ユーザ権限とデバイス アクセス

ユーザインターフェイス、ユーザタイプ、およびそれらの間の遷移

これらのトピックでは、Cisco EPN Manager で使用される GUI と CLI インターフェイス、および Cisco EPN Manager と Linux CLI インターフェイス間の遷移について説明します。

ユーザ インターフェイスとユーザ タイプ

次の表に、Cisco EPN Manager （CEPNM）によって採用されたユーザ インターフェイスと、各インターフェイスにアクセス可能なユーザのタイプの説明を示します。

CEPNM ユーザ インターフェイス	インターフェイスの説明	CEPNM ユーザ タイプ
CEPNM Web GUI	Web GUI を使用して日常業務と管理業務を容易にする Web インターフェイス。これらのユーザは、さまざまなレベルの権限を持つことができ、ロールベース アクセス コントロール（RBAC）クラスとサブクラスに分類されます。 このインターフェイスは、Cisco EPN Manager の CLI 管理ユーザと CLI 構成ユーザによって提供される操作のサブセットを提供します。	[Web GUI通常ユーザ（Web GUI everyday users）]**Cisco EPN Manager**：Web GUI のルートユーザによって作成されます。このユーザは、さまざまなレベルの権限を持ち、ユーザ グループ（管理者、スーパーユーザ、構成マネージャなど）と呼ばれるロールベースアクセスコントロール（RBAC）クラスとサブクラスに分類されます。ユーザ グループについては、ユーザ グループのタイプ （5 ページ）を参照してください。 **Cisco EPN Manager** Web GUI ルート ユーザ：インストール時に作成され、Web GUI への 1 回目のログインと他のユーザ アカウントの作成に使用されます。このアカウントは、管理者権限を持つ少なくとも 1 人の Web GUI ユーザ、つまり、管理者ユーザまたはスーパーユーザユーザグループに属している Web GUI ユーザの作成後に無効にする必要があります。Web GUI ルート ユーザの無効化および有効化 （4 ページ）を参照してください。 （注） Cisco EPN Manager Web GUI ルート ユーザは、Linux CLI ルート ユーザと同じではなく、Cisco EPN Manager CLI 管理者ユーザとも異なります。 .
[ノースバウンドインターフェイス（NBI）REST API（North Bound Interface (NBI) REST API）]	NBI は REST アプリケーション プログラミング インターフェイスであり、クライアントシステムが Cisco EPN Manager と通信して通常の操作および管理操作を実行できるようにします。NBI は REST アプリケーション プログラミング インターフェイスであり、クライアントシステムが Cisco EPN Manager と通信して日常的な操作および管理操作を実行できるようにします。 また、これらの NBI ユーザは、さまざまなレベルの権限を持つこともでき、ロールベース アクセス コントロール（RBAC）クラスとサブクラスにも分類されます。	[Cisco EPN Manager NBI ユーザ（Cisco EPN Manager NBI users）]：Web GUI ルートユーザによって作成されます。これらのユーザには、3 種類の異なる権限があり、ロールベースのアクセスコントロール（RBAC）クラスと NBI ユーザグループというサブクラス（NBI 読み取り、NBI 書き込み、NBI クレデンシャル（廃止））に分類されます。ユーザグループの詳細については、次の項を参照してください。 ユーザ グループ - NBI （6 ページ）

CEPNM ユーザ インターフェイス	インターフェイスの説明	CEPNM ユーザ タイプ
CEPNM 管理者 CLI	システムへのセキュアで限定的なアクセスを提供するシスコ独自のシェル（Linux シェルと比較した場合）。この管理者シェルと CLI は、高度な Cisco EPN Manager 管理タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、Cisco EPN Manager CLI 管理者ユーザ アクセス権を持っている必要があります。SSH を使用してリモート コンピュータからこのシェルにアクセスできます。	**Cisco EPN Manager CLI 管理者ユーザ**：インストール時に作成され、アプリケーションの停止と再起動やリモート バックアップ リポジトリの作成などの管理操作に使用されます（この管理操作のサブセットは、Web GUI から使用できます）。 このユーザが実行可能な操作のリストを表示するには、プロンプトで **?** と入力します。 一部のタスクは、コンフィギュレーション モードで実行する必要があります。コンフィギュレーション モードに移行するには、Cisco EPN Manager 管理 CLI と Cisco EPN Manager 構成 CLI の切り替え （4 ページ）内の手順を使用します。
CEPNM 構成 CLI	Linux シェルよりセキュアで限定されたシスコ独自のシェル。この構成シェルと CLI は、Cisco EPN Manager システム設定タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、管理者レベルのユーザ アクセス権を持っている必要があります（この表の [ユーザ タイプ（User Types）] 列内の情報を参照）。管理者 CLI シェルからこのシェルにアクセスできます。	管理者 CLI ユーザは、次のコマンドを使用して、さまざまな理由で他の CLI ユーザを作成できます。 `(config) username username password role {admin|user} password` これらのユーザには、作成期間に定義された管理者に準ずる権限/ロールまたはより低レベルの権限を付与できます。管理者権限を持つ Cisco EPN Manager CLI ユーザを作成するには、**admin** キーワードを指定して **username** コマンドを実行します。それ以外のユーザを作成する場合は、**user** キーワードを使用します。
Linux CLI	すべての Linux コマンドを提供する Linux シェル。Linux シェルは、シスコ テクニカル サポート担当者のみが使用できます。標準のシステム管理者は、Linux シェルを使用しないでください。SSH を使用してリモート コンピュータからこのシェルに到達することはできません。到達するには、Cisco EPN Manager 管理者シェルと CLI を経由する必要があります。	**Linux CLI 管理ユーザ**：インストール時に作成され、Linux レベルの管理目的に使用されます。

Cisco EPN Manager で CLI ユーザ インターフェイスを切り替える方法

Cisco EPN Manager 管理 CLI と Cisco EPN Manager 設定 CLI 間の移行方法については、次のセクションを参照してください

Cisco EPN Manager 管理 CLI と Cisco EPN Manager 構成 CLI の切り替え

Cisco EPN Manager 管理 CLI から Cisco EPN Manager 構成 CLI に移行するには、admin プロンプトで **config** と入力します。

```
(admin)# config
(config)#
```

構成 CLI から管理 CLI に戻るには、config プロンプトで **exit** または **end** と入力します。

```
(config)# exit
(admin)#
```

Cisco EPN Manager Web GUI のルートへのアクセスの有効化および無効化

管理者権限またはスーパーユーザ権限を持つ他の Web GUI ユーザを 1 人以上作成したら、Cisco EPN Manager Web GUI **root** ユーザを無効にする必要があります。Web GUI ルート ユーザの無効化および有効化 （4 ページ）を参照してください。

Web GUI ルート ユーザの無効化および有効化

ステップ 1 ルートとして Cisco EPN Manager Web GUI にログインし、ルート権限を持つ別の Web GUI ユーザ（つまり、管理ユーザ グループまたはスーパー ユーザ グループに属する Web GUI ユーザ）を作成します。ユーザの追加およびユーザ アカウントの管理 （27 ページ）を参照してください。上記のステップが完了すると、Web GUI **root** アカウントを無効化できるようになります。

ステップ 2 次のコマンドを実行して Cisco EPN Manager Web GUI ルート ユーザ アカウントを無効化します（Web GUI 管理アカウントはアクティブな状態に維持されるので、必要なすべての CLI 関数を実行できます）。

```
ncs webroot disable
```

ステップ 3 アカウントを再び有効にするには、次のコマンドを実行します。

```
ncs webroot enable
```

ユーザが実行できるタスクの制御（ユーザグループ）

Web インターフェイス ユーザの場合、Cisco EPN Manager では、ユーザ認証はユーザグループを使用して実装されます。ユーザ グループには、ユーザがアクセスできる Cisco EPN Manager の部分およびユーザがその部分で実行できるタスクを制御するタスクの一覧が含まれています。

ユーザ グループはユーザの操作を制御しますが、仮想ドメインはユーザがこれらのタスクを実行できるデバイスを制御します。仮想ドメインの詳細については、「デバイスへのユーザ アクセスを制御するための仮想ドメインの作成 （36 ページ）」を参照してください。

Cisco EPN Manager では、いくつかのユーザ グループが事前定義されています。ユーザがユーザ グループに属している場合、ユーザはそのグループのすべての認証設定を継承します。ユーザは通常、アカウントが作成されるときにユーザ グループに追加されます。

次のトピックでは、ユーザ認証の管理方法について説明します。

ユーザ グループのタイプ

Cisco EPN Manager は、次の事前定義のユーザ グループを提供します。

CLI ユーザについては、ユーザ インターフェイスとユーザ タイプ （1 ページ）を参照してください）。

ユーザ グループ：Web UI

Cisco EPN Manager は、次の表にリストされているデフォルトの Web GUI ユーザ グループを提供します。Monitor Lite ユーザ グループに属するユーザを除き、ユーザを複数のグループに割り当てることができます（Monitor Lite は、権限が非常に制限されているユーザ向けであるためです）。

各ユーザ グループとデフォルト設定に関係するタスクについては、グループで実行できるタスクを表示および変更する （25 ページ）を参照してください。

ユーザ グループ	グループ タスク フォーカス
Root	すべての操作。このグループの権限は編集できません。インストール後に、root Web UI ユーザが使用可能になります。ユーザ インターフェイスとユーザ タイプ （1 ページ）を参照してください。Web GUI ルート ユーザの無効化および有効化 （4 ページ）に説明されているとおり、Admin または Super Users 権限で別のユーザを作成し、root Web UI ユーザを無効にすることをお勧めします。
スーパーユーザ	すべての操作（デフォルトなし）。このグループの権限は編集できます。ルートユーザの権限に類似した権限を有効にすることができます。
Admin	システムとサーバを管理します。モニタリングや設定に関する操作を実行できます。このグループの権限は編集できます。
Config Managers	ネットワークを設定およびモニタします（管理タスクは行いません）。このグループに割り当てられる権限は、編集可能です。
System Monitoring	ネットワークをモニタします（設定タスクは行いません）。このグループの権限は編集できます。
Help Desk Admin	ヘルプ デスクとユーザ設定関連のページにしかアクセスできません。これは、ユーザ インターフェイスへのアクセスがない特殊なグループです。
Lobby Ambassador	ゲスト ユーザのみのユーザ管理。このユーザ グループのメンバーは、他のユーザ グループのメンバーを兼ねることはできません。
ユーザ定義 1 - 4	N/A：これらはブランクのグループで、必要に応じて編集したり、カスタマイズしたりできます。
Monitor Lite	ネットワーク トポロジおよびユーザ タグを表示します。このグループの権限は編集できません。このユーザ グループのメンバーは、他のユーザ グループのメンバーを兼ねることはできません。
North Bound API	SOAP API にアクセスします。
User Assistant	ローカル ネット ユーザ管理のみ。このユーザ グループのメンバーは、他のユーザ グループのメンバーを兼ねることはできません。
mDNS Policy Admin	mDNS ポリシー管理機能。

ユーザ グループ - NBI

Cisco EPN Manager は、次の表に記載されているデフォルトの NBI ユーザ グループを提供します。これらのグループ内の権限は編集できません。

各ユーザ グループとデフォルト設定に関係するタスクについては、グループで実行できるタスクを表示および変更する （25 ページ）を参照してください。

ユーザ グループ	アクセス対象：
NBI クレデンシャル（廃止）	MTOSI NBI を使用したクレデンシャル管理。他の NBI または Web UI ユーザ グループに属することもできます。
NBI Read	RESTCONF NBI 読み取り操作（HTTP GET）。他の NBI または Web UI ユーザ グループに属することもできます。
NBI Write	RESTCONF NBI 書き込み操作（HTTP PUT、POST、DELETE）。他の NBI または Web UI ユーザ グループに属することもできます。

