設定されたデフォルトのユーザ ロールに関連付けられたすべてのアクセス許可より優先されます。

始める前に

- 同じユーザ名を持つユーザ レコードが外部認証サーバに存在する必要があります。

手順

ステップ 1 LDAP（CAC を使用する場合または使用しない場合）あるいはRADIUS認証を有効にします。詳細については、LDAP 認証 （51 ページ）またはRADIUS 認証 （78 ページ）を参照してください。

ステップ 2 外部サーバに保存されているそのユーザのパスワードを使用してログインするようユーザに指示します。

ユーザ アカウント ログイン オプション

次の表に、Firepower システム ユーザのパスワードおよびアカウント アクセスの調整に使用できるオプションの一部について説明します。

（注）
- パスワード管理オプションは、外部ディレクトリ サーバに対して認証されるユーザには適用されません。これらの設定は外部認証サーバで管理します。[外部認証方式を使用する（Use External Authentication Method）] を有効にすると、ディスプレイからパスワード管理オプションが削除されます。
- アプライアンスでセキュリティ認定コンプライアンスまたはLights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。セキュリティ認定コンプライアンスの詳細については、セキュリティ認定準拠の を参照してください。

表 *9*:ユーザ アカウント ログイン オプション

オプション	説明
外部認証方式を使用する（Use External Authentication Method）	このユーザの資格情報を外部で認証する場合に、このチェックボックスをオンにします。このオプションを有効にすると、パスワード管理オプションが表示されなくなります。 （注） • 外部ディレクトリ サーバに対してユーザを認証する場合は、使用するサーバの認証オブジェクトを作成し、認証が有効な状態でプラットフォーム設定ポリシーを適用します。 • 外部認証ユーザの場合、サーバの認証オブジェクトを無効にすると、[ユーザ（Users）] リストの [認証方式（Authentication Method）] カラムに [外部（無効）（External (Disabled)）] と表示されます。 • ユーザに対してこのオプションを選択した場合に外部認証サーバが使用できないと、そのユーザは Web インターフェイスにログインできますが、どの機能にもアクセスできません。

オプション	説明
ログイン失敗の最大許容回数（Maximum Number of Failed Logins）	各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は5回です。ログイン失敗回数を無制限にするには、**0** を設定します。
パスワード長の最小値（Minimum Password Length）	ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は **8** です。値 **0** は、最小長が必須ではないことを示します。 [パスワード強度のチェック（Check Password Strength）] オプションを有効にして、[パスワード長の最小値（Minimum Password Length）] を 8 文字を超える値に設定すると、いずれか大きい値が適用されます。
パスワードの有効期限の残日数（Days Until Password Expiration）	ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す **0** です。このオプションを設定すると、[ユーザ（Users）] リストの [パスワードのライフタイム（Password Lifetime）] カラムに、各ユーザのパスワードの残っている日数が表示されます。
パスワードの有効期限の残日数警告（Days Before Password Expiration Warning）	パスワードが実際に期限切れになる何日前に、ユーザがパスワードを変更する必要があるという警告を表示するかを入力します。デフォルト設定は **0** 日間です。 **（注）** 警告日数は、パスワードの残りの有効期間の日数**未満**である必要があります。
ログイン時にパスワードのリセットを強制（Force Password Reset on Login）	次回ログイン時に、ユーザに強制的に各自のパスワードを変更させるには、このオプションを選択します。
パスワード強度のチェック（Check Password Strength）	強力なパスワードを必須にするには、このオプションを選択します。強力なパスワードとは、8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用するパスワードです。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
ブラウザ セッション タイムアウトから除外する（Exempt from Browser Session Timeout）	操作が行われなかったことが原因でユーザのログインセッションが終了しないようにするには、このオプションを選択します。管理者ロールが割り当てられているユーザを除外することはできません。

コマンド ラインのアクセス レベル

7000 または 8000 シリーズ デバイスでローカル Web インターフェイスを使用して、コマンド ライン インターフェイス アクセスをローカル デバイスのユーザに割り当てることができます。NGIPSv ではコマンド ライン アクセスをユーザに割り当てることもできますが、コマンドはコマンド ライン インターフェイスから使用することに注意してください。

ユーザが実行できるコマンドは、ユーザに割り当てられているアクセスのレベルによって決まります。[コマンドライン インターフェイス アクセス（Command-Line Interface Access）] 設定で指定できる値は、次のとおりです。

なし（None）

ユーザは、コマンドラインでアプライアンスにログインすることはできません。ユーザが資格情報を入力すると、ユーザが開始したセッションがすべて終了します。ユーザ作成時に、アクセス レベルはデフォルトで [なし（None）] に設定されます。

設定（Configuration）

ユーザは、任意のコマンド ライン オプションにアクセスできます。このアクセス レベルをユーザに割り当てるときには注意してください。

⚠

注意 外部認証ユーザに付与されるコマンド ライン アクセスは、デフォルトで [設定（Configuration）] レベルのコマンド ライン アクセスになり、すべてのコマンド ライン ユーティリティに対する権限が付与されます。

基本

特定の一連のコマンドはユーザが実行できます。それらは、次のとおりです。

表 *10*：基本的なコマンド ライン コマンド

configure password	interfaces
終了	lcd
exit	link-state
ヘルプ	log-ips-connection
history	managers
ログアウト	memory
?	model
??	mpls-depth
access-control-config	NAT
alarms	network

arp-tables	network-modules
audit-log	ntp
bypass	perfstats
high-availability	portstats
cpu	power-supply-status
データベース	process-tree
device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	時刻
fastpath-rules	traffic-statistics
gui	version
hostname	virtual-routers
hyperthreading	virtual-switches
inline-sets	

Firepower Threat Defense の CLI ユーザ アカウントの作成

Firepower Threat Defense デバイスで CLI にアクセスするユーザを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニタリング用に役立ちます。

複数のデバイス上にアカウントを一度に作成することはできません。デバイスごとに固有の CLI アカウントのセットがあります。

手順

ステップ 1 config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config権限を持っていればどのアカウントでも問題ありません。SSH セッションまたはコンソール ポートを使用できます。

特定のデバイス モデルでは、コンソール ポートから FXOS CLI に移動します。**connect ftd** コマンドを使用して Firepower Threat Defense CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

configure user add *username* {**basic** | **config**}

次の権限レベルを持つユーザを定義できます。

- **config**：ユーザに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。
- **basic**：ユーザに基本的なアクセス権を付与します。ユーザはコンフィギュレーション コマンドを入力することはできません。

例：

次の例では、configアクセス権を使用して、joecoolという名前のユーザアカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注） **configure password** コマンドを使用して自分のパスワードを変更できることをユーザに伝えます。

ステップ 3 （オプション）セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

  ユーザパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も1～9999ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** ユーザ名

  次回ログイン時にユーザにパスワードを強制的に変更してもらいます。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を1～9999までで設定します。アカウントをロック解除するには、**configure user unlock** コマンドを使用します。新しいアカウントのデフォルトは、5回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

  パスワードの最小長を1～127までで設定します。

- **configure user strengthcheck** ユーザ名 {**enable** | **disable**}

パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザ パスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりする必要があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** ユーザ名 {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** ユーザ名