ユーザが実行できるタスクの表示と変更

ユーザが実行できるタスクは、ユーザが所属するユーザ グループによって制御されます。ユーザが所属するグループと、ユーザが実行する権限を持つタスクを確認するには、次の手順を実行します。

（注） ユーザがアクセスできるデバイスを確認する場合は、ユーザへの仮想ドメインの割り当て（43 ページ）を参照してください。

ステップ 1 **[管理（Administrration）]** > **[ユーザ（Users）]** > **[ユーザ、ロール、およびAAA（Users, Roles & AAA）]** を選択し、ユーザ名を見つけます。

ステップ 2 ユーザ名を見つけて、[以下のメンバー（Member of）] の列をチェックして、ユーザが所属するユーザ グループを見つけます。

ステップ 3 ユーザ グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウで、グループのメンバーが実行できるタスクと実行できないタスクのリストを表示します。

- チェックが付けられているチェックボックスは、グループ メンバーがそのタスクを実行する権限を持っていることを意味します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。たとえば、Cisco EPN Manager では、Monitor Lite ユーザ グループの [タグの表示（View tags）] タスクを削除できません。これは、そのユーザ グループにとって不可欠なタスクであるためです。
- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザ グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 4 権限を変更するには、次の選択肢があります。

（注） この操作は慎重に行ってください。[グループ詳細（Group Detail）] ウィンドウでタスクのチェックボックスをオンまたはオフにすると、すべてのグループ メンバーに変更が適用されます。

- すべてのユーザ グループのメンバーの権限を変更します。グループで実行できるタスクを表示および変更する （25 ページ）を参照してください。
- 別のユーザ グループにユーザを追加します。事前定義されたユーザ グループについては、ユーザ グループ：Web UI （5 ページ） とユーザ グループ - NBI （6 ページ） で説明します。これらのトピックでは、グループの制限についても説明します。たとえば、ユーザが事前定義済みの Monitor Lite ユーザ グループに属している場合、そのユーザは他のグループに所属することはできません。
- このグループからユーザを削除します。ユーザが属しているグループを表示して変更する （8 ページ）を参照してください。
- カスタマイズされたユーザ グループを使用し、ユーザをそのグループに追加します。既存のカスタマイズされたグループを確認するには、グループで実行できるタスクを表示および変更する （25 ページ）を参照してください。新たにカスタマイズされたグループを作成するには、カスタム ユーザ グループの作成 （25 ページ）を参照してください。

ユーザが属しているグループを表示して変更する

ユーザが実行可能なタスクは、そのユーザが属しているユーザ グループによって決定されます。通常は、ユーザ アカウントの作成時に設定されます（ユーザの追加および削除 （29 ページ）を参照）。ユーザ グループについては、ユーザ グループのタイプ （5 ページ）で説明します。

この手順では、ユーザが属しているグループを表示し、必要に応じて、ユーザのグループ メンバーシップを変更する方法について説明します。

ステップ 1 >[管理（Administration）]>[ユーザ、ロール、およびAAA（Users, Roles & AAA）] を選択してから、[ユーザ（Users）] をクリックします。

ステップ 2 [ユーザ名（User Name）] 列で、ユーザ名のハイパーリンクを探してクリックし、[ユーザの詳細（User Details）] ウィンドウを開きます。すべてのユーザ グループが [一般（General）] タブの下に一覧表示されます。

- オンになっているチェックボックスは、ユーザがそのグループに属していることを意味します。オンになっているボックスが灰色表示されている場合は、そのグループからユーザを削除できないことを意味します。たとえば、Cisco EPN Manager では、ルート ユーザ グループから **root** という名前のユーザを削除できません。
- オフになっているチェックボックスは、ユーザがそのグループに属していないことを意味します。オフになっているチェックボックスが灰色表示されている場合は、そのグループにユーザを追加できないことを意味します

（グループが実行可能なタスクをチェックするには、左側のサイドバー メニューで、[ユーザ グループ（User Groups）] を選択し、グループ名をクリックします）。

ステップ 3 ユーザが属しているグループを変更するには、[ユーザの詳細（User Details）] ウィンドウで該当するグループを選択して選択解除してから、[保存（Save）] をクリックします。

ユーザ グループとそのメンバーの表示

ユーザは、Monitoring Liteなどの非常に制限されたグループに属していない限り、複数のグループに所属できます。この手順では、既存のユーザ グループとそのメンバーを表示する方法を説明します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザ グループ（User Groups）] をクリックします。

[ユーザ グループ（User Groups）] ページには、既存のすべてのユーザ グループとそのメンバーの短いリストが表示されます。これらのグループの詳細については、ユーザ グループのタイプ （5 ページ）を参照してください。

ステップ 2 グループのすべてのメンバーを表示するには、グループのハイパーリンクをクリックして[グループの詳細（Group Details）] ウィンドウを開き、[メンバー（Members）] タブをクリックします。

ステップ 3 これらのグループを変更する場合は、以下を参照してください。

- グループで実行できるタスクを表示および変更する （25 ページ）
- ユーザが属しているグループを表示して変更する （8 ページ）

ユーザグループの権限とタスクの説明

次の表に、ユーザグループの権限とタスクの説明を示します。

表 *1:* ユーザグループの権限とタスクの説明

タスクグループ名	タスク名	説明
Administrative Operations	デバイスコンソール設定	ユーザはデバイスコンソールで設定コマンドを実行できます
	デバイスコンソール表示	ユーザはデバイスコンソールで show コマンドを実行できます
	監査ログのエクスポート（Export Audit Logs Access）	ユーザは [管理メガ（Admin Mega）] メニューから [インポートポリシーの更新（Import Policy Update）] にアクセスできます
	ヘルスモニタの詳細（Health Monitor Details）	ユーザはサイトのヘルススコア定義を変更できます
	ハイ アベイラビリティ設定	ユーザはプライマリサーバとセカンダリサーバのペアリングに [ハイアベイラビリティ（High Availability）] を設定できます
	インポートポリシーの更新（Import Policy Update）	ユーザはポリシーの更新を手動でダウンロードし、コンプライアンスおよび監査マネージャエンジンにインポートできます
	ライセンスセンター/スマートライセンス（License Center/Smart License）	ユーザはライセンスセンター/スマートライセンスにアクセスできます
	ログ	ユーザはログレベルを設定できるメニュー項目にアクセスできます
	スケジュールされたタスクとデータコレクション（Scheduled Tasks and Data Collection）	バックグラウンドタスクを表示する画面へのアクセスを制御します
	システム設定（System Settings）	

タスクグループ名	タスク名	説明
		[管理（Administration）] > [システム設定（System Settings）] メニューへのアクセスを制御します
	ユーザ定義フィールド	ユーザはユーザ定義フィールドを作成できます
	ユーザ設定	[管理（Administration）] > [ユーザ設定（User Preference）] メニューへのアクセスを制御します。
	監査ログの表示へのアクセス（View Audit Logs Access）	ユーザは [ネットワーク（Network）] および [システム監査（System audits）] を表示できます

タスクグループ名	タスク名	説明
Alerts and Events	ACK アラートおよび UNACK アラート（Ack and Unack Alerts）	ユーザは既存のアラームの確認応答または確認応答解除を実行できます
	アラームポリシー（Alarm Policies）	ユーザはアラームポリシーにアクセスできます。
	アラームポリシーの編集アクセス（Alarm Policies Edit Access）	ユーザはアラームポリシーを編集できます
	アラートの削除およびクリア（Delete and Clear Alerts）	ユーザはアクティブアラームをクリアおよび削除できます
	電子メール通知	ユーザは電子メール通知の転送を設定できます
	通知ポリシーの読み取りアクセス（Notification Policies Read Access）	ユーザはアラーム通知ポリシーを表示できます
	通知ポリシーの読み取り/書き込みアクセス（Notification Policies Read-Write Access）	ユーザはアラーム通知ポリシーを設定できます
	アラートの選択および選択解除（Pick and Unpick Alerts）	ユーザはアラートを選択および選択解除できます
	トラブルシューティング	ユーザはアラームで traceroute や ping などの基本的なトラブルシューティングを実行できます
	アラート状態の表示（View Alert Condition）	ユーザはアラート条件を表示できます。
	アラートとイベントの表示（View Alerts and Events）	ユーザはイベントおよびアラームのリストを表示できます
ライセンスの確認	ライセンスの確認	ユーザはコントローラライセンスやMSEライセンスなどのライセンスの有効性を確認できます

タスクグループ名	タスク名	説明
[設定（Configure）] メニュータスク	[設定（Configure）] メニューアクセス	ユーザは設定メニューのすべての機能にアクセスできます
	デバイス設定エクスポートのサニタイズの解除	ユーザは、サニタイズされていない設定アーカイブを公開できます
診断タスク（Diagnostic Tasks）	診断情報（Diagnostic Information）	[診断（Diagnostic）] ページへのアクセスを制御します。
	デバイス設定エクスポートのサニタイズの解除	ユーザは、サニタイズされていない設定アーカイブを公開できます
フィードバックタスクとサポートのタスク	自動フィードバック（Automated Feedback）	自動フィードバックにアクセスできます
	TAC ケース管理ツール（TAC Case Management Tool）	ユーザは TAC ケースを開くことができます
グローバル変数の設定（Global Variable Configuration）	グローバル変数へのアクセス（Global Variable Access）	ユーザはグローバル変数にアクセスできます。
グループ管理（Groups Management）	グループメンバーの追加（Add Group Members）	ユーザはデバイスやポートなどのエンティティをグループに追加できます
	グループの追加（Add Groups）	ユーザはグループを作成できます
	グループメンバーの削除（Delete Group Members）	ユーザはグループからメンバーを削除できます
	グループの削除	ユーザはグループを削除できます
	グループのエクスポート（Export Groups）	ユーザはグループをエクスポートできます
	グループのインポート（Import Groups）	ユーザはグループをインポートできます
	グループの変更（Modify Groups）	ユーザは名前、親、ルールなどのグループ属性を編集できます

タスクグループ名	タスク名	説明
[ヘルプ（Help）] メニュータスク	[ヘルプ（Help）] メニューアクセス	ユーザは [ヘルプ（Help）] メニューにアクセスできます
[ホーム（Home）] メニュータスク	[ホーム（Home）] メニューアクセス	ユーザはホームページにアクセスできます

タスクグループ名	タスク名	説明
ジョブ管理	ジョブの承認（Approve Job）	ユーザは別のユーザに承認を得るためにジョブを送信できます
	ジョブのキャンセル（Cancel Job）	ユーザは実行中のジョブをキャンセルできます
	[ジョブの削除（Delete Job）]	ユーザは[ジョブ（Jobs）]ダッシュボードからジョブを削除できます
	[ジョブの編集（Edit Job）]	ユーザは[ジョブ（Jobs）]ダッシュボードからジョブを編集できます
	ジョブの一時停止（Pause Job）	ユーザは実行中のジョブとシステムジョブを一時停止できます
	ジョブのスケジュール（Schedule Job）	ユーザはジョブをスケジュールできます
	ジョブの表示（Schedule Job）	ユーザはスケジュール済みのジョブを表示できます
	編集ジョブの展開の設定（Config Deploy Edit Job）	ユーザは展開済みのジョブの設定を編集できます
	デバイス設定バックアップジョブの編集アクセス（Device Config Backup Job Edit Access）	ユーザはリポジトリやファイル暗号化パスワードなどの外部バックアップ設定を変更できます
	ジョブ通知メール（Job Notification Mail）	ユーザはさまざまなジョブタイプに関して通知メールを設定できます
	ジョブの実行（Run Job）	ユーザは一時停止されたジョブとスケジュール済みのジョブを実行できます
	[システムジョブ（System Jobs）] タブへのアクセス	ユーザはシステムジョブを表示できます
[モニタ（Monitor）] メニュータスク	[モニタ（Monitor）] メニューアクセス	ユーザは [モニタ（Monitor）] メニューのすべての機能にアクセスできます

タスクグループ名	タスク名	説明
ネットワーク構成	デバイスの追加アクセス（Add Device Access）	ユーザはCisco EPN Managerにデバイスを追加できます
	管理テンプレートへの書き込みアクセス（Admin Templates Write Access）	ユーザ定義ロールの管理テンプレートへの書き込みアクセスを有効にするには、このチェックボックスをオンにします
	自動プロビジョニング（Auto Provisioning）	自動プロビジョニングにアクセスできます
	アラームモニタポリシー	アラームモニタポリシーにアクセスできます
	コンプライアンス監査の修正アクセス（Compliance Audit Fix Access）	ユーザはコンプライアンス修正ジョブおよびレポートを表示、スケジュール、エクスポートできます
	コンプライアンス監査 PAS へのアクセス（Compliance Audit PAS Access）	ユーザは「PSIRT」および「EOX」のジョブおよびレポートを表示、スケジュール、エクスポートできます。
	コンプライアンス監査ポリシーへのアクセス（Compliance Audit Policy Access）	ユーザはコンプライアンスポリシーを作成、変更、削除、インポート、エクスポートできます
	コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）	ユーザはコンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます
	コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）	ユーザはコンプライアンス プロファイルについては作成、変更、削除でき、コンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます

タスクグループ名	タスク名	説明
	設定アーカイブの読み取りタスク	設定アーカイブの読み取りアクセスを許可します
	設定アーカイブの読み取り/書き込みタスク	設定アーカイブの読み取り/書き込みアクセスを許可します
	設定テンプレートへの読み取りアクセス（Configuration Templates Read Access）	読み取り専用モードで設定テンプレートにアクセスできます
	ACS View Server の設定（Configure ACS View Servers）	ACS View Server にアクセスして管理できます
	設定グループの設定（Configure Config Groups）	設定グループにアクセスできます
	ISE サーバの設定	ユーザは Cisco EPN Manager で ISE サーバを管理できます
	テンプレートの設定（Configure Templates）	ユーザは機能テンプレートの CRUD 操作を実行してテンプレートを設定できます
	クレデンシャルプロファイルの Add_Edit へのアクセス（Credential Profile Add_Edit Access）	ユーザはクレデンシャルプロファイルを追加および編集できます
	クレデンシャルプロファイルの削除アクセス（Credential Profile Delete Access）	ユーザはクレデンシャルプロファイルを削除できます
	クレデンシャルプロファイルの表示アクセス（Credential Profile View Access）	ユーザはクレデンシャルプロファイルを表示できます
	デバイスアクセスの削除（Delete Device Access）	ユーザは Cisco EPN Manager からデバイスを削除できます
	アクセス設定の展開（Deploy Configuring Access）	ユーザは設定と IWAN テンプレートを展開できます
	設計設定テンプレートへのアクセス（Design Configuration Template Access）	ユーザは、[設定（Configuration）] から共有ポリシー オブジェクト テンプレートや設定グループテンプレートを作成できます

タスクグループ名	タスク名	説明
	デバイス一括インポートアクセス（Device Bulk Import Access）	ユーザはCSVファイルからデバイスの一括インポートを実行できます
	デバイス表示設定アクセス（Device View configuration Access）	ユーザはデバイスワークセンターでデバイスを設定できます
	デバイスアクセスのエクスポート（Export Device Access）	ユーザはデバイスクレデンシャルやデバイスのその他の詳細情報を編集できます
	デバイスアクセスのエクスポート（Export Device Access）	ユーザはクレデンシャルなどのデバイスのリストをCSVファイルとしてエクスポートできます。
	ネットワーク デバイス	ユーザはネットワークデバイスにアクセスできます
	ネットワークトポロジの編集（Network Topology Edit）	ユーザはトポロジマップでデバイス、リンク、ネットワークを作成でき、手動で作成したリンクを編集して、インターフェイスを割り当てることができます
	プロビジョニングアクセス	プロビジョニングにアクセスできます
	QoSプロファイル設定アクセス	ユーザは次の操作を行えます。QoSプロファイルの作成/変更/削除、QoSプロファイルの展開ジョブのスケジュール、またはインターフェイスの関連付け/関連付け解除、および検出済みQoSプロファイルのインポート/エクスポート

タスクグループ名	タスク名	説明
ネットワーク モニタリング	管理ダッシュボードへのアクセス（Admin Dashboard Access）	ユーザは管理ダッシュボードにアクセスできます
	シャーシビューの読み取り	シャーシビューの読み取りにアクセスできます
	シャーシビューの読み取り/書き込み	シャーシビューの読み取り/書き込みにアクセスできます
	設定監査ダッシュボード（Config Audit Dashboard）	ユーザは設定監査ダッシュボードにアクセスできます
	データ収集管理アクセス（Data Collection Management Access）	ユーザは[アシュアランスデータソース（Assurance Data Sources）]ページにアクセスできます
	詳細ダッシュボードへのアクセス（Details Dashboard Access）	ユーザは詳細ダッシュボードにアクセスできます
	インシデントアラームイベントへのアクセス（Incidents Alarms Events Access）	ユーザはインシデントアラームイベントにアクセスできます。
	最新の設定監査レポート（Latest Config Audit Report）	ユーザは最新の設定監査レポートを表示できます
	ネットワーク トポロジ	ユーザはネットワークトポロジマップを起動し、マップ内のデバイスとリンクを表示できます
	パフォーマンス ダッシュボードへのアクセス（Performance Dashboard Access）	ユーザはパフォーマンス ダッシュボードにアクセスできます

タスクグループ名	タスク名	説明
OTDR	OTDR 設定プロファイル	OTDR 設定プロファイルにアクセスできます
	OTDR 実行スキャン	ユーザは OTDR スキャンにアクセスできます
	OTDR 設定基準	OTDR 基準にアクセスできます
	OTDR ビューのスキャン結果	ユーザは OTDR スキャン結果を表示できます
製品使用状況レポート	製品のフィードバック	ユーザは[改善にご協力ください（Help Us Improve）]ページにアクセスできます

タスクグループ名	タスク名	説明
レポート	コンプライアンス レポート	ユーザは設定監査、ネットワークの不一致、PCI DSS 詳細レポートおよび PCI DSS サマリーレポート、PSIRT 詳細レポートおよび PSIRT サマリーレポートをカスタマイズできます
	読み取り専用コンプライアンスレポート（Compliance Reports Read Only）	ユーザは設定監査、ネットワークの不一致、PCI DSS 詳細レポートおよび PCI DSS サマリーレポート、PSIRT 詳細レポートおよび PSIRT サマリーレポートを表示できます
	カスタムコンポジットレポート（Custom Composite Report）	ユーザは 2 つ以上（最大 5 つのレポート）の既存のレポートテンプレートを使用して「カスタム」レポートを単一レポートに作成できます
	デバイス レポート	ユーザはデバイスに関連する特定のレポートのモニタリングに固有のレポートを実行できます
	読み取り専用デバイスレポート（Device Reports Read Only）	ユーザは生成されたデバイスレポートを読むことができます。
	Network Summary レポート	ユーザはネットワーク サマリー レポートを作成および実行できます。
	読み取り専用ネットワーク サマリー レポート（Network Summary Reports Read Only）	ユーザはすべてのサマリーレポートを表示できます
	光パフォーマンス レポート	ユーザは光パフォーマンスレポートを作成できます
	読み取り専用光パフォーマンスレポート	ユーザは光パフォーマンスレポートを表示できます
	パフォーマンス レポート	ユーザはパフォーマンスレポートを作成できます

タスクグループ名	タスク名	説明
	読み取り専用パフォーマンスレポート（Performance Reports Read Only）	ユーザはパフォーマンスレポートを表示できます
	レポート ラウンチ パッド	ユーザは[レポート（Report）]ページにアクセスできます
	レポート実行履歴（Report Run History）	ユーザはレポート履歴を表示できます
	レポートリストの実行（Run Reports List）	ユーザはレポートを実行できます
	保存済みレポートリスト（Saved Reports List）	ユーザはレポートを保存できます
	システム モニタリング レポート	ユーザはシステム モニタリング レポートを表示できます
	仮想ドメインリスト（Virtual Domains List）	ユーザは仮想ドメインの関連のレポートを作成できます。

タスクグループ名	タスク名	説明
ソフトウェア イメージの管理	ソフトウェアイメージ管理サーバの追加（Add Software Image Management Servers）	ユーザはソフトウェアイメージ管理サーバを追加できます
	イメージ詳細ビュー	ユーザはイメージの詳細を表示できます
	プロトコルの管理	ユーザはプロトコルを管理できます
	SWIM のアクセス権限	SWIM のアクセス権限
	SWIM の有効化	SWIM の有効化
	SWIM 収集	SWIM 収集
	SWIM の削除	SWIM の削除
	SWIM のディストリビューション	SWIM のディストリビューション
	SWIM のユーザ設定の保存	ユーザは [システム設定（System Settings）] > [イメージ管理（Image Management）] ページで設定オプションを保存できます
	ソフトウェア情報の更新	ユーザは最小 RAM、最小 FLASH、最小ブート ROM のバージョンなど、イメージのプロパティを編集して保存できます
	SWIM の推奨事項	ユーザは Cisco.com およびローカルリポジトリからイメージを推奨できます
	SWIM のアップグレード分析	ユーザはソフトウェアイメージを分析して、ソフトウェアのアップグレードを実行する前に、ハードウェアのアップグレード（該当する場合はブート ROM、フラッシュメモリ、RAM、ブートフラッシュ）が必要かどうかを判断できます

タスクグループ名	タスク名	説明
ユーザ管理	監査証跡	ユーザはユーザのログインおよびログアウトに関する[監査証跡（Audit trails）] にアクセスできます
	LDAP サーバ（LDAP Server）	ユーザは[LDAPサーバ（LDAP Server）] メニューにアクセスできます
	RADIUS サーバ	ユーザは [RADIUSサーバ（RADIUS Servers）] メニューにアクセスできます
	SSO サーバ AAA モード（SSO Server AAA Mode）	ユーザは [AAA] メニューにアクセスできます。
	SSO サーバ	ユーザは [SSO] メニューにアクセスできます。
	TACACS+ サーバ	ユーザは [TACACS+サーバ（TACACS+ Servers）] メニューにアクセスできます。
	ユーザとグループ	ユーザは [ユーザとグループ（Users and Groups）] メニューにアクセスできます
	仮想ドメイン管理（Virtual Domain Management）	ユーザは [仮想ドメイン管理（Virtual Domain Management）] メニューにアクセスできます
	[仮想要素（Virtual Elements）] タブへのアクセス（Virtual Elements Tab Access）	仮想ドメインを作成、またはメンバーを仮想ドメインに追加する場合、ユーザは[仮想要素（Virtual Elements）] タブにアクセスすることができ、仮想要素（データセンター、クラスタ、ホスト）を仮想ドメインに追加できます
オンラインヘルプの表示（View Online Help）	OnlineHelp	ユーザはオンラインヘルプにアクセスできます

カスタム ユーザ グループの作成

Cisco EPN Manager に用意されている一連の定義済みユーザ グループを利用してユーザの権限を制御できます。これらの定義済みグループ（ユーザ グループのタイプ （5 ページ）を参照）に含まれているユーザ定義グループをカスタマイズすることで、展開に固有のユーザ グループを作成できます。次の手順で、4 つの定義済みユーザ定義グループ テンプレートのうちの 1 つを使用してカスタム グループを作成する方法を説明します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザ グループ（User Groups）] を選択します。

ステップ 2 メンバーがないユーザ定義グループを見つけて、そのグループ名のハイパーリンクをクリックします。

ステップ 3 [グループの詳細（Group Detail）] ウィンドウでタスクをオンまたはオフにして、グループ アクセス権限をカスタマイズします。タスクが灰色で表示されている場合、その設定を調整することはできません。ユーザグループの名前を変更することはできません。.