  指定したアカウントを削除します。

- **configure user disable** ユーザ名

  指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** ユーザ名

  指定したアカウントを有効にします。

- **configure user password** ユーザ名

  指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** ユーザ名

  ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

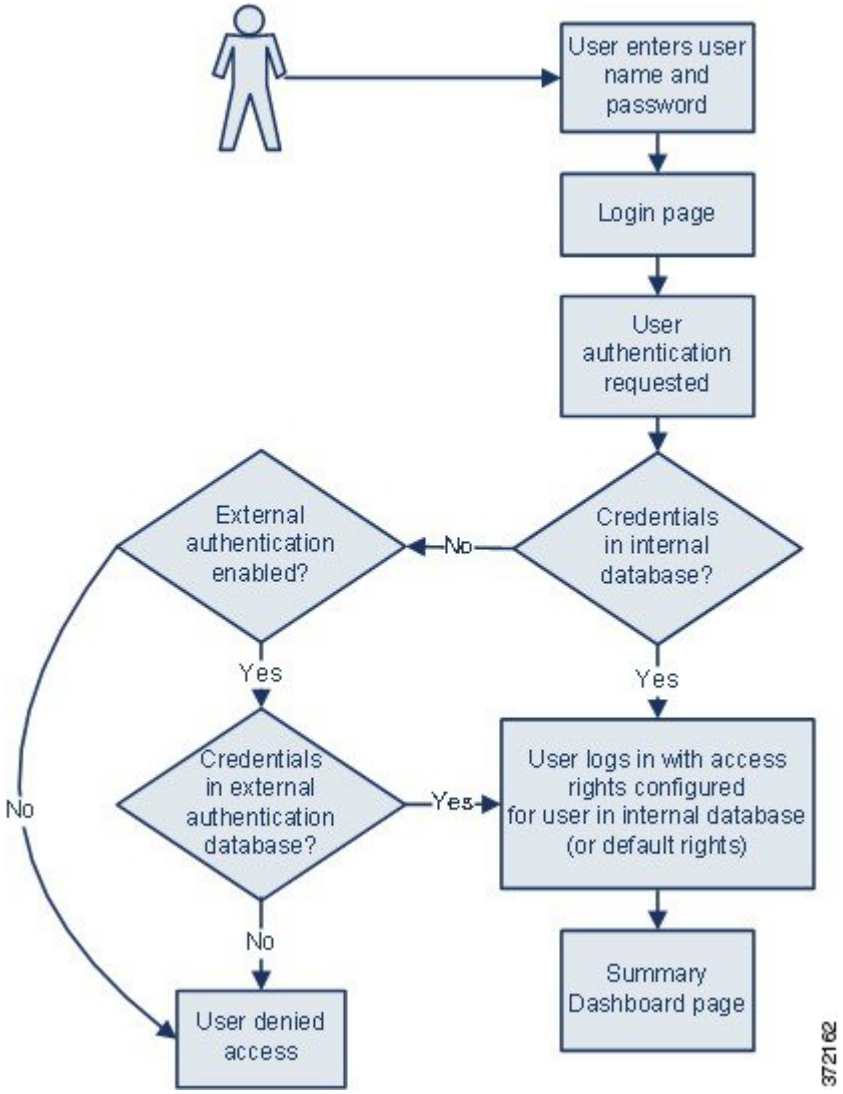
Firepower システムのユーザ認証

Firepower Management Center または管理対象デバイスでユーザが Web インターフェイスにログインすると、アプライアンスがローカルのユーザ リストでユーザ名とパスワードに一致するものを検索します。このプロセスは認証と呼ばれます。

認証には次の 2 種類あります。

- 内部認証：システムはユーザについてローカル データベースのリストを確認します。
- 外部認証：システムはユーザについてローカルデータベースのリストを確認し、そのリストにユーザが存在しない場合は、そのユーザ リストを外部認証サーバに照会します。

認証プロセスは、次のとおりです。



ユーザアカウントを作成する場合は、そのユーザに対して内部認証または外部認証を指定します。

内部認証

内部認証では、ユーザ クレデンシャルは、内部 Firepower システムのデータベースのレコードに照らして検証されます。これがデフォルトの認証タイプです。

ユーザのアカウントを作成する際に、内部認証のユーザにアクセス権を設定します。

（注） 内部認証ユーザが外部認証に変換された場合、内部認証に戻すことはできません。

外部認証（External Authentication）

外部認証では、Firepower Management Center または管理対象デバイスによって、外部サーバのリポジトリからユーザ クレデンシャルが取得されます。外部サーバは、Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバまたは Remote Authentication Dial In User Service（RADIUS）認証サーバにすることができます。

プラットフォーム設定ポリシーおよび個別のユーザアカウントの設定で外部認証を有効にします。アプライアンスに対して使用できる外部認証形式は 1 つだけです。

ユーザがアプライアンスに初めてログインすると、アプライアンスは、ローカルユーザ レコードを作成して、これらの外部クレデンシャルを一連のアクセス許可に関連付けます。ユーザには、次のいずれかに基づいて権限が割り当てられます。

- 属するグループまたはアクセス リスト
- アプライアンスのプラットフォーム設定ポリシーで設定したデフォルトのユーザアクセス ロール

権限がグループまたはリストのメンバーシップによって付与される場合は、権限を変更できません。ただし、デフォルトのユーザ ロールによって割り当てられている場合は、ユーザ アカウントで変更でき、この変更でデフォルトの設定がオーバーライドされます。次に例を示します。

- 外部認証ユーザ アカウントのデフォルト ロールとして特定のアクセス ロールが設定されている場合、ユーザは外部アカウント クレデンシャルを使用してアプライアンスにログインでき、この際にシステム管理者による追加の設定は必要ありません。
- アカウントが外部で認証され、デフォルトではアクセス権限が付与されない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザ（またはシステム管理者）は、ユーザ機能へ適切なアクセス権を付与する権限を変更することができます。

Firepower システム インターフェイスでは、外部認証ユーザのパスワード管理および外部認証ユーザの非アクティブ化は実行できません。外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの Firepower システム ユーザ管理ページでは、最小アクセス権を削除することができません。外部認証ユーザの [ユーザの編集（Edit User）] ページでは、外部認証サーバの設定により付与された権限は、[外部変更済み（Externally Modified）] ステータスでマークされます。

ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] カラムに、[外部：ローカルで変更済み（External - Locally Modified）] というステータスが表示されます。

関連トピック

LDAP 認証 （51 ページ）
RADIUS 認証 （78 ページ）

LDAP 認証

LDAP（Lightweight Directory Access Protocol）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

LDAP 認証オブジェクトは Firepower Management Center 上に作成する必要がありますが、Web インターフェイスを備えた管理対象デバイス（つまり、7000 および 8000 シリーズ デバイス）であればどれでも、オブジェクトを有効にするプラットフォーム設定ポリシーをそのデバイスに導入することで、外部認証オブジェクトを使用できます。ポリシーを導入すると、オブジェクトがデバイスにコピーされます。

（注） 7000 および 8000 シリーズ デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザまたは CLI ユーザをすべて削除してください。

LDAP 命名標準は、アドレスの指定と、認証オブジェクトのフィルタおよび属性の構文に使用できることに注意してください。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

（注） 現在 Firepower システムでは、Microsoft Active Directory on Windows Server 2008、Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0、OpenLDAP on Linux が稼働する LDAP サーバでの LDAP 外部認証がサポートされています。ただし、Firepower システムでは NGIPSv または ASA FirePOWER デバイスの外部認証はサポートされていません。

LDAP 認証オブジェクトを作成するために必要な情報

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトを作成するのに必要な情報を収集する必要があります。

（注） ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認する必要があります。

基本的な認証オブジェクトを作成するには、少なくとも以下が必要です。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバ タイプ
- LDAP ツリーを参照できる十分な権限が付与されているユーザ アカウントのユーザ名とパスワード。シスコはこの目的でドメイン管理ユーザのアカウントを使用することを推奨します。
- アプライアンスと LDAP サーバの間にファイアウォールがある場合、発信接続を許可するファイアウォールの項目
- ユーザ名が存在するサーバ ディレクトリのベース識別名（可能な場合）

ヒント サードパーティの LDAP クライアントを使用して、LDAP ツリーを参照し、ベース DN と属性の説明を確認できます。またそのクライアントを使用して、選択したユーザが、選択したベース DN を参照できることを確認することもできます。LDAP 管理者に連絡し、ご使用の LDAP サーバ向けの推奨される認定 LDAP クライアントを確認してください。

詳細な LDAP 認証オブジェクト設定をどのようにカスタマイズするかによって、次の表に示す情報が必要となることがあります。

表 *11 :* 追加の *LDAP* 設定情報

目的	必要な項目
389 以外のポートを介した接続	ポート番号
暗号化接続を使用した接続	接続の証明書
属性値に基づいてアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
ユーザ識別名を検査するのではなく、属性を UI アクセス属性として使用する	属性の名前
ユーザ識別名を検査するのではなく、属性をシェル ログイン属性として使用する	属性の名前
属性値に基づいてシェルを介してアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア

目的	必要な項目
特定のユーザ ロールへのグループの関連付け	各グループの識別名、およびグループがスタティック グループの場合はグループ メンバー属性、グループがダイナミック グループの場合はグループ メンバーの URL 属性
認証用および承認用に使用する CAC	CAC。CAC を発行したのと同じ CA によって署名されたサーバ証明書、両方の証明書の証明書チェーン

CAC 認証

部門で共通アクセス カード（CAC）が使用される場合は、Web インターフェイスにログインするユーザを認証し、グループ メンバーシップまたはデフォルト アクセス権に基づいて特定機能へのアクセスを許可するように、LDAP認証を設定できます。CAC認証および認可が設定されている場合、ユーザは、アプライアンスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。

（注） CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡されるサーバ証明書）が存在している**必要があります**。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたってCAC接続を維持する**必要があります**。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。

システムでは、CAC 認証ユーザは Electronic Data Interchange Personal Identifier（EDIPI）番号により識別されます。ユーザが CAC クレデンシャルを使用して初めてログインした後で、[ユーザ管理（User Management）] ページでのこれらのユーザのアクセス権限を手動で追加または削除できます。グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、プラットフォーム設定ポリシーでデフォルトで付与される権限だけが与えられています。

ヒント 操作が行われない状態で 24 時間が経過すると、システムによって [ユーザ管理（User Management）] ページから CAC 認証ユーザを消去されるときに、手動で設定されたアクセス権限が削除されることに注意してください。その後ユーザがログインするたびに、ユーザがページに復元されますが、ユーザのアクセス権限に対する手動での変更はすべて再設定する必要があります。

CAC 認証の設定

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）	任意（Any）	7000 および 8000 シリーズ	任意（Any）	Admin/Network Admin

ネットワークのユーザが各自の CAC クレデンシャルを使用して Firepower Management Center および 7000 および 8000 シリーズ デバイスにログインする前に、適切なアクセス許可を持つユーザが、CAC 認証および認可のマルチステップ設定プロセスを完了しておく必要があります。

始める前に

- LDAP 認証オブジェクトを作成するために必要な情報 （51 ページ）の説明に従って情報を収集します。

手順

ステップ 1 組織の指示に従い CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` を開きます（hostname はご使用の Firepower Management Center のホスト名に対応しています）。

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 ログインページで、[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、管理者権限を持つユーザとしてログインします。ユーザ名では、大文字と小文字が区別されます。

ヒント CAC 認証および認可の設定が完了するまで、CAC クレデンシャルを使用したログインは**できません**。

ステップ 6 **[システム（System）]** > **[ユーザ（Users）]** に移動し、[外部認証（External Authentication）] タブをクリックします。

ステップ 7 および拡張 LDAP 認証オブジェクトの作成 （58 ページ）の手順に従い、CAC 認証および認可専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- [LDAP 固有パラメータ（LDAP-Specific Parameters）] セクションの詳細設定オプションの [ユーザ名テンプレート（User Name Template）]。
- [属性マッピング（Attribute Mapping）] セクションの [UI アクセス属性（UI Access Attribute）]。

- [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションの既存の LDAP グループの識別名（LDP グループ メンバーシップによってアクセス権を事前に設定する場合）。

ヒント 同一認証オブジェクトで CAC 認証とシェル アクセスの両方を設定**できない**ことに注意してください。また、ユーザにシェルアクセスを許可する場合は、個別の認証オブジェクトを作成し、有効にします。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 外部認証の有効化の説明に従って、外部認証と CAC 認証を有効にします。

注意 設定変更を展開するまで変更は有効に**なりません**。

ステップ 10 **[システム（System）]** > **[設定（Configuration）]** に移動し、[HTTPS 証明書（HTTPS Certificate）] をクリックします。

ステップ 11 HTTPS サーバ証明書をインポートし、必要に応じて HTTPS サーバ証明書のインポート で説明する手順に従います。

（注） 認証および認可に使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局（CA）により発行される**必要があります**。

ステップ 12 [HTTPS ユーザ証明書設定（HTTPS User Certificate Settings）] の [ユーザ証明書を有効にする（Enable User Certificates）] を選択します。詳細については、有効な HTTPS クライアント証明書の強制を参照してください。

次のタスク

- ユーザが初めてログインした後、手動でユーザのアクセス権を追加または削除できます。権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。詳細については、ユーザ アカウントの編集 （41 ページ）を参照してください。

関連トピック

LDAP グループ フィールド （70 ページ）
LDAP 固有フィールド （64 ページ）
CAC クレデンシャルを使用した管理対象デバイスへのログイン
CAC クレデンシャルを使用した Firepower Management Center へのログイン

基本 LDAP 認証オブジェクトの作成

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）	任意（Any）	任意（Any）	任意（Any）	Admin

LDAP 認証オブジェクトをセットアップできます。LDAP 認証オブジェクトでは多くの値をカスタマイズします。ただし、特定ディレクトリ内のすべてのユーザを認証するだけの場合は、そのディレクトリのベース DN を使用して基本認証オブジェクトを作成できます。ご使用のサーバ タイプでベース DN のデフォルトを設定し、サーバからユーザ データを取得するために使用するアカウントの認証クレデンシャルを指定すれば、認証オブジェクトを簡単に作成できます。このためには、次の手順に従います。

（注） （たとえば、シェルアクセスを付与するために）認証オブジェクトを作成するときに、各認証設定を検討してカスタマイズする場合は、高度な手順を使用してオブジェクトを作成します。サーバへの接続の暗号化、ユーザ タイムアウトの設定、ユーザ名テンプレートのカスタマイズ、または LDAP グループ メンバーシップに基づく Firepower システム ユーザ ロールの割り当てを行う場合にも、この高度な手順を使用してください。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

始める前に

- LDAP 認証オブジェクトを作成するために必要な情報 （51 ページ）の説明に従って情報を収集します。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウンリストから [LDAP] を選択します。

ステップ 5 LDAP 認証サーバの特定 （63 ページ）の説明に従って、[名前（Name）]、[説明（Description）]、[サーバ タイプ（Server Type）]、[プライマリ サーバ ホスト名/IP アドレス（Primary Server Host Name/IP Address）] を入力します。

ヒント [デフォルトの設定（Set Defaults）] をクリックすると、システムにより、[ユーザ名テンプレート（User Name Template）]、[UI アクセス属性（UI Access Attribute）]、[シェル アクセス属性（Shell Access Attribute）]、[グループ メンバ属性（Group Member Attribute）]、[グループ メンバ URL 属性（Group Member URL Attribute）] フィールドにデフォルト値が設定されます。

ステップ 6 LDAP 固有パラメータの設定 （68 ページ）の説明に従って、[DN の取得（Fetch DNs）] を選択して基本識別名を指定し、オプションで [基本フィルタ（Base Filter）] に入力します。

ステップ 7 LDAP 固有パラメータの設定 （68 ページ）の説明に従って、[ユーザ名（User Name）] として識別名を入力し、LDAP サーバを参照するための十分なクレデンシャルを持っているユーザの [パスワード（Password）] を入力します。

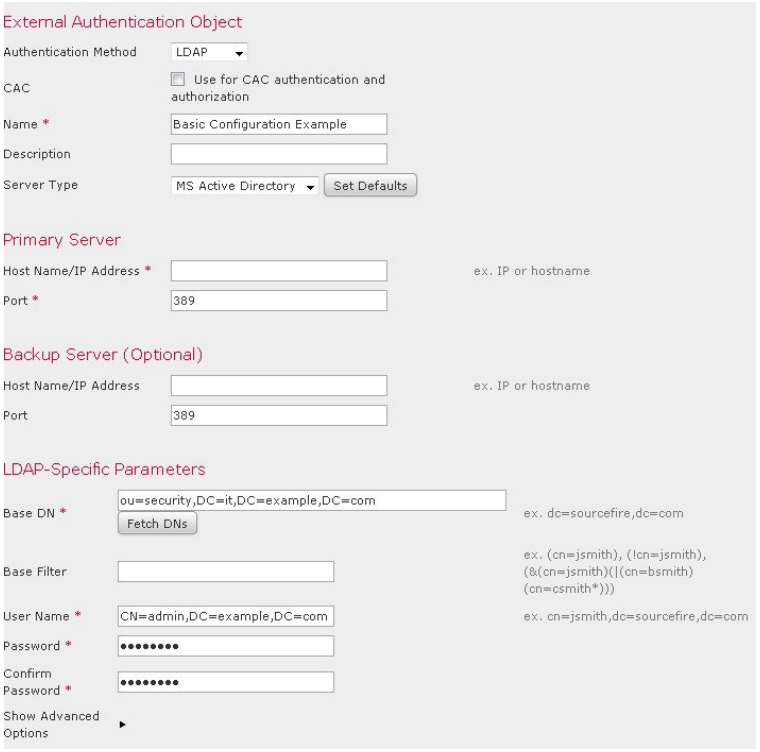
ステップ 8 [パスワードの確認（Confirm Password）] フィールドに、パスワードを再度入力します。

ステップ 9 LDAP 認証接続のテスト （75 ページ）の説明に従って、接続をテストします。

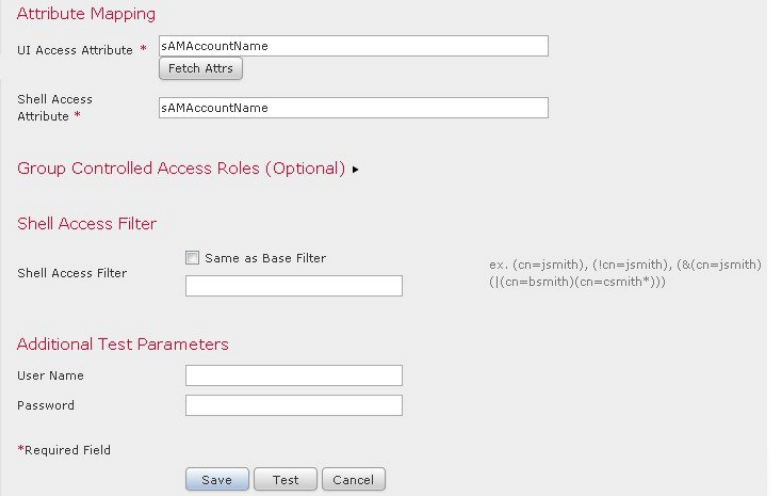
ステップ 10 [保存（Save）] をクリックします。

例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。



ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェル アクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスでシェル アカウントまたは CLI アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、Firepower システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

次のタスク

- LDAP 認証を有効にするには、外部認証の有効化の説明に従って、認証オブジェクトを有効にします。
- 取得されるユーザのリストを絞り込む場合の詳細は、LDAP 認証接続のトラブルシューティング （76 ページ）を参照してください。