ステップ 4 [保存（Save）] をクリックして設定を保存します。

ステップ 5 グループにメンバーを追加するには、該当するユーザ アカウントを編集して、そのユーザを新しいグループに追加します。ユーザ アカウントの調整の詳細については、ユーザの追加および削除 （29 ページ）を参照してください。

グループで実行できるタスクを表示および変更する

既存のユーザ グループに関する情報と、グループ メンバーが実行できるタスクに関する情報を入手するには、次の手順に従ってください。事前定義されているユーザ グループの詳細については、「ユーザ グループとそのメンバーの表示 （9 ページ）」を参照してください。

（注） デバイス アクセスを変更する場合は、「ユーザへの仮想ドメインの割り当て （43 ページ）」を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザ グループ（User Groups）] を選択します。

[ユーザ グループ（User Groups）] ページには、既存のすべてのユーザ グループが一覧表示されます。

ステップ 2 ユーザ グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウに、グループのアクセス許可が一覧表示されます。

- チェックマークの付いているタスクは、グループ メンバーがそのタスクを実行する権限を持っていることを示します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。

- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザ グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 3 すべてのグループ メンバーに影響するグループの権限を変更する場合は、タスクのチェックボックスをオンまたはオフにして、[保存（Save）] をクリックします。

（注） この操作は慎重に行ってください。[グループ詳細（Group Detail）] ウィンドウでタスクのチェックボックスをオンまたはオフにすると、すべてのグループ メンバーに変更が適用されます。この操作の代わりに、[ユーザ定義（User Defined）] グループ テンプレートの 1 つを使用して新しいグループを作成する方法もあります。「カスタム ユーザ グループの作成 （25 ページ）」を参照してください。

RADIUS および TACACS+ での Cisco EPN Manager ユーザ グループの使用

Cisco EPN Manager に存在するユーザ グループを認識するように、RADIUS または TACACS+ サーバを設定する必要があります。RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート （26 ページ）の手順に従って、これを実行できます。

RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート

RADIUS または TACACS+ を使用している場合は、すべての Cisco EPN Manager ユーザ グループおよびロール情報を Cisco Access Control Server（ACS）または Cisco Identity Services Engine（ISE）サーバにコピーする必要があります。これを行うには、Cisco EPN Manager Web GUI にある [タスク リスト（Task List）] ダイアログボックスを使用します。データを Cisco ACS または Cisco ISE サーバにエクスポートしない場合、Cisco EPN Manager は、ユーザに割り当てられたタスクの実行を許可しません。

次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメインおよびロールの情報が必要です（タスクは自動的に追加されます）。
- RADIUS：仮想ドメインおよび権限の情報が必要です（タスクは自動的に追加されます）。

[タスク リスト（Task List）] ダイアログの情報は、Cisco ACS サーバ用に事前に書式設定されています。

（注） 外部サーバにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザで必須です。

始める前に

「外部認証の設定 （46 ページ） 」の説明に従い、AAA サーバを追加し、AAA モードを設定していることを確認してください。

ステップ 1 Cisco EPN Manager で、次の手順を実行します。

a) **[管理（Administration）] > [ユーザ（Users）] > [ユーザグループ（User Groups）]** を選択します。

b) [ユーザグループ（User Groups）] テーブルで、ユーザ グループ行の末尾にある [タスクリスト（Task List）] ハイパーリンクをクリックして、各ユーザ グループのロールをコピーします。

- RADIUS を使用している場合は、[RADIUSカスタム属性（RADIUS Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。
- TACACS+ を使用している場合は、[TACACS+カスタム属性（TACACS+ Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザ グループに情報を追加する方法を示しています。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ を使用した外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証 （49 ページ）

a) [ユーザ設定（User Setup）] または [グループ設定（Group Setup）] に移動します。

b) 該当するユーザまたはグループの [設定の編集（Edit Settings）] をクリックします。

c) 該当するテキスト ボックスに属性一覧を貼り付けます。

d) これらの属性を有効にするチェックボックスをオンにしてから、[送信して再起動（Submit + Restart）] をクリックします。

ユーザの追加およびユーザ アカウントの管理

管理者権限を持つ Web GUI ユーザの作成

インストール後、Cisco EPN Manager には **root** という名前の GUI ルート アカウントが作成されています。このアカウントは、サーバに初めてログインして次のものを作成するために使用されます。

- 製品および機能を管理する、管理者権限を持つ Web GUI ユーザ
- その他すべてのユーザ アカウント

通常の操作には Web GUI root アカウントを使用しないでください。セキュリティ上の理由から、管理者権限（およびすべてのデバイスへのアクセス権）を持つ新しい Web GUI ユーザを作成した後には Web GUI root アカウントを無効にしてください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザ（Users）] を選択します。

ステップ 2 [ユーザ名（Username）] テキストボックスにユーザ名を入力します。

ステップ 3 パスワードを入力します。新しいパスワードは、パスワードポリシーで指定された条件を満たす必要があります。[?] アイコンをクリックして、パスワードポリシーを表示します。

（オプション）[新しいパスワードを生成（Generate New Password）] ボタンをクリックして、システムによって生成されるセキュアなパスワードを設定します。このボタンをクリックすると、新しいパスワードが隣のテキストボックスに表示されます。[新しいパスワード（New password）] および [パスワードの確認（Confirm password）] テキストボックスにも同じものが表示されます。目のアイコンをクリックするとパスワードの表示/非表示が切り替わります。[コピー（Copy）] ボタンをクリックして、パスワードをクリップボードにコピーすることもできます。

ダイアログボックス内の値をクリアするには、[リセット（Reset）] ボタンをクリックします。

ステップ 4 （オプション）ユーザの [名（First Name）]、[姓（Last Name）]、および [説明（Description）] を入力します。

ステップ 5 [電子メールアドレス（Email Address）] テキストボックスに電子メールアドレスを入力します。

ステップ 6 [一般（General）] タブの [このユーザに割り当てられているグループ（Groups Assigned to This User）] で、[管理（Admin）] をクリックします。

ステップ 7 [仮想ドメイン（Virtual Domains）] タブをクリックして、ユーザがアクセスできるデバイスを指定します。すべてのデバイスへのアクセス権を持つ管理者 Web GUI ユーザ（ROOT-DOMAIN）を 1 つ以上作成する必要があります。仮想ドメインの詳細については、デバイスへのユーザ アクセスを制御するための仮想ドメインの作成 （36 ページ）を参照してください。

（注） 親仮想ドメインを選択すると、その下の子（従属）仮想ドメインも選択されます。

ステップ 8 [保存（Save）] をクリックします。

（注） 新しいユーザを作成するときは、ブラウザにユーザのログイン情報を自動入力したり保存したりしないでください。

次のタスク

まだ行っていない場合は、セキュリティ上の理由から、Web GUI ルート ユーザの無効化および有効化 （4 ページ）の説明に従って Web GUI root アカウントを無効にしてください。

ユーザの追加および削除

ユーザ アカウントを作成する前に、デバイス アクセスを制御するための仮想ドメインを作成し、アカウントの作成時にそれらの仮想ドメインを適用できるようにします。この作業を行わないと、ユーザアカウントを編集してドメインアクセスを追加しなければならなくなります。デバイスへのユーザ アクセスを制御するための仮想ドメインの作成 （36 ページ）を参照してください。

アカウントを（削除するのではなく）一時的に無効にするには、ユーザ アカウントの無効化（ロック） （30 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザ（Users）] を選択します。

ステップ 2 [ユーザの追加（Add User）] をクリックします。

ステップ 3 ユーザ アカウントを設定します。

a) ユーザ名とパスワードを入力します。

（注） パスワードを自動生成するには、ユーザ名と電子メールアドレスを入力します。詳細については、ユーザのパスワードの自動生成 （30 ページ）を参照してください。

b) ユーザの名、姓、説明を入力します。

c) ユーザが実行できるアクションを制御するために、1 つ以上のユーザ グループを選択します。ユーザ グループについては、ユーザ グループとそのメンバーの表示 （9 ページ）を参照してください。

d) ユーザがアクセスできるデバイスを制御するために、[仮想ドメイン（Virtual Domains）] タブをクリックし、ドメインをユーザに割り当てます。（デバイスへのユーザ アクセスを制御するための仮想ドメインの作成 （36 ページ）を参照）。

ステップ 4 **[保存（Save）]** をクリックします。

（注） 新しいユーザを作成するときは、ブラウザにユーザのログイン情報を自動入力したり保存したりしないでください。

ステップ 5 ユーザを削除するには、ユーザを選択して **[ユーザの削除（Delete User(s)）]** をクリックします。

ユーザ アカウントの無効化（ロック）

一時的にユーザが Cisco EPN Manager GUI にログインできないようにするには、ユーザ アカウントを無効にします。ユーザが一時的にジョブ機能を変更する場合にこのように設定することがあります。ユーザがログインしようとすると、Cisco EPN Manager では、アカウントがロックされているためにログインが失敗したことを伝えるメッセージが表示されます。ユーザを再作成することなく、後でアカウントをアンロックできます。ユーザアカウントを削除する場合は、ユーザの追加および削除 （29 ページ）を参照してください。

期限失効前にパスワードを変更しなかった場合は、自動的にユーザアカウントが無効になります。この場合、パスワードをリセットできるのは管理者だけです。ユーザのパスワードを変更する （30 ページ）およびローカル認証のためのグローバル パスワード ポリシーの設定 （33 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、次に [ユーザ（Users）] をクリックします。

ステップ 2 アクセスを無効または有効にするユーザを選択します。

ステップ 3 [ユーザのロック（Lock User(s)）]（または [ユーザのロック解除（Unlock User(s)）] をクリックします。

ユーザのパスワードを変更する

パスワードルールを設定して、ユーザにパスワードの変更を義務付けることができます（ローカル認証のためのグローバル パスワード ポリシーの設定 （33 ページ）を参照）。ユーザは、パスワードの変更の説明に従って、自分のパスワードを変更できます。ユーザのパスワードを手動で変更するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[ユーザ（Users）] をクリックします。

ステップ 2 ユーザ名のハイパーリンクをクリックします。

ステップ 3 新しいパスワードをパスワード フィールドに入力してから、[保存（Save）] をクリックします。

ユーザのパスワードの自動生成

Cisco EPN Manager には、電子メールサーバの可用性に基づいて新規および既存のユーザのパスワードを自動生成するオプションが用意されています。このオプションが有効になっている場合、システムはパスワードの詳細を含む電子メールをユーザに送信します。

（注） [パスワードの自動生成（Auto-generate Passwords）] オプションは、電子メールサーバが設定されている場合にのみ使用できます。

パスワードを自動生成してユーザに電子メールで送信するには、次の手順を実行します。

始める前に

電子メールサーバを設定します。詳細については、SMTP 電子メール サーバの設定を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles, & AAA）] > [ローカルパスワードポリシー（Local Password Policy）]** を選択します。

ステップ 2 [パスワードの自動生成（Auto-generate Passwords）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックして変更を保存します。

ステップ 4 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** に移動し、[ユーザ（Users）] をクリックします。

a) 新しいユーザの場合は、ユーザ名と電子メールアドレスを入力します。

b) 既存のユーザの場合は、[パスワードのリセット（Reset Password）] を選択します。

ステップ 5 [保存（Save）] をクリックして変更を保存し、ユーザに電子メール通知を送信します。

現在ログイン中のユーザの確認

現在 Cisco EPN Manager サーバにログインしているユーザを確認するには、この手順に従います。また、現在の Web GUI セッションおよび過去のセッションでユーザが実行した操作の履歴リストを参照することもできます。

（注） デフォルトでは、Cisco EPN Manager は後続の 50 個のレコードをページネーションなしで表示します。50 個を超えるレコードを表示するには、画面の右上隅にある [settings] アイコンをクリックし、**[My Preferences] > [General] > [Items per Page List]** フィールドに必要な値を入力します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、およびAAA（Users, Roles & AAA）]** を選択してから、[アクティブなセッション（Active Sessions）] を選択します。Cisco EPN Manager により、Cisco EPN Manager サーバに現在ログインしているすべてのユーザと、各ユーザのクライアント マシンの IP アドレスがリストされます。ユーザが管理対象デバイスに対して何らかのアクションを実行すると（ユーザが新しいデバイスを Cisco EPN Manager に追加する場合など）、デバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列にリストされます。

ステップ 2 このユーザが実行したすべてのアクションの履歴リストを表示するには、ユーザ名に対応する監査証跡アイコンをクリックします。

ステップ 3 アクティブなユーザセッションを終了する場合は、[セッションの終了（End Session）] をクリックします。

（注） [セッションの終了（End Session）] は、アクティブなユーザセッションのみを終了します。ユーザが再度ログインしないようにするには、ユーザ アカウントの無効化（ロック） （30 ページ）を参照してください。

ユーザが実行するタスクを表示する（監査証跡）

Cisco EPN Manager は、アクティブな Web GUI セッションおよび過去の Web GUI セッションでユーザが実行したすべてのアクションの履歴を保持します。特定のユーザまたは特定のユーザ グループのすべてのメンバーが実行したタスクの履歴を一覧表示するには、次の手順に従ってください。監査情報には、タスクの説明、ユーザがタスクを実行したクライアントの IP アドレス、およびタスクが実行された時刻が含まれます。タスクが管理対象デバイスに影響した場合（ユーザが新しいデバイスを追加したまたは [デバイスコンソール（Device Console）] を使用してネットワーク要素上でコマンドを発行した場合など）は、影響を受けたデバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列に表示されます。複数のデバイスが変更された場合（たとえば、ユーザが構成テンプレートを 10 個のスイッチに展開した場合）は、Cisco EPN Manager によって、各スイッチの監査エントリが表示されます。

Cisco EPN Manager Web GUI に現在ログインしているユーザを確認するには、「現在ログイン中のユーザの確認 （31 ページ）」を参照してください。

ユーザ固有ではない監査を表示するには、次のトピックを参照してください。

- GUI から実行されたアクションを監査する（システムの監査）
- 設定アーカイブとソフトウェア管理の変更を監査する（ネットワーク監査）
- ユーザによって行われる変更の監査（変更の監査）

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択します。

ステップ 2 特定のユーザが実行するタスクを表示するには：

1. [ユーザ（Users）] を選択します。
2. ユーザ名を見つけて、そのユーザに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ステップ 3 ユーザ グループのすべてのメンバーが実行したタスクの履歴リストを表示するには、次の手順に従ってください。

1. [ユーザ グループ（User Groups）] を選択します。

2. ユーザ グループ名を見つけて、そのグループに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ジョブ承認者を設定してジョブを承認する

ネットワークに大きな影響を与える可能性があるジョブを制御するには、ジョブ承認を使用します。ジョブを承認する必要がある場合は、Cisco EPN Manager が管理者権限を持っているすべてのユーザに電子メールを送信し、彼らの誰かが承認するまでジョブを実行しません。ジョブが承認者によって拒否された場合は、そのジョブがデータベースから削除されます。デフォルトでは、どのジョブでも承認は不要です。

ジョブ承認がすでに有効になっており、承認が必要なジョブを表示したり、ジョブを承認したり、ジョブを拒否したりする場合は、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）]** を選択してから、[ジョブ承認（Job Approval）] リンクをクリックします。

ジョブ承認を有効にし、実行する前に承認が必要なジョブを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[一般（General）] > [ジョブ承認（Job Approval）]** を選択します。

ステップ 2 [ジョブ承認の有効化（Enable Job Approval）] チェックボックスをオンにします。

ステップ 3 承認用に設定するジョブを探して、それらを左側のフィールドから右側のフィールドに移動します。たとえば、管理ユーザがデバイスの新規追加を承認するように設定する場合は、[インポートジョブ（Import job）] タイプを移動します。

ステップ 4 カスタマイズされたジョブのタイプを指定するには、正規表現を使用して [ジョブ タイプ（Job Type）] フィールドに文字列を入力し、[追加（Add）] をクリックします。たとえば、Config で始まるすべてのジョブ タイプに対してジョブ承認を有効にするには、「**Config.***」と入力します。

ステップ 5 [保存（Save）] をクリックします。

ローカル認証のためのグローバルパスワードポリシーの設定

ローカル認証（Cisco EPN Manager の認証メカニズム）を使用している場合、Web GUI からグローバル パスワード ポリシーを制御します。外部認証を使用して Cisco EPN Manager ユーザを認証している場合、ポリシーは、外部アプリケーションによって制御されます（CLI を使用した外部認証の設定を参照）。

デフォルトでは、ユーザは、任意の期間の経過後にパスワードの変更が強制されることはありません。パスワード変更を強制し、他のパスワード ルールを設定するには、**[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ローカル パスワード ポリシー（Local Password Policy）] を選択します。

（注） 新しいユーザが Cisco EPN Manager への初回ログイン時にデフォルトのパスワードを変更するように要求するには、[パスワードの変更（Change password）] を選択する必要があります。このチェックボックスをオフにすると、ログイン時に [ホームダッシュボード（Home Dashboard）] ページが開きます。

許可される同時セッションの数の設定

Cisco EPN Manager は、同時に実行できる同時セッションの数を設定するオプションを提供します。最大 15 の同時セッションを設定できます。

（注） この設定は、Cisco EPN Manager Web インターフェイスからログインしたセッションにのみ適用されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバ（Server）]** を選択します。

ステップ 2 [Parallel Sessions] で、[Number of parallel sessions allowed] フィールドに 1 ～ 50 の範囲の値を入力します。

ステップ 3 [保存（Save）] をクリックします。この変更を有効にするには、システムを再起動する必要があります。

アイドルユーザ用のグローバルタイムアウトを設定する

Cisco EPN Manager には、アイドル ユーザを自動的にログアウトするタイミングと方法を制御する、以下の 2 つの設定があります。

- [ユーザ アイドル タイムアウト（User Idle Timeout）] : タイムアウトになったときにユーザセッションを自動的に終了するこの設定を無効にするか設定することができます。この設定はデフォルトで有効になっており、15 分に設定されています。
- [グローバル アイドル タイムアウト（Global Idle Timeout）] : [ユーザ アイドル タイムアウト（User Idle Timeout）] 設定よりも優先されます。[グローバルアイドルタイムアウト（Global Idle Timeout）] はデフォルトで有効になっており、15 分に設定されています。管理者権限を持つユーザのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を無効化したり、そのタイムリミットを変更できます。

アイドルタイムアウト機能は、ブラウザが開くと動作し始めますが、ユーザの操作はありません。つまり、アイドルタイムアウトが10分で、ブラウザが開いており、ユーザにキーストロークやマウスクリックがない場合、ユーザは10分間非アクティブになるとログアウトされます。ただし、ブラウザがCisco EPN Managerからログアウトすることなく強制終了されると、デフォルトではCisco EPN Managerに設定されたアイドルタイムアウト値に関わらず、60分後に期限切れになります。

デフォルトで、クライアント セッションは無効になっており、ユーザは 15 分間非アクティブだった場合に自動的にログアウトされます。これは、すべてのユーザに適用されるグローバル設定です。セキュリティ上の理由から、このメカニズムは無効にしないでください。ただし、次の手順を使用して、タイムアウト値を調整できます。アイドルユーザのタイムアウトを無効にする/変更するには、以下を参照してください。アイドル ユーザのタイムアウトの無効化（35 ページ）

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[一般（General）] > [サーバ（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] 領域で、[すべてのアイドル ユーザをログアウトする（Logout all idle users）] チェックボックスがオンになっていること確認します（これは、メカニズムが有効になっていることを意味します）。

ステップ 3 [後にすべてのアイドル ユーザをログアウトする（Logout all idle users after）] ドロップダウン リストで、値を選択することによって、タイムアウトを設定します。

ステップ 4 [保存（Save）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

アイドル ユーザのタイムアウトの無効化

デフォルトでは、一定の期間にわたって何も行われないと、クライアントセッションが無効になりユーザは自動的にログアウトされます。これはすべてのユーザに適用されるグローバル設定です。インストール中にログアウトしないようにするには、次の手順に従って、システム設定でアイドル ユーザの自動ログアウトを無効にすることを推奨します。

（注） [グローバル アイドル タイムアウト（Global Idle Timeout）] 設定は、[ユーザ アイドル タイムアウト（User Idle Timeout）] 設定より優先されます。グローバルアイドルタイムアウトを設定するには、『CiscoPrime Infrastructure Administrator Guide』を参照してください。

顧客がシステム設定で [すべてのアイドルユーザをログアウト（Logout all idle users）] を無効にするか、またはルートユーザのマイプリファレンス設定で [アイドルユーザをログアウト（Logout idle user）] を無効にするか、あるいはその両方で無効にするかに関係なく、Web サーバのセッションタイムアウトに到達すると、セッションは最終的にタイムアウトします。これは、基本的にセキュリティポスチャを維持するためです。セッションタイムアウトの増減に関

するガイドラインについては、https://owasp.org/www-community/Session_Timeout を参照してください。

（注） セッションは非アクティブな場合にのみタイムアウトしますが、アクティブなユーザセッションはタイムアウトしません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバ（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] エリアで、[すべてのアイドル ユーザをログアウトする（Logout all idle users）] チェックボックスをオフにし、[保存（Save）] をクリックします。

ステップ 3 Web GUI ウィンドウの右上にある ⚙ をクリックし、[マイ プリファレンス（My Preferences）] を選択します。

ステップ 4 [ユーザ アイドル タイムアウト（User Idle Timeout）] エリアで [アイドル状態ユーザのログアウト（Logout idle user）] チェックボックスをオフにし、[保存（Save）] をクリックします。

アイドル タイムアウトの値を変更する必要がある場合は、[アイドル状態ユーザのログアウト（Logout idle user）] チェックボックスをオンにし、[アイドル ユーザをログアウトするまでの時間（Logout idle user after）] ドロップダウンリストから、アイドル タイムアウト制限を 1 つ選択します。（ただし、この値は [グローバル アイドル タイムアウト（Global Idle Timeout）] に設定されている値を超えることはできません）。