拡張 LDAP 認証オブジェクトの作成

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）	任意（Any）	任意（Any）	任意（Any）	Admin

基本認証オブジェクトの作成時に、認証サーバに接続できるようにする基本設定を定義します。拡張認証オブジェクトを作成する場合は、基本設定を定義し、サーバからユーザデータを取得するために使用するディレクトリ コンテキストおよび検索条件も選択します。オプションで、シェル アクセス認証を設定できます。

ご使用のサーバ タイプのデフォルト設定を使用して LDAP 設定を迅速にセットアップできますが、詳細設定をカスタマイズして、アプライアンスから LDAP サーバに暗号化接続するかどうか、接続のタイムアウト、およびサーバがユーザ情報を検査する属性を制御することもできます。

LDAP 固有のパラメータの場合、LDAP 命名基準とフィルタおよび属性のシンタックスを使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定シンタックスを使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Server を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

（注） CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後は、CAC が常に挿入された状態にしておく**必要があります**。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

始める前に

- LDAP 認証オブジェクトを作成するために必要な情報 （51 ページ）の説明に従って情報を収集します。
- シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除します。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。
ステップ 2 [外部認証（External Authentication）] タブをクリックします。
ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。
ステップ 4 LDAP 認証サーバの特定 （63 ページ）の説明に従って、認証サーバを指定します。
ステップ 5 LDAP 固有パラメータの設定 （68 ページ）の説明に従って、認証設定を行います。
ステップ 6 オプションで、グループによるアクセス権の設定 （71 ページ）の説明に従って、デフォルト アクセス ロール割り当ての基準として使用する LDAP グループを設定します。

ヒント CAC 認証および認可にこのオブジェクトを使用する予定の場合、Cisco としてはアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。

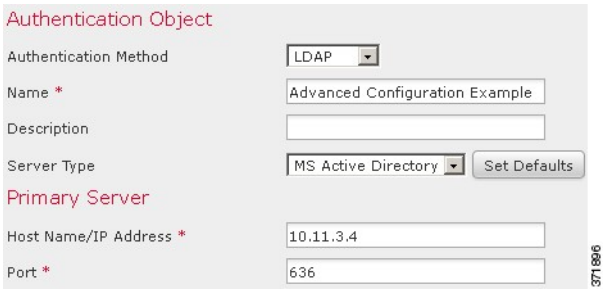
ステップ 7 オプションで、LDAP シェル アクセスの設定 （73 ページ）の説明に従って、シェル アクセスの認証設定を行います。

ステップ 8 LDAP 認証接続のテスト （75 ページ）の説明に従って、設定をテストします。

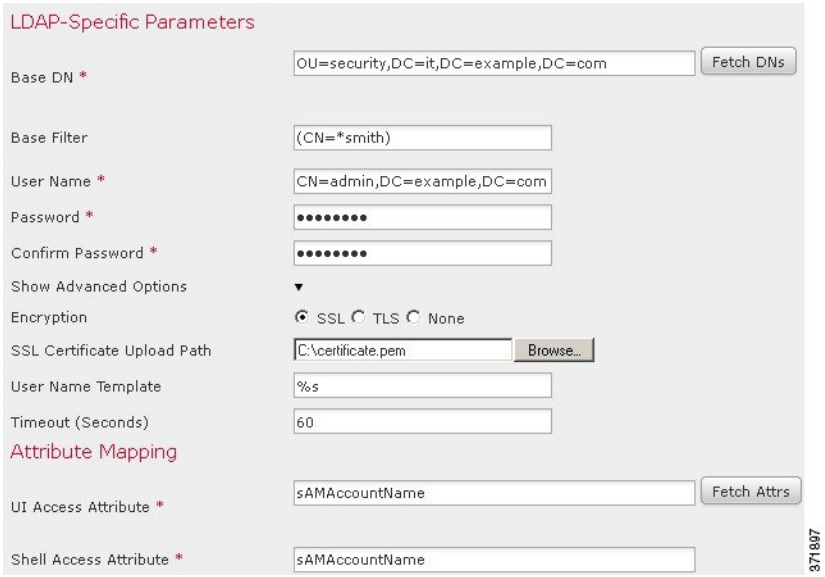
ステップ 9 [保存（Save）] をクリックします。

例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。ただし、このサーバに基本フィルタ `(cn=*smith)` が設定されていることに注意してください。このフィルタは、サーバから取得するユーザを、一般名が `smith` で終わるユーザに限定します。

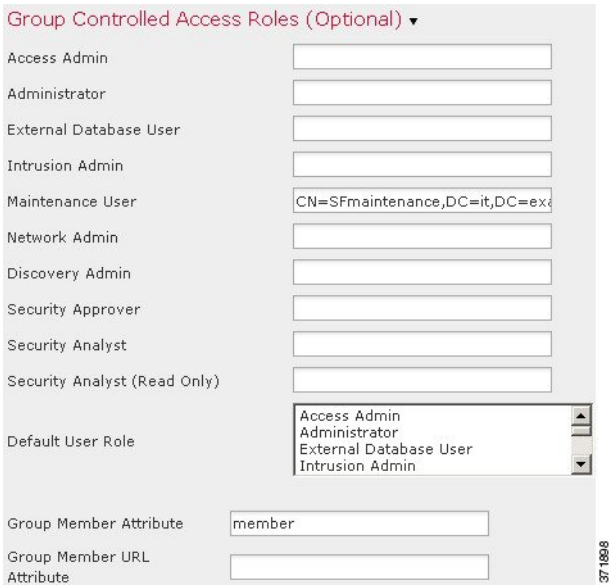


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（Timeout）] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

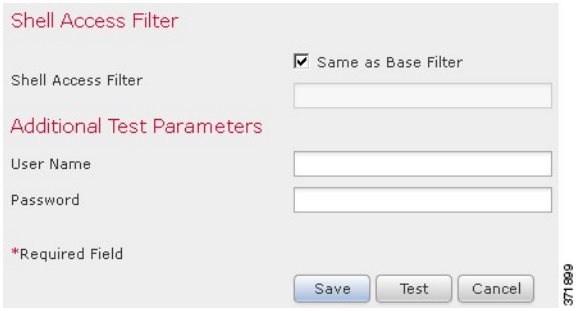
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。設定では、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` であることに注意してください。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェル アクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスでシェル アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。[メンテナンス ユーザ（Maintenance User）] ロールが、`member` グループ属性を持ち、ベース ドメイン名が `CN=SFmaintenance,=it,=example,=com` であるグループのすべてのメンバーに自動的に割り当てられます。



シェル アクセス フィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルまたは CLI を介してアプライアンスにアクセスできます。



次のタスク

- LDAP 認証を有効にするには、外部認証の有効化で認証オブジェクトを有効化します。

LDAP 認証サーバのフィールド

CAC

認証および許可に CAC を使用するには、このチェックボックスをオンにします。

[名前（Name）]

認証サーバの名前。

説明

認証サーバの説明。

サーバ タイプ（Server Type）

接続する LDAP サーバのタイプ。タイプを選択する際には、次のオプションから選択できます。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択します。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択します。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択します。
- 上記のサーバ以外の LDAP サーバに接続し、デフォルト設定をクリアする場合は、[その他（Other）] を選択します。

ヒント [デフォルトにセット（Set Defaults）] をクリックすると、[ユーザ名テンプレート（User Name Template）]、[UI アクセス属性（UI Access Attribute）]、[シェル アクセス属性（Shell Access Attribute）]、[グループ メンバー属性（Group Member Attribute）]、および [グループ メンバー URL 属性（Group Member URL Attribute）] フィールドにデフォルト値が入力されます。

[プライマリ サーバのホスト名/IP アドレス（Primary Server Host Name/IP Address）]

認証データを取得するプライマリ サーバの IP アドレスまたはホスト名。

（注） 証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

[プライマリ サーバのポート（Primary Server Port）]

プライマリ認証サーバで使用されるポート。

[バックアップ サーバのホスト名/IP アドレス（Backup Server Host Name/IP Address）]

認証データを取得するバックアップ サーバの IP アドレスまたはホスト名。

[バックアップサーバポート（Backup Server Port）]

バックアップ認証サーバで使用されるポート。

LDAP 認証サーバの特定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

認証オブジェクトの作成時には、管理対象デバイスまたは Firepower Management Center が認証のために接続する、プライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

（注） CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後は、CAC が常に挿入された状態にしておく**必要があります**。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウンリストから [LDAP] を選択します。

ステップ 5 オプションで、CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

（注） CAC 認証および認可を完全に設定するには、CAC 認証の設定 （54 ページ）の手順に従う必要があります。

ステップ 6 [名前（Name）] フィールドと [説明（Description）] フィールドに、認証サーバの名前と説明を入力します。

ステップ 7 ドロップダウンリストから [サーバ タイプ（Server Type）] を選択します。詳細については、LDAP 認証サーバのフィールド （62 ページ）を参照してください。必要に応じて、[デフォルトの設定（Set Defaults）] をクリックします。