ステップ 5 [保存（Save）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

デバイスへのユーザアクセスを制御するための仮想ドメインの作成

• 仮想ドメインの編集 （43 ページ）
• 仮想ドメインの削除 （44 ページ）

仮想ドメインとは

仮想ドメインは、デバイス、サイト、およびその他の NE の論理グループで、それらの NE にアクセスできるユーザを制御するために使用されます。仮想ドメインに含める要素とその仮想ドメインへのアクセス権を付与するユーザを選択します。仮想ドメインは、物理サイト、デバイス タイプ、ユーザ コミュニティ、または選択するあらゆる指定項目に基づいて設定できます。すべてのデバイスはROOT-DOMAINに属します。ROOT-DOMAINはすべての新しい仮想ドメインの親ドメインです。

仮想ドメインは、ユーザ グループと連携します。仮想ドメインは、ユーザがアクセスできるデバイスを制御しますが、ユーザ グループは、ユーザがそれらのデバイスで実行できるアクションを決定します。仮想ドメインへのアクセス権を持つユーザは、ユーザの権限に応じて、デバイスを設定したり、アラームを表示したり、仮想ドメインの NE に関するレポートを生成したりできます。

デバイスを Cisco EPN Manager に追加したら、仮想ドメインを作成できます。各仮想ドメインには名前が必要です。必要に応じて、説明、電子メール アドレス、およびタイム ゾーンも指定できます。Cisco EPN Manager はドメイン固有のレポートをスケジュールおよび電子メール送信する際に、この電子メール アドレスとタイム ゾーンを使用します。

ユーザは、一度に 1 つの仮想ドメインで作業します。ユーザは、[仮想ドメイン（Virtual Domain）] ドロップダウン リストから別の仮想ドメインを選択することによって、現在の仮想ドメインを変更できます（別の仮想ドメインで作業するを参照してください）。

仮想ドメインをセットアップする前に、ネットワークの特定の領域を管理するユーザを決定します。次に、ニーズに応じて（たとえば、地域ごと、デバイス タイプごと、ネットワークが機能するユーザ コミュニティごと）仮想ドメインを編成します。

仮想ドメインが Cisco EPN Manager 機能に及ぼす影響

仮想ドメインは、階層構造で編成されています。ROOT-DOMAIN ドメインには、すべての仮想ドメインが含まれています。

ネットワーク要素は階層的に管理されるため、デバイス（および一部の関連する機能とコンポーネント）のユーザ ビューがユーザの仮想ドメインの影響を受けます。次のトピックでは、これらの機能に対する仮想ドメインの影響について説明します。

• レポートと仮想ドメイン （38 ページ）
• 検索と仮想ドメイン （38 ページ）
• アラームと仮想ドメイン （38 ページ）
• マップおよび仮想ドメイン （38 ページ）
• 設定テンプレートと仮想ドメイン （38 ページ）

• グループおよび仮想ドメインの設定 （39 ページ）
• 電子メール通知と仮想ドメイン （39 ページ）

レポートと仮想ドメイン

レポートには、アクティブ仮想ドメインに属しているコンポーネントのみが含まれています。親仮想ドメインは、その子ドメインからのレポートは表示できません。新しいコンポーネントは、その追加後に生成されたレポートにのみ反映されます。

検索と仮想ドメイン

検索結果には、アクティブ ドメインに属しているコンポーネントのみが含まれます。検索が実行され保存されたドメインと同じドメインに位置している場合にのみ保存した検索結果が表示されます。親ドメインで作業する場合、子ドメインで実行した検索結果は表示されません。

アラームと仮想ドメイン

コンポーネントが仮想ドメインに追加された場合、そのコンポーネントの以前のアラームは、該当する仮想ドメインに表示されません。新しいアラームだけが表示されます。たとえば、ネットワーク要素が Cisco EPN Manager に追加され、追加の前後でそのネットワーク要素がアラームを生成した場合は、追加後に生成されたアラームのみがアラーム履歴に記録されます。

（注） アラーム電子メール通知の場合は、ROOT-DOMAIN 仮想ドメインだけがロケーション通知、ロケーション サーバ、および Cisco EPN Manager 電子メール通知を有効にできます。

マップおよび仮想ドメイン

マップには、アクティブな仮想ドメインのメンバーであるネットワーク要素のみが表示されます。

設定テンプレートと仮想ドメイン

仮想ドメインで作成または検出した設定テンプレートは、その仮想ドメイン内のネットワーク要素にのみ適用できます。テンプレートをデバイスに適用してから、そのデバイスを子ドメインに追加した場合は、その子ドメイン内の同じデバイスでもテンプレートを使用できるようになります。

（注） 子ドメインを作成してから、設定テンプレートを仮想ドメイン内の両方のネットワーク要素に適用した場合は、テンプレートが適用されたパーティションの数が Cisco EPN Manager に正しく反映されない場合があります。

グループおよび仮想ドメインの設定

親ドメインは、子ドメインの設定グループ内のネットワーク要素を表示できます。親ドメインは、子ドメインの設定グループを編集することもできます。

電子メール通知と仮想ドメイン

仮想ドメインごとに電子メール通知を設定できます。

アラーム電子メール通知の場合は、ROOT-DOMAIN だけがロケーション通知、ロケーション サーバ、および電子メール通知を有効にできます。

新しい仮想ドメインの作成

新しい仮想ドメインを作成するには、仮想ドメインの目的の階層に応じて、次のいずれかの手順を実行します。

新しい仮想ドメイン（*new-domain*）の作成場所：	**手順の参照先：**
ROOT-DOMAIN > ***new-domain***	ROOT-DOMAIN 直下での仮想ドメインの作成 （39 ページ）
ROOT-DOMAIN > *existing-domain* > ***new-domain***	子仮想ドメイン（サブドメイン）の作成 （40 ページ）
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
（その他）	

ROOT-DOMAIN 直下での仮想ドメインの作成

ROOT-DOMAIN の下に空の仮想ドメインを作成する手順を次に示します。また、複数の仮想ドメインを一括に作成するには、仮想ドメインのリストのインポート （41 ページ）の手順を使用します。

ROOT-DOMAIN の下に仮想ドメインがすでに存在しており、その仮想ドメインの下に新しいドメイン（子ドメイン）を作成するには、子仮想ドメイン（サブドメイン）の作成 （40 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで [+] アイコン（[新規ドメインの追加（Add New Domain）]）をクリックします。

ステップ 3 [名前（Name）] テキスト ボックスに名前を入力します。これは必須です。

ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）] をクリックして、新しく作成された仮想ドメインの概要を表示します。

次のタスク

仮想ドメインへのネットワーク デバイスの追加 （42 ページ）の説明に従って、仮想ドメインにデバイスを追加します。

子仮想ドメイン（サブドメイン）の作成

次の手順を実行すると、仮想子ドメイン（サブドメインともいう）が作成されます。子仮想ドメインはROOT-DOMAINの直下にあるドメインではなく、ROOT-DOMAIN直下のドメインの下にあるドメインです。

ROOT-DOMAIN の直下に新しい仮想ドメインを表示させるには、この手順を使用しないでください。その場合には、ROOT-DOMAIN 直下での仮想ドメインの作成 （39 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** を選択します。

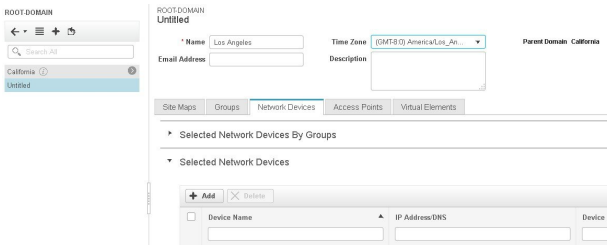
ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、次の手順を実行します。

a) その下に新しい子ドメインを作成するドメインを見つけます。（これは親ドメインと呼ばれます。）この例では、親ドメインは **California** です。

b) ドメイン名の隣にある情報（[i]）アイコンをクリックします。データ ポップアップ ウィンドウが開きます。

c) ポップアップ ウィンドウで、[サブドメインの作成（Create Sub Domain）] をクリックします。ナビゲーション ペインがリスト ビューに切り替わり、親ドメイン [California] が [無題（Untitled）] の上に表示されます。

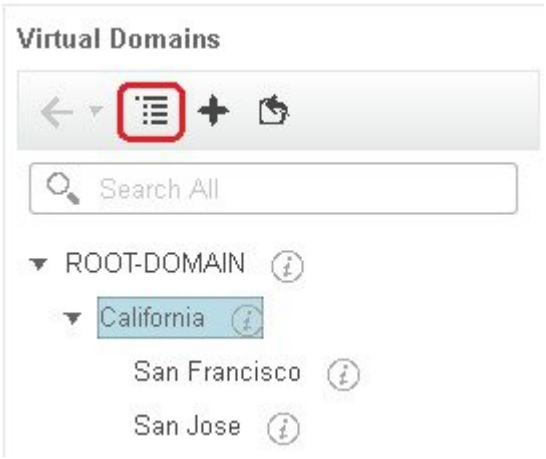
ステップ 3 [名前（Name）] テキスト ボックスに名前を入力します。これは必須です。この例では、新しい子ドメインに **Los Angeles** という名前を付けます。（ナビゲーション ペインに表示される名前は、新しい子ドメインを保存するまでは、[無題（Untitled）] から [Los Angeles] に変更されません。）



ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）] をクリックし、新しい子ドメインを作成することを確認します。階層ビューに戻るには、ナビゲーション ペイの上部にある表示トグル ボタンをクリックします。

表示が階層ビューに戻ります。



次のタスク

仮想ドメインへのネットワーク デバイスの追加 （42 ページ）の説明に従って、仮想ドメインにデバイスを追加します。

仮想ドメインのリストのインポート

複数の仮想ドメインを作成する予定の場合、またはドメインを複雑な階層にする場合は、より簡単な方法として、それらを正しくフォーマットされた CSV ファイルで指定して、そのファイルをインポートできます。CSV フォーマットを使用すれば、作成した仮想ドメインだけでなく、その親ドメインの名前、説明、タイム ゾーン、および電子メール アドレスも指定できます。仮想ドメインへのネットワーク要素の追加は、別途行う必要があります。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [ドメインのインポート（Import Domain(s)）] アイコンをクリックし、ポップアップに表示されるリンクからサンプル CSV ファイルをダウンロードして CSV ファイルを用意します。

ステップ 3 [ファイルの選択（Choose File）] をクリックし、CSV ファイルに移動します。

ステップ 4 [インポート（Import）] をクリックして、CSV ファイルをインポートし、指定した仮想ドメインを作成します。

次のタスク

仮想ドメインにデバイスを追加します（仮想ドメインへのネットワーク デバイスの追加 （42 ページ）を参照）。

仮想ドメインへのネットワーク デバイスの追加

ネットワーク デバイスを仮想ドメインに追加するには、次の手順に従います。新しいネットワーク デバイスを既存の仮想ドメインに追加すると、そのドメインへのアクセス権を持つユーザに対し、追加されたネットワーク デバイスがただちにアクセス可能になります（Web GUI を再起動する必要はありません）。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、ネットワーク デバイスを追加する仮想ドメインをクリックします。

ステップ 3 [ネットワーク デバイス（Network Devices）] タブをクリックし、[追加（Add）] をクリックします。

ステップ 4 ドメインに追加するネットワーク デバイスを選択します。[ネットワーク デバイスの選択（Select Network Devices）] ダイアログには、親ドメインに含まれるデバイスだけでなく、管理対象デバイスのすべてがリストされることに注意してください。親ドメインに含まれていないデバイスを追加すると、Cisco EPN Manager により、そのデバイスは子ドメインと親ドメインの両方に追加されます。

a) ドメインに追加するデバイスを選択します。[フィルタ条件（Filter By）] ドロップダウン リストを使用して、追加するデバイスを見つけることができます。

b) [選択（Select）] をクリックします。

（注） [すべて選択（Select All）] 機能を使用して、1 つのショットに 500 を超えるネットワークデバイスを追加することはできません。500 を超えるデバイスを追加するには、[フィルタ条件（Filter By）] オプションを複数回使用します。

ステップ 5 [送信（Submit）] をクリックして、仮想ドメインの内容を表示します。

ステップ 6 [保存（Save）] をクリックして変更を確定します。

次のタスク

ユーザへの仮想ドメインの割り当て （43 ページ）で説明されている手順に従って、仮想ドメインへのアクセス権をユーザに付与します。

ユーザへの仮想ドメインの割り当て

仮想ドメインをユーザアカウントに割り当てると、そのユーザが表示して操作を実行できるデバイスは、ユーザに割り当てられたドメイン内のデバイスに制限されます。

（注） 外部 AAA を使用しているときは、外部 AAA サーバの該当するユーザまたはグループ設定に仮想ドメインのカスタム属性を追加してください。RADIUS と TACACS+ で Cisco EPN Manager 仮想ドメインを使用する （44 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）] > [ユーザ（Users）]** の順に選択します。

ステップ 2 デバイス アクセス権を付与するユーザを選択します。

ステップ 3 [仮想ドメイン（Virtual Domains）] タブをクリックします。

ステップ 4 [追加（Add）] ボタンと [削除（Remove）] ボタンを使用して割り当てを変更してから、[保存（Save）] をクリックします。

仮想ドメインの編集

仮想ドメインを調節するには、左側のサイドバー メニューの [仮想ドメイン階層（Virtual Domain Hierarchy）] から仮想ドメインを選択し、このドメインに割り当てられているネットワーク デバイスを表示または編集します。ROOT-DOMAIN の設定はすべて編集できません。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、編集する仮想ドメインをクリックします。

ステップ 3 名前、電子メール アドレス、タイム ゾーン、説明を調整するには、テキスト ボックスに変更内容を入力します。

ステップ 4 デバイス メンバーを調整するには、次の手順を実行します。

- デバイスを追加するには、[追加（Add）] をクリックし、仮想ドメインへのネットワーク デバイスの追加 （42 ページ）の手順に従います。
- デバイスを削除するには、デバイスのチェックボックスを使用してデバイスを選択し、[削除（Delete）] をクリックします。

ステップ 5 [送信（Submit）] をクリックし、変更内容のサマリーを確認します。

ステップ 6 [保存（Save）] をクリックして編集内容を適用、保存します。

仮想ドメインの削除

仮想ドメインをCisco EPN Managerから削除するには、以下の手順に従います。この手順では、仮想ドメインだけが削除され、ネットワーク要素は Cisco EPN Manager から削除されません（ネットワーク要素は引き続き Cisco EPN Manager で管理されます）。

始める前に

仮想ドメインを削除できるのは、以下の場合に限られます。

- 仮想ドメインにネットワーク要素も子ドメインも一切含まれていない場合。
- ユーザがアクセスできる唯一のドメインではない場合。つまり、Cisco EPN Manager ユーザがそのドメインにしかアクセスできない場合、ドメインを削除することはできません。
- ドメインにログインしているユーザがいない場合。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、仮想ドメイン名の横にある情報（[i]）アイコンをクリックします。これにより、データ ポップアップ ウィンドウが開きます。

ステップ 3 ポップアップ ウィンドウで [削除（Delete）] をクリックします。

ステップ 4 [OK] をクリックして、仮想ドメインの削除を確認します。

RADIUS と TACACS+ で Cisco EPN Manager 仮想ドメインを使用する

RADIUS または TACACS+ サーバは、Cisco EPN Manager 内に存在する仮想ドメインを認識するように設定する必要があります。これを実行するは、「RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （44 ページ） 」の手順を使用します。

RADIUS または TACACS+ サーバにユーザ向けの仮想ドメイン情報が保存されていない場合は、Cisco EPN Manager で設定された仮想ドメインの数に応じて、以下が発生します。

- Cisco EPN Manager に 1 つの仮想ドメイン（ROOT-DOMAIN）しか割り当てられていない場合は、デフォルトで ROOT-DOMAIN がユーザに割り当てられます。
- Cisco EPN Manager に複数の仮想ドメインが割り当てられている場合は、ユーザがログインできなくなります。

RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート

RADIUS または TACACS+ を使用する場合は、Cisco EPN Manager 仮想ドメイン情報をすべて Cisco ACS または Cisco ISE サーバにコピーする必要があります。Cisco EPN Manager Web GUI に表示される [仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログボックスを使用して、この操作を実行できます。Cisco ACS または Cisco ISE サーバにデータをエクスポートしない場合、Cisco EPN Manager ではユーザがログインできなくなります。

使用するプロトコルに応じて、次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメイン、権限、およびタスク情報が必要です。
- RADIUS：仮想ドメインとロールの情報が必要です（タスクは自動的に追加されます）。

既存の仮想ドメインの子ドメインを作成すると、親仮想ドメインでRADIUS/TACACS+カスタム属性のシーケンス番号も更新されます。これらのシーケンス番号は表示専用で、AAA 統合には影響しません。

[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログボックスの情報は、Cisco ACS サーバで使用できるように事前にフォーマットされています。

（注） 外部サーバにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザで必須です。

始める前に

外部認証の設定 （46 ページ）の説明に従い、AAA サーバを追加し、AAA モードを設定していることを確認してください。

ステップ 1 Cisco EPN Manager で、次の手順を実行します。

a) **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

b) ウィンドウ右上の [カスタム属性のエクスポート（Export Custom Attributes）] をクリックします。これにより、[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログが表示されます。

c) 属性リストをコピーします。

- RADIUS を使用する場合は、[RADIUS カスタム属性（RADIUS Custom Attributes）] フィールドのすべてのテキストを選択して右クリックし、[コピー（Copy）] を選択します。
- TACACS+を使用している場合は、[TACACS+カスタム属性（TACACS+Custom Attributes）]フィールドですべてのテキストを右クリックして、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザ グループに情報を追加する方法を示しています。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ による外部認証 （55 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （49 ページ）

a) [ユーザ設定（User Setup）] または [グループ設定（Group Setup）] に移動します。

ユーザ ベースで仮想ドメインを指定する場合、（たとえば、タスク、ロール、仮想ドメインなど）すべてのカスタム属性情報を[User]カスタム属性ページに追加していることを確認する必要があります。

a) 該当するユーザまたはグループの [設定の編集（Edit Settings）] をクリックします。

b) 該当するテキスト ボックスに属性一覧を貼り付けます。
c) これらの属性を有効にするチェックボックスをオンにしてから、[送信して再起動（Submit＋Restart）] をクリックします。

ローカル認証の設定

Cisco EPN Manager はデフォルトでローカル認証を使用します。つまり、ユーザ パスワードが Cisco EPN Manager データベースに保管されて、データベース内のパスワードが検証されます。使用中の認証モードを確認するには、**[管理（Administration）]>[ユーザ（Users）]>[ユーザ、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、**[AAA モードの設定（AAA Mode Settings）]** を選択します。これにより、[AAA モードの設定（AAA Mode Settings）] ページが表示されます。ローカル認証を使用する場合、必ず強力なパスワード ポリシーを設定する必要があります。ローカル認証のためのグローバル パスワード ポリシーの設定 （33 ページ）を参照してください。

ローカル認証で SSO を使用するには、ローカル認証での SSO の使用 （46 ページ）を参照してください。

外部認証については、「外部認証の設定 （46 ページ） 」を参照してください。

ローカル認証での SSO の使用

ローカル認証で SSO を使用するには、SSO サーバを追加し、ローカル モードで SSO を使用するように Cisco EPN Manager を設定する必要があります。

プライマリ サーバとバックアップ サーバが存在するハイ アベイラビリティ環境で Cisco EPN Manager を導入した場合、HA 環境での SSO サーバの設定の手順を参照してください。

Cisco EPN Manager は、SSO サインイン ページでのローカライズをサポートしていません。

以下のトピックでは、外部認証用に SSO を設定する方法について説明していますが、同じ手順を使用して、ローカル認証用に SSO を設定することもできます。唯一の違いは、Cisco EPN Manager サーバで SSO モードを設定するときに、[ローカル（Local）] モード（RADIUS や TACACS+ ではない）を選択することです。

-
- SSO サーバの追加 （62 ページ）
- Cisco EPN Manager サーバ上で SSO モードを設定する （63 ページ）

外部認証の設定

Web GUI のルートユーザまたはスーパーユーザ権限を持つユーザは、外部認証、認可、およびアカウンティング（AAA）のために外部 LDAP、RADIUS、TACACS+、SSO サーバと通信す

るように Cisco EPN Manager を設定できます。外部認証を設定することを選択した場合、ユーザ グループ、ユーザ、認証プロファイル、認証ポリシー、およびポリシー ルールが、Cisco EPN Manager へのすべてのアクセス要求がルーティングされる外部サーバで作成済みである必要があります。

最大 3 つの AAA サーバを使用できます。ユーザは、最初のサーバが到達不能であるかネットワークに問題がある場合にのみ、2 番目のサーバで認証されます。

（注） 同じ RADIUS、TACACS+、または LDAP プロトコルをサポートしている場合にのみ、最大 3 つの AAA サーバを一緒に使用できます。プロトコルが異なるサーバどうしを一緒に使用することは、サポートされていません。ただし、異なるプロトコルを実行している複数の AAA サーバを使用する場合は、Cisco ISE または ACS を EPNM と AAA サーバ間のプロキシとして使用する必要があります。この場合、Cisco ISE または Cisco ACS の設定に基づいて認証ロジックを設定する必要があります。

CLI から外部認証を設定するには、CLI を使用した外部認証の設定を参照してください。

詳細については、次のトピックを参照してください。

- Cisco ISE と RADIUS または TACACS+ による外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証 （49 ページ）
- Cisco ACS と RADIUS または TACACS+ による外部認証 （55 ページ）
- SSO による外部認証 （62 ページ）

外部認証での RADIUS または TACACS+ の使用

以下のトピックでは、RADIUS または TACACS+ サーバを使用するように Cisco EPN Manager を設定する方法について説明します。

- Cisco EPN Manager への RADIUS または TACACS+ サーバの追加 （47 ページ）
- Cisco EPN Manager サーバ上で RADIUS または TACACS+ モードを設定する （48 ページ）

Cisco EPN Manager への RADIUS または TACACS+ サーバの追加

RADIUS または TACACS+ サーバを Cisco EPN Manager に追加するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[RADIUS サーバ（RADIUS Servers）] を選択します。

ステップ 2 追加するサーバのタイプを選択します。

- RADIUS の場合は、[RADIUS サーバ（RADIUS Servers）] を選択します。[コマンドの選択（Select a command）] ドロップダウン リストから、[RADIUS サーバの追加（Add RADIUS Server）] を選択し、[実行（Go）] をクリックします。