ステップ 8 [プライマリ サーバのホスト名または IP アドレス（Primary Server Host Name/IP Address）] を入力します。

（注） 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 9 必要に応じて、[プライマリ サーバ ポート（Primary Server Port）] を入力します。

ステップ 10 必要に応じて、[バックアップ サーバのホスト名または IP アドレス（Backup Server Host Name/IP Address）] を入力します。

ステップ 11 必要に応じて、[バックアップ サーバ ポート（Backup Server Port）] を入力します。

次のタスク

- LDAP 認証オブジェクトの作成を続行します。詳細については、拡張 LDAP 認証オブジェクトの作成 （58 ページ）を参照してください。

LDAP 固有フィールド

次の表で、各 LDAP 固有パラメータについて説明します。

表 *12 : LDAP* 固有パラメータ

設定	説明	例
ベース DN（Base DN）	アプライアンスがユーザ情報を検索する LDAP サーバのディレクトリのベース識別名を指定します。 通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。 プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。	Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。
[基本フィルタ（Base Filter）]	ベース DN でフィルタに設定されている特定の属性と値のペアを含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは、カッコ内に囲まれるフィルタとして使用する属性タイプ、比較演算子、および属性値です。	F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。
[ユーザ名（User Name）]/[パスワード（Password）]	ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにします。取得する認証オブジェクトに対する適切な権限を持つユーザのユーザ資格情報を指定します。指定するユーザの識別名は、LDAP サーバのディレクトリ情報ツリーで一意である必要があります。Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはなりません。	Example 社のセキュリティ（Security）部門の `admin` ユーザのユーザ名は、`cn=admin, ou=security, dc=example,dc=com` となります。

設定	説明	例
暗号化（Encryption）	通信が暗号化されるかどうかと、暗号化方法を示します。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。TLS または SSL 経由で接続するときに認証に証明書を使用する場合、証明書の LDAP サーバ名が、指定する**ユーザ名**と一致している**必要がある**ことに注意してください。 ポートを指定した後で暗号化方式を変更すると、ポートが、選択されているサーバタイプのデフォルト値にリセットされます。	外部認証の設定に `10.10.10.250` を、証明書に `computer1. example.com` を入力すると、`computer1. example.com` に IP アドレス `10.10.10.250` がある場合であっても、接続に失敗します。外部認証設定のサーバ名を `computer1. example.com` に変更すると、接続が正常に行われます。
[SSL 証明書アップロード パス（SSL Certificate Upload Path）]	ローカル コンピュータで、暗号化に使用する証明書のパスを指定します。	`c:/server.crt`
[ユーザ名テンプレート（User Name Template）]	文字列変換文字（`%s`）をユーザの [UI アクセス属性（UI Access Attribute）] の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定します。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、アプライアンスにより文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ資格情報の検索に使用されます。 CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート（User Name Template）] に入力する**必要があります**。	`%s@security.example.com`, `%s@mail.com`, `%s@mil`, `%s@smil.mil`,

設定	説明	例
Timeout	プライマリ サーバへの接続試行のタイムアウトを設定します。これにより、接続がバックアップ サーバにロールオーバーされます。プライマリ認証サーバからの応答がない状態でこのフィールドに示されている秒数（またはLDAPサーバのタイムアウト）が経過すると、アプライアンスはバックアップサーバに対してクエリを実行します。 ただしLDAPがプライマリ LDAPサーバのポートで実行されており、何らかの理由で要求の処理を拒否する場合は、バックアップサーバへのフェールオーバーは行われません。	プライマリ サーバでLDAPが無効な場合、アプライアンスはバックアップサーバに対してクエリを実行します。
[UI アクセス属性（UI Access Attribute）]	ローカルアプライアンスに対し、ユーザ識別名の値ではなく、特定の属性の値の照合を行うように指示します。Firepower システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。 サーバタイプを選択し、デフォルトを設定すると、[UI アクセス属性（UI Access Attribute）] に、そのサーバ タイプに適した値が取り込まれます。 このフィールドを空白のままにすると、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードのユーザ識別名値を調べ、ユーザ名に一致しているかどうかを確認します。 CAC認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート（User Name Template）] の値に対応する値を入力する**必要があります**。	`sAMAccountName`, `userPrincipalName`, メール アドレス

LDAP 固有パラメータの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

LDAP 固有パラメータ セクションの設定により、アプライアンスがユーザ名を検索する LDAP ディレクトリの領域が決定され、アプライアンスから LDAP サーバへの接続の詳細が制御されます。

有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。

ほとんどの LDAP 固有設定の他に、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定シンタックスを使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Server を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

（注） CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく**必要があります**。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページの [LDAP 固有パラメータ（LDAP-Specific Parameters）] セクションには、ベース DN を設定する 2 つのオプションがあります。

- [DN の取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。
- アクセスする LDAP ディレクトリのベース識別名を [ベース DN（Base DN）] フィールドに入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。

ステップ 2 必要に応じて、[基本フィルタ（Base Filter）] を入力します。

例：

たとえば、ディレクトリ ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、

New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

ステップ 3 LDAP サーバを参照する十分なクレデンシャルがあるユーザの [ユーザ名（User Name）] として識別名と、[パスワード（Password）] を入力します。

例：

たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

注意 Microsoft Active Directory Server に接続する場合は、末尾の文字が `$` のサーバ ユーザ名は指定できません。

ステップ 4 [パスワードの確認（Confirm Password）] フィールドに、パスワードを再度入力します。

ステップ 5 基本的な LDAP 固有パラメータの設定後に行う手順には、いくつかの選択肢があります。

- 詳細オプションにアクセスするには、[詳細オプションを表示（Show Advanced Options）] の横の矢印をクリックし、次のステップに進みます。
- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定 （71 ページ）に進みます。
- 認証に LDAP グループを使用しない場合は、LDAP シェル アクセスの設定 （73 ページ）に進みます。

ステップ 6 必要に応じて、LDAP 接続に [暗号化（Encryption）] モードを選択します。

（注） ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされることに注意してください。[なし（None）] または [TLS] の場合、ポートはデフォルト値 389 を使用します。SSL 暗号化を選択した場合は、ポートはデフォルト値 636 を使用します。

ステップ 7 TLS または SSL が暗号化を選択し、認証に証明書を使用する場合は、有効な TLS または SSL 証明書の場所を**参照**します。

（注） 以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をアプライアンスに再展開して、新しい証明書を上書きコピーします。

ステップ 8 必要に応じて、[UI アクセス属性（UI Access Attribute）] に対応する [ユーザ名テンプレート（User Name Template）] を指定します。

例：

たとえば、UI アクセス属性が `uid` である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート（User Name Template）] フィールドに `uid=%s,ou=security,dc=example,dc=com` と入力します。Microsoft Active Directory Server の場合は `%s@security.example.com` と入力します。

（注） 認証および認可に CAC 資格情報を使用するには、[ユーザ名テンプレート（User Name Template）] フィールドに値を入力する**必要があります**。

ステップ 9 オプションで、バックアップ接続にロールオーバーするまでの経過秒数を [タイムアウト（Timeout）] フィールドに入力します。

ステップ 10 オプションで、ベース DN および基本フィルタの代わりに属性に基づいてユーザを取得する場合、2 つのオプションがあります。

- [属性を取得（Fetch Attrs）] をクリックして使用可能な属性のリストを取得し、適切な属性を選択します。
- [UI アクセス属性（UI Access Attribute）] を入力します。たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに `uid` 属性がないため、[UI アクセス属性（UI Access Attribute）] を使用してユーザを取得することがあります。代わりに [UI アクセス属性（UI Access Attribute）] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

（注） 認証および認可に CAC 資格情報を使用するには、[UI アクセス属性（UI Access Attribute）] フィールドに値を入力する**必要があります**。

次のタスク

- 拡張 LDAP 認証オブジェクトの作成 （58 ページ）の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

LDAP グループ フィールド

参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ユーザが Firepower システムにログインするときに付与されるアクセス権は、LDAP 構成によって異なります。

- LDAP サーバでグループ アクセス権が設定されていない場合、新しいユーザがログインすると、Firepower システムはそのユーザを LDAP サーバに対して認証し、プラットフォーム設定ポリシーに設定されているデフォルトの最小アクセス ロールに基づいてユーザ権限を付与します。
- グループ設定を設定すると、指定されたグループに属している新しいユーザは、メンバーとなっているグループの最小アクセス設定を継承します。
- 新しいユーザが指定のどのグループにも属していない場合は、認証オブジェクトの [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションに指定されているデフォルトの最小アクセス ロールが割り当てられます。
- 設定されている複数のグループにユーザが属している場合、ユーザは最も高いアクセスを持つグループのアクセス ロールを最小アクセス ロールとして受け取ります。

Firepower システム ユーザ管理ページでは、LDAP グループ メンバーシップによってアクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] カラムに、[外部 - ローカルで変更済み（External - Locally Modified）] というステータスが表示されます。

（注） ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されている通りに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、Firepower システムでは検索の再帰回数が 4 回に制限されています。この再帰回数内でユーザのグループ メンバーシップが確立されない場合、[グループ制御アクセス ロール（Group Controlled Access Roles）] セクションで定義されているデフォルト アクセス ロールがユーザに付与されます。

[Firepower システムのユーザ権限（Firepower System User Roles）]

各ユーザ ロールを割り当てる必要があるユーザを含む LDAP グループの識別名。

[デフォルトのユーザ ロール（Default User Role）]

指定したグループのいずれにも属していないユーザのデフォルトの最小アクセス。

[グループ メンバーの属性（Group Member Attribute）]

スタティック グループに LDAP 検索文字列を含む LDAP 属性。

[グループ メンバーの URL 属性（Group Member URL Attribute）]

ダイナミック グループのメンバーシップを指定する LDAP 属性。

グループによるアクセス権の設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、Firepower システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、Firepower システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてデフォルト アクセス権を割り当てます。

グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、プラットフォーム設定ポリシーでデフォルトで付与される権限だけが与えられています。

CAC 認証および認可にオブジェクトを使用する予定の場合、CAC 認証ユーザへのアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。

（注） CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく**必要があります**。

始める前に

- 参照する予定のグループが LDAP サーバに存在することを確認します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、[グループ制御アクセス ロール（Group Controlled Access Roles）] の横の下矢印をクリックします。

ステップ 2 必要に応じて、Firepower システム ユーザ ロールに対応する [DN] フィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

例：

たとえば、`Example` 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[管理者（Administrator）] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

ステップ 3 [デフォルト ユーザ ロール（Default User Role）] を選択します。

ステップ 4 スタティック グループを使用する場合は、[グループ メンバー属性（Group Member Attribute）] を入力します。

例：

たとえば、デフォルトの Security Analyst アクセスのために参照するスタティック グループのメンバーシップを示すために `member` 属性を使用する場合は、`member` と入力します。

ステップ 5 ダイナミック グループを使用する場合は、[グループ メンバー URL 属性（Group Member URL Attribute）] を入力します。

例：

たとえば、デフォルトの Admin アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

次のタスク

- 拡張 LDAP 認証オブジェクトの作成 （58 ページ）の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

LDAP シェル アクセスのフィールド

adminアカウントを除き、シェルアクセスは設定したシェルアクセス属性によって完全に制御されます。設定するシェル アクセス フィルタにより、シェルにログインできる LDAP サーバのユーザが決定します。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェルアクセスユーザアカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホームディレクトリを使用してシェルがリセットされます。

シェルユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

[シェル アクセス属性（Shell Access Attribute）]

ユーザがフィルタリング用に使用するアクセス属性です。シェルアクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。

このフィールドを空白のままにした場合、シェルアクセス認証にはユーザ識別名が使用されます。

ヒント　サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した属性がこのフィールドに事前に取り込まれます。

[シェル アクセス フィルタ（Shell Access Filter）]

シェル アクセス用の管理ユーザのエントリを取得するために使用する属性値です。フィルタは、属性名、比較演算子、および属性値です。

[ベース フィルタと同じ（Same as Base Filter）] チェックボックスを使用すると、ベース DN で限定されるすべてのユーザが、シェルアクセス権限でも限定される場合に、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。シェル アクセス フィルタが基本フィルタと同一である場合は、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。[ベース フィルタと同じ（Same as Base Filter）] オプションを使用すると、この両方の目的でクエリを 1 回だけ実行することができます。

このフィールドを空白のままにすると、シェル アクセスの LDAP 認証が回避されます。

LDAP シェル アクセスの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

LDAP サーバを使用して、管理対象デバイスまたは Firepower Management Center でシェル アクセス用のアカウントを認証できます。シェルアクセスを付与するユーザの項目を取得する検索フィルタを指定します。

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。代わりに、別の認証オブジェクトを作成し、有効にします。

シェル アクセスの認証オブジェクトは、Firepower Management Center の最初の認証オブジェクトである必要があります。

シスコは、NGIPSv デバイスまたは ASA FirePOWER デバイスの外部認証をサポートしていません。さらに、シェル アクセス認証では IPv6 がサポートされていません。

⚠

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。Firepower Management Center で追加のシェル ユーザを設定しないことをお勧めします。

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。[CAC] チェックボックスをオンにすると、そのページのシェル アクセス設定のオプションが無効になります。代わりに、別の認証オブジェクトを作成し、有効にします。

始める前に

- シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証 CLI またはシェル ユーザを削除します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、ユーザ識別以外のシェル アクセス属性を使用する場合は、[シェル アクセス属性（Shell Access Attribute）] に入力します。

例：

たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性（Shell Access Attribute）] フィールドに `sAMAccountName` と入力します。

ステップ 2 シェル アクセス アカウント フィルタを設定します。次の複数のオプションがあります。

- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで [シェル アクセス フィルタ（Shell Access Filter）] フィールドに入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。

次のタスク

- 拡張 LDAP 認証オブジェクトの作成 （58 ページ）の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

LDAP 認証接続のテスト

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）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

LDAP サーバを設定し、認証設定を行ったら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

[ユーザ名（User Name）] にテストに使用するユーザの `uid` 属性の値を入力できます。Microsoft Active Directory Server に接続して `uid` の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

同じユーザのパスワードを使用します。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。

Web インターフェイスのページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。最初に、追加のテストパラメータを使用せずにサーバ設定をテストします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

手順

ステップ 1 [外部認証オブジェクトの追加（Add External Authentication Object）] ページで、[ユーザ名（User Name）] と [パスワード（Password）] を入力します。

例：

たとえば、Example 社のユーザ `JSmith` の資格情報を取得できるかどうかをテストするには、「`JSmith`」および「`password`」を入力します。

ステップ 2 [テスト（Test）] をクリックします。次の 2 つの対処法があります。

- テストが成功した場合、テストの出力がページ下部に表示されます。[保存（Save）] をクリックします。
- テストが失敗した場合は、接続のトラブルシューティングの提案事項について、LDAP 認証接続のトラブルシューティング （76 ページ）を参照してください。

次のタスク

- LDAP 認証を有効にするには、外部認証の有効化の説明に従って、認証オブジェクトを有効にします。

LDAP 認証接続のトラブルシューティング

LDAP 認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- 画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
  - サードパーティの LDAP ブラウザを使用して LDAP サーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
  - ユーザ名が、LDAP サーバのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティ アプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
  - サーバの IP アドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
  - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
  - 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。

- シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。
- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。

- ベース識別名を入力した場合は、[DN を取得（Fetch DNs）] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタがカッコで囲まれており、有効な比較演算子を使用していることを確認します。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書の LDAP サーバの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テストユーザを使用する場合、ユーザ資格情報を削除してオブジェクトをテストします。
- 次の構文を使用して、接続するアプライアンスでコマンド ラインから LDAP サーバに接続し、使用するクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、`domainadmin@myrtle.example.com` ユーザと基本フィルタ (`cn=*`) を使用して `myrtle.example.com` のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、アプライアンスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

正常に接続されたが、接続で取得されたユーザ リストを調整する必要がある場合は、基本フィルタまたはシェル アクセス フィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。

RADIUS 認証

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

RADIUS サーバで認証されたユーザが初めてログインすると、認証オブジェクトでそのユーザに指定されている権限がユーザに付与されます。どのユーザ ロールにもリストされていないユーザには、認証オブジェクトで選択されているデフォルト アクセス権限が付与されます。認証オブジェクトでデフォルト アクセス権限が選択されていない場合は、プラットフォームの設定ポリシーに設定されているデフォルト アクセス権限が付与されます。設定が認証オブジェクトのユーザ リストを介して付与されていない場合は、必要に応じてユーザの権限を変更できます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

（注） 7000 または 8000 シリーズ デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証 CLI ユーザをすべて削除してください。

Firepower システムの RADIUS 実装では、SecurID® トークンの使用がサポートされています。SecurID を使用したサーバによる認証を設定すると、そのサーバに対して認証されているユーザが、SecurID PIN の末尾に SecurID トークンを付加し、Cisco システムへのログイン時にそれをパスワードとして使用します。SecurID が外部のユーザを認証するように適切に設定されている限り、これらのユーザは PIN と SecurID を使用して Firepower Management Center または 7000 または 8000 シリーズ デバイスにログインできるので、追加の設定は不要です。

RADIUS 認証オブジェクトの作成

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）	任意（Any）	任意（Any）	任意（Any）	Admin

RADIUS 認証オブジェクトの作成時に、認証サーバに接続できるようにする設定を定義します。また、特定のユーザおよびデフォルト ユーザにユーザ ロールを付与します。RADIUS サーバから、認証予定のユーザのカスタム属性が返される場合は、これらのカスタム属性を定義する必要があります。オプションで、CLI またはシェル アクセス認証も設定できます。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

始める前に

- ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。
ステップ 2 [外部認証（External Authentication）] タブをクリックします。
ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。
ステップ 4 [認証方式（Authentication Method）] ドロップダウン リストから [RADIUS] を選択します。
ステップ 5 RADIUS 接続の設定 （81 ページ）の説明に従って、認証サーバを指定します。
ステップ 6 RADIUS ユーザ ロールの設定 （83 ページ）の説明に従って、ユーザ ロールを設定します。
ステップ 7 オプションで、RADIUS シェル アクセスの設定 （85 ページ）の説明に従ってシェル アクセスを設定します。
ステップ 8 オプションで、カスタム RADIUS 属性の定義 （86 ページ）の説明に従ってカスタム属性を定義します。
ステップ 9 RADIUS 認証接続のテスト （87 ページ）の説明に従って、設定をテストします。

例

例

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

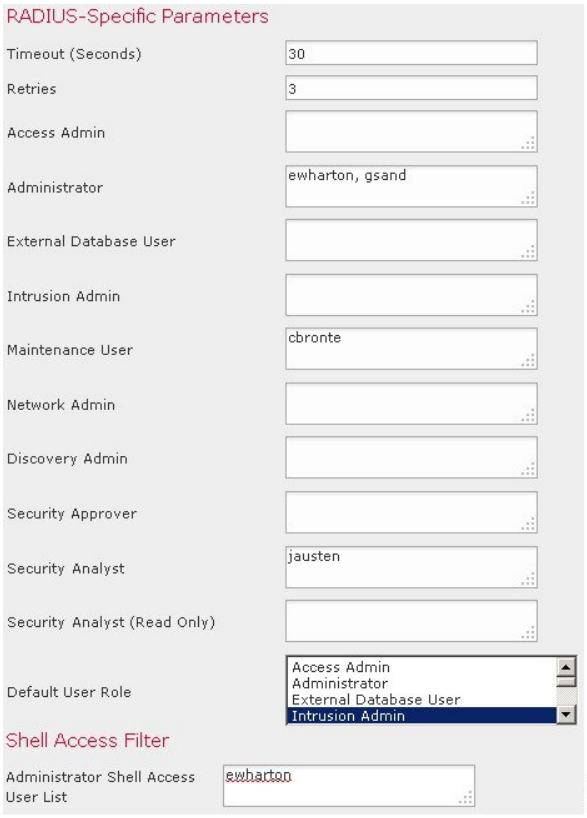
ユーザ `ewharton` と `gsand` には、この認証オブジェクトが有効になっているアプライアンスへの管理アクセスが付与されます。

ユーザ `cbronte` には、この認証オブジェクトが有効になっているアプライアンスへの [メンテナンス ユーザ（Maintenance User）] アクセスが付与されます。

ユーザ `cbronte` には、この認証オブジェクトが有効になっているアプライアンスへの [セキュリティ アナリスト（Security Analyst）] アクセスが付与されます。

ユーザ `ewharton` は、シェル アカウントを使用してアプライアンスにログインできます。

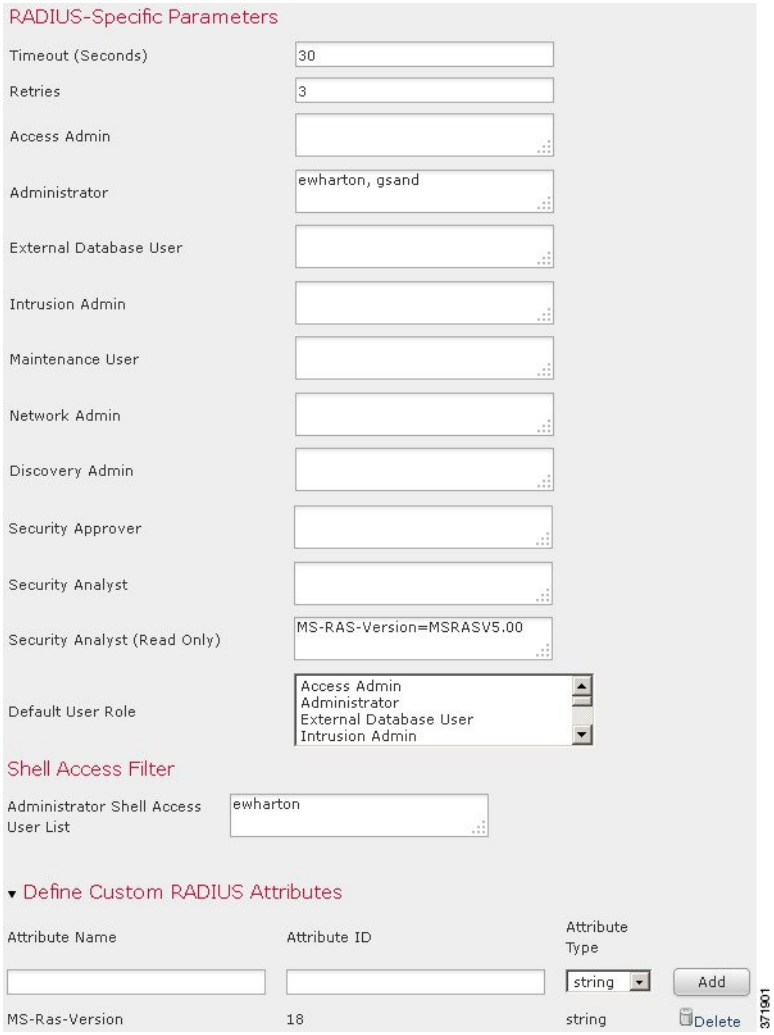
次の図に、この例のロール設定を示します。



属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバが使用されているため、1 人以上のユーザの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバ経由で RADIUS にログインするすべてのユーザに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



次のタスク

- RADIUS認証を有効にするには、外部認証の有効化の説明に従って認証オブジェクトを有効にします。

RADIUS 接続の設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

RADIUS認証オブジェクトの作成時には、ローカルアプライアンス（管理対象デバイスまたはFirepower Management Center）が認証のために接続するプライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

（注） RADIUSが正しく機能するためは、ファイアウォールで認証ポートとアカウンティング ポート（デフォルトでは 1812 および 1813）を開く必要があります。

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバからの応答がない状態で[タイムアウト（Timeout）] フィールド（またはLDAPサーバのタイムアウト）に指定された秒数が経過すると、アプライアンスはプライマリ サーバに対してクエリを再実行します。

アプライアンスがプライマリ認証サーバに対してクエリを再実行した後に、プライマリ認証サーバからの応答がない状態で [再試行（Retries）] フィールドに指定された回数を超え、[タイムアウト（Timeout）] フィールドに指定された秒数が再び経過すると、アプライアンスはバックアップ サーバにロールオーバーします。

たとえば、プライマリ サーバで RADIUS が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。ただし RADIUS がプライマリ RADIUS サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

手順

ステップ 1 **[システム（System）] > [ユーザ（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 **[外部の作成（Create External）] > [認証オブジェクト（Authentication Object）]** をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウン リストから [RADIUS] を選択します。

ステップ 5 認証サーバの名前と説明を入力します。

ステップ 6 認証データを取得するプライマリ RADIUS サーバの IP アドレスまたはホスト名を [プライマリ サーバ ホスト名/IP アドレス（Primary Server Host Name/IP Address）] フィールドに入力します。

（注） シェル認証では IPv6 アドレスはサポートされていません。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてその IPv4 オブジェクトを使用します。

ステップ 7 オプションで、[プライマリ サーバ ポート（Primary Server Port）] フィールドでプライマリ RADIUS 認証サーバが使用するポートを変更します。

（注） 認証ポート番号とアカウンティングポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

ステップ 8 プライマリ RADIUS 認証サーバの RADIUS 秘密キーを入力します。

ステップ 9 オプションで、認証データを取得するバックアップ RADIUS 認証サーバの IP アドレスまたはホスト名を [バックアップ サーバ ホスト名/IP アドレス（Backup Server Host Name/IP Address）] フィールドに入力します。

ステップ 10 バックアップ サーバを設定する場合は、[バックアップ サーバ ポート（Backup Server Port）]、[RADIUS 秘密キー（RADIUS Secret Key）]、および [タイムアウト（Timeout）] を変更し、[再試行（Retries）] フィールドに、バックアップ接続にロールオーバーするまでプライマリ サーバ接続を試行する回数を入力します。

（注） 認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

次のタスク

- RADIUS 認証オブジェクトの作成 （78 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS ユーザ ロールの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

ユーザがログインすると、Firepower システムは RADIUS サーバを検査し、RADIUS 構成に基づいてアクセス権を付与します。

- ユーザに対して特定のアクセス権が設定されておらず、デフォルト アクセス ロールが指定されていない場合、新しいユーザがログインすると、Firepower システムは RADIUS サーバに対してそのユーザを認証してから、プラットフォーム設定ポリシーで設定されているデフォルト アクセス ロールに基づいてユーザ権限を付与します。
- 新しいユーザがどのリストにも指定されておらず、認証オブジェクトの [デフォルト ユーザ ロール（Default User Role）] リストでデフォルト アクセス ロールが指定されている場合、ユーザにはこのデフォルト アクセス ロールが割り当てられます。
- 1 つ以上の特定のロールのリストにユーザを追加すると、割り当てられているすべてのアクセス ロールがそのユーザに付与されます。

また、ユーザ名の代わりに属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。たとえば、セキュリティ アナリストとする必要があるすべてのユーザの `User-Category` 属性の値が `Analyst` である場合、これらのユーザにそのロールを付与するには、[セキュリティ アナリスト リスト（Security Analyst List）] フィールドに `User-Category=Analyst` と入力します。

外部認証されるが、特定のロールにリストされないすべてのユーザに、デフォルトのユーザ ロールを割り当てることができます。[デフォルト ユーザ ロール（Default User Role）] リストでは、複数のロールを指定できます。

Firepower システムのユーザ管理ページで RADIUS ユーザ リスト メンバーシップが設定されているため、アクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。

注意 ユーザの最小アクセス設定を変更するには、[RADIUS 固有パラメータ（RADIUS Specific Parameters）] セクションのリスト間でユーザを移動するかまたは RADIUS サーバでユーザの属性を変更する他に、構成を管理対象デバイスに再展開し、ユーザ管理ページで割り当てられているユーザ権限を削除する必要があります。

始める前に

- ユーザ ロール メンバーシップの設定に使用する場合は、カスタム RADIUS 属性の定義 （86 ページ）の説明に従ってカスタム属性を定義します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、Firepower システムのユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはそれらのロールに割り当てる属性と値のペアを指定します。

ユーザ名と属性と値のペアは、カンマで区切ります。

例：

たとえば、ユーザ `jsmith` と `jdoe` に管理者ロールを付与する場合は、[管理者（Administrator）] フィールドに `jsmith, jdoe` と入力します。もう 1 つの例として `User-Category` の値が `Maintenance` であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンス ユーザ（Maintenance User）] フィールドに `User-Category=Maintenance` と入力します。

ステップ 2 [デフォルト ユーザ ロール（Default User Role）] リストから、指定のどのグループにも属していないユーザのデフォルト最小アクセス ロールを選択します。

次のタスク

- RADIUS 認証オブジェクトの作成 （78 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS シェル アクセスの設定

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）	任意（Any）	任意（Any）	任意（Any）	Admin

RADIUS サーバを使用して、ローカル アプライアンス（管理対象デバイスまたは Firepower Management Center）で、CLI またはシェル アクセスについてアカウントを認証することもできます。CLI またはシェル アクセスを付与するユーザのユーザ名を指定します。

（注） シェル認証では IPv6 アドレスはサポートされていません。IPv6 アドレスを使用してプライマリ RADIUS サーバを設定し、管理シェル アクセスも設定すると、シェル アクセスの設定は無視されます。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して別の認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてそのオブジェクトを使用します。

Admin アカウント以外は、RADIUS 認証オブジェクトで設定したシェル アクセス リストにより、アプライアンスでの CLI またはシェル アクセスが完全に制御されます。CLI またはシェル ユーザは、プラットフォーム設定ポリシーを展開するときに、アプライアンスでローカル ユーザとして設定されます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

ログイン時に各 CLI またはシェル ユーザのホーム ディレクトリが作成されること、および（RADIUS 接続を無効にすることで）RADIUS シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

CLI またはシェル ユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインできます。CLI またはシェルのログイン認証では大文字と小文字が区別されます。

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。Firepower Management Center で追加のシェル ユーザを設定しないことをお勧めします。

手順

[外部認証オブジェクトの作成（Create External Authentication Object）] ページで、[管理者シェル アクセス ユーザ リスト（Administrator Shell Access User List）] フィールドにユーザ名をカンマで区切って入力します。

（注） シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

次のタスク

- RADIUS 認証オブジェクトの作成 （78 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

カスタム RADIUS 属性の定義

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）	任意（Any）	任意（Any）	任意（Any）	Admin

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、ログイン認証オブジェクトでこれらの属性を定義する必要があります。RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。また、指定する属性 ID は整数であり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合していてはなりません。属性のタイプ（文字列、IP アドレス、整数、または日付）も指定します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルがアプライアンスの `/var/sf/userauth` ディレクトリに作成されます。認証オブジェクトに追加するカスタム属性はすべて、そのディクショナリ ファイルに追加されます。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

手順

ステップ 1 [外部認証オブジェクトの追加（Add External Authentication Object）] ページで、矢印をクリックして [カスタム RADIUS 属性の定義（Define Custom RADIUS Attributes）] セクションを展開します。

ステップ 2 [属性名（Attribute Name）] フィールドに属性名を入力します。

ステップ 3 [属性 ID（Attribute ID）] フィールドに、属性 ID を整数形式で入力します。

ステップ 4 [属性タイプ（Attribute Type）] ドロップダウン リストから、属性のタイプを選択します。

ステップ 5 認証オブジェクトにカスタム属性を追加するには、[追加（Add）] をクリックします。

ヒント 認証オブジェクトからカスタム属性を削除するには、その属性の横にある [削除（Delete）] をクリックします。

例

シスコ ルータが接続しているネットワーク上でRADIUS サーバが使用される場合に、`Ascend-Assign-IP-Pool` 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザに特定のロールを付与するとします。`Ascend-Assign-IP-Pool` は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が `Ascend-IP-Pool-Definition`、属性 ID が `218`、属性タイプが `integer` のカスタム属性を作成します。

次に、`Ascend-IP-Pool-Definition` 属性値が `2` のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、`Ascend-Assign-IP-Pool=2` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。

次のタスク

- RADIUS 認証オブジェクトの作成 （78 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS 認証接続のテスト

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）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

RADIUS接続、ユーザ ロール、およびカスタム属性を設定したら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

ユーザ名として、テストするユーザのユーザ名を入力できます。

UI のページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント　テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテストパラメータ（Additional Test Parameters）] フィールドにユーザ情報を入力せずに [テスト（Test）] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

手順

ステップ 1　[外部認証オブジェクトの追加（Add External Authentication Object）] ページの [ユーザ名（User Name）] フィールドと [パスワード（Password）] フィールドに、RADIUS サーバへのアクセスの検証に資格情報が使用されるユーザのユーザ名とパスワードを入力します。

例：

たとえば、Example 社の `jsmith` のユーザ資格情報を取得できるかどうかをテストするには、「`jsmith`」と入力します。

ステップ 2　[詳細の表示（Show Details）] を選択し、[テスト（Test）] をクリックします。

ステップ 3　テストが成功した場合は [保存（Save）] をクリックします。

次のタスク

- RADIUS 認証を有効にするには、外部認証の有効化の説明に従って、認証オブジェクトを有効にします。

シングル サインオン（SSO）

シングル サインオン（SSO）により、Cisco Security Manager（CSM）バージョン 4.7 以上と Firepower Management Center を統合して、ログインの追加認証なしで CSM から Firepower Management Center にアクセスできるようにすることができます。ASA FirePOWER モジュールの管理では、モジュールに展開したポリシーの変更が必要となる場合もあります。CSM で Firepower Management Center を管理して、Web ブラウザで起動するという方法を選択することもできます。

ユーザ ロールに基づくアクセス権限がある場合、CSM でクロス起動したデバイスの [デバイス管理（Device Management）] ページの [デバイス（Device）] タブに移動します。それ以外の場合は、[サマリー ダッシュボード（Summary Dashboard）] ページ（**[概要（Overview）] > [ダッシュボード（Dashboards）]**）に移動します。ただしダッシュボードにアクセスできないユーザ アカウントの場合は、[ようこそ（Welcome）] ページが使用されます。

（注） 組織で認証に CAC が使用されている場合、シングル サインオンでログインすることはできません。

関連トピック

セキュリティ認定準拠

SSO の設定

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）	任意（Any）	ASA FirePOWER	任意（Any）	Admin

シングル サインオンを設定する前に、CSM から Firepower Management Center への一方向の暗号化認証パスを設定する必要があります。

NAT 環境では、Firepower Management Center と CSM は NAT 境界の同じ側に存在している必要があります。CSM と Firepower Management Center 間の通信を有効にする特定の基準を入力する必要があります。

（注） 組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。

手順

ステップ 1 CSM から、接続を識別する SSO 共有暗号キーを生成します。詳細については、CSM のマニュアルを参照してください。

ステップ 2 Firepower Management Center から、**[システム（System）]** > **[ユーザ（Users）]** を選択します。

ステップ 3 [CSM シングル サインオン（CSM Single Sign-on）] を選択します。

ステップ 4 CSM ホスト名または IP アドレスとサーバのポートを入力します。

ステップ 5 CSM から生成した共有キーを入力します。

ステップ 6 オプションで、Firepower Management Center のプロキシ サーバを使用して CSM と通信する場合は、[接続にプロキシを使用（Use Proxy For Connection）] チェックボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [証明書の確認（Confirm Certificate）] をクリックして証明書を保存します。
これで CSM から Firepower Management Center にログインできるようになります。追加のログインを実行する必要はありません。