- TACACS+ の場合は、[TACACS+ サーバ（TACACS+ Servers）] を選択します。[コマンドの選択（Select a command）] ドロップダウン リストから、[TACACS+ サーバの追加（Add TACACS+ Server）] を選択し、[実行（Go）] をクリックします。

（注） [上へ移動（Move Up）] および [下へ移動（Move Down）] 矢印を使用して、使用可能な IP アドレスの順序を並べ替えることができます。

ステップ 3 必要な情報（IP アドレス、DNS 名など）を入力します。Cisco EPN Manager が外部認証サーバと通信するためには、このページで入力する共有秘密が RADIUS または TACACS+ サーバに設定された共有秘密と一致している必要があります。サードパーティ製の TACACS+ または RADIUS サーバ用の共有秘密キーを入力するときに、'（一重引用符）と "（二重引用符）を除く、アルファベット、数字、および特殊文字を使用できます。

ステップ 4 認証タイプを選択します。

- PAP：パスワード ベースの認証は、2 つのエンティティが 1 つのパスワードを事前に共有し、そのパスワードを認証の基準に使用するプロトコルです。
- CHAP：チャレンジ ハンドシェイク認証プロトコルでは、クライアントとサーバの両方がプレーンテキストの秘密キーを認識しており、その秘密キーは絶対にネットワーク上に送信されないことが必要になります。CHAP は、パスワード認証プロトコル（PAP）より優れたセキュリティを提供します。

ステップ 5 高可用性機能を有効にして、**[ローカルインターフェイス IP（Local Interface IP）]** に仮想 IP アドレスを設定した場合、**eth0** の仮想 IP アドレスを選択します。（セカンダリ サーバでの高可用性の設定とインストールについては、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください）。

（注） 外部認証サーバに設定された IP アドレスは、[ローカル インターフェイス IP（Local Interface IP）] の値と一致していなければなりません。

ステップ 6 [保存（Save）] をクリックします。

Cisco EPN Manager サーバ上で RADIUS または TACACS+ モードを設定する

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[AAA モード（AAA Mode）] を選択します。

ステップ 2 [TACACS+] または [RADIUS] を選択します。

ステップ 3 [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバがダウンした場合にローカル データベースの使用が有効になります。

ステップ 4 外部 RADIUS または TACACS+ サーバがダウンした場合にローカル認証に戻すには、次の手順を実行します。

a) [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] を選択します。

b) フォールバック条件（[サーバが応答しないときのみ（ONLY on no server response）] または [認証に失敗したかサーバが応答しないとき（on authentication failure or no server response）]）を指定します。

ステップ 5 [保存（Save）] をクリックします。

Cisco ISE と RADIUS または TACACS+ による外部認証

Cisco Identity Services Engine（ISE）は、認証、認可、およびアカウンティング（AAA）に RADIUS または TACACS+ プロトコルを使用します。Cisco ISE に Cisco EPN Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco EPN Manager ユーザを認証できます。外部認証を使用する場合は、ユーザ、ユーザ グループ、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ISE データベースから保存および確認する必要があります。

（注） Cisco EPN Manager は LDAP をネイティブにサポートしています。

Cisco ISE で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ISE を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ISE のサポートされるバージョンを使用していることを確認します。	Cisco EPN Manager でサポートされる Cisco ISE のバージョン（50 ページ）
Cisco ISE で Cisco EPN Manager を AAA クライアントとして追加します。	Cisco ISE にクライアントとして Cisco EPN Manager を追加する （50 ページ）
Cisco ISE でユーザ グループを作成します。	Cisco ISE でのユーザ グループの作成 （51 ページ）
Cisco ISE でユーザを作成し、そのユーザを Cisco ISE で作成したユーザ グループに追加します。	Cisco ISE でのユーザの作成およびユーザ グループへのユーザの追加 （51 ページ）
（RADIUS を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、Cisco EPN Manager で作成したユーザ ロールと仮想ドメインを使用して RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザ タスクの属性を追加する必要はありません。これらはユーザ ロールに基づいて自動的に追加されます。	Cisco ISE での RADIUS の認証プロファイルの作成 （51 ページ）

（TACACS+ を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、で作成したユーザ ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 Cisco EPN Manager （注） TACACS+ では、ユーザ タスクの属性を追加する必要はありません。これらはユーザ ロールに基づいて自動的に追加されます。	Cisco ISE での TACACS+ の認証プロファイルの作成 （52 ページ）
Cisco ISE で認証ポリシーを作成し、Cisco ISE で作成したユーザ グループと認証プロファイルにポリシーを関連付けます	Cisco ISE での認可ポリシーを設定する （53 ページ）
認証ポリシーを作成して、Cisco ISE が Cisco EPN Manager と通信するために使用する必要があるプロトコルと Cisco EPN Manager に対してユーザを認証するために使用するアイデンティティ ソースを定義します。	Cisco ISE での認証ポリシーの作成 （54 ページ）
Cisco EPN Manager で RADIUS または TACACS+ サーバとして Cisco ISE を追加します。	
Cisco EPN Manager サーバで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバ上で RADIUS または TACACS+ モードを設定する （48 ページ）

Cisco EPN Manager でサポートされる Cisco ISE のバージョン

Cisco EPN Manager は Cisco ISE 1.*x* および 2.*x* リリースをサポートしています。

Cisco ISE にクライアントとして Cisco EPN Manager を追加する

ステップ 1 admin ユーザとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [追加（Add）] をクリックします。

ステップ 4 Cisco EPN Manager サーバのデバイス名と IP アドレスを入力します。

ステップ 5 [認証設定（Authentication Settings）] チェックボックスをオンにして、共有秘密を入力します。

（注） この共有秘密は、Cisco EPN Manager で Cisco ISE サーバを RADIUS サーバとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ISE でのユーザ グループの作成

ステップ 1 管理ユーザとして Cisco ISE にログインします。
ステップ 2 **[管理（Administration）] > [ID管理（Identity Management）] > [グループ（Groups）]** を選択します。
ステップ 3 [ユーザ アイデンティティ グループ（User Identity Groups）] ページで、[追加（Add）] をクリックします。
ステップ 4 [アイデンティティ グループ（Identity Group）] ページで、ユーザ グループの名前と説明を入力します。
ステップ 5 **[送信（Submit）]** をクリックします。

Cisco ISE でのユーザの作成およびユーザ グループへのユーザの追加

ステップ 1 管理ユーザとして Cisco ISE にログインします。
ステップ 2 **[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）]** を選択します。
ステップ 3 [ネットワーク アクセス ユーザ（Network Access Users）] ページで [追加（Add）] をクリックします。
ステップ 4 [項目の選択（Select an item）] ドロップダウン リストから、ユーザを割り当てるユーザ グループを選択します。
ステップ 5 **[送信（Submit）]** をクリックします。

Cisco ISE での RADIUS の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN接続を介してネットワークへのアクセスを試みるユーザには、有線接続を介してネットワークへのアクセスを試みるユーザよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザ ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザ ロールの属性を追加できます。タスクはユーザ ロールによって自動的に追加されます。

Cisco ISE の認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーとプロファイルの管理に関する情報を参照してください。

Cisco ISE で RADIUS の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示す RADIUS のすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ISE に追加する必要があります。

- Cisco EPN Manager ユーザ ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート （26 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （44 ページ）を参照してください。

ステップ 1 管理ユーザとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** を選択します。

ステップ 3 左側のサイドバーのメニューから **[認証（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 4 [標準認証プロファイル（Standard Authorization Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [認証プロファイル（Authorization Profile）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 6 [アクセス タイプ（Access Type）] ドロップダウンリストから、[ACCESS_ACCEPT] を選択します。

ステップ 7 [詳細な属性設定（Advanced Attributes Settings）] エリアで、次のアイテムのずべての RADIUS カスタム属性のリストを貼り付けます。

- ユーザ ロール
- 仮想ドメイン

（注） ユーザ タスクを追加する場合は、必ずホーム メニュー アクセス タスクを追加してください。これは必須です。

ステップ 8 **[送信（Submit）]** をクリックします。

Cisco ISE での TACACS+ の認証プロファイルの作成

権限プロファイルを作成して、さまざまなタイプのユーザにネットワークへのアクセスを認可する方法を定義できます。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザには、有線接続を介してネットワークへのアクセスを試みるユーザよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザ ロール、タスク、仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

Cisco ISE 認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーおよび認証プロファイルの管理に関する情報を参照してください。

Cisco ISE で TACACS+ 用の認証プロファイルを作成するには、次の手順に従います。

始める前に

次に示す TACACS+ のすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ISE に追加する必要があります。

- Cisco EPN Manager ユーザ ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート （26 ページ）
- Cisco EPN Manager 仮想ドメイン。参照先：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （44 ページ）

ステップ 1 管理ユーザとして Cisco ISE にログインします。

ステップ 2 **[ワークセンター（Work Center）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）]** を選択します。

ステップ 3 左側のサイドバーから、**[結果（Results）] > [TACACS プロファイル（TACACS Profiles）]** を選択します。

ステップ 4 [TACACS プロファイル（TACACS Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [アクセス タイプ（Access Type）] ドロップダウンリストから、[ACCESS_ACCEPT] を選択します。

ステップ 6 [TACACS プロファイル（TACACS Profiles）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 7 [プロファイル属性の raw ビュー（Raw View Profile Attributes）] 領域に、次についての TACACS+ のカスタム属性の完全なリストを貼り付けます。

- タスクを含むユーザ ロール
- 仮想ドメイン

（注） [ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これは必須です。

ステップ 8 **[送信（Submit）]** をクリックします。

Cisco ISE で の認可ポリシーを設定する

認可ポリシーは、認可プロファイルで定義された特定の権限のセットを形成する、ユーザ定義のルールまたはルールのセットで構成されます。認可プロファイルに基づいて、Cisco EPN Manager へのアクセス要求が処理されます。

設定可能な認可ポリシーには、次の 2 つのタイプがあります。

- 標準：標準ポリシーは、安定化を目的としており、長期間にわたって効果を発揮し、より大きなユーザのグループ、デバイス、または権限の共通セットを共有するグループに適用するために作成します。
- 例外：例外ポリシーは、限定数のユーザ、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザまたはユーザのサブセットに合わせて調

整された、ID グループ、条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。

認可ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authorization Policies and Profiles」の章を参照してください。

Cisco ISE で認可ポリシーを作成するには、次の手順を実行します。

ステップ 1 管理者ユーザとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [許可（Authorization）]** を選択します。

ステップ 3 [標準（Standard）] 領域で、右端にある下矢印をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のどちらかを選択します。

ステップ 4 ルール名を入力して、認可ポリシーの ID グループ、条件、属性、および権限を選択します。

たとえば、ユーザ グループを Cisco EPN Manager-SystemMonitoring-Group として定義して、そのグループを [アイデンティティ グループ（Identity Groups）] ドロップダウン リストから選択することができます。同様に、認可プロファイルを Cisco EPN Manager-SystemMonitoring-authorization プロファイルとして定義し、[権限（Permissions）] ドロップダウン リストからそのプロファイルを選択します。これで、Cisco EPN Manager システム モニタリング アイデンティティ グループに属しているすべてのユーザに、システム モニタリングのカスタム属性が定義された適切な認証ポリシーが適用されます。

ステップ 5 [完了（Done）] をクリックしてから、[保存（Save）] をクリックします。

Cisco ISE での認証ポリシーの作成

認証ポリシーは、Cisco ISE が Cisco EPN Manager と通信するために使用するプロトコルを定義します。また、Cisco EPN Manager に対するユーザの認証に使用するアイデンティティ ソースを特定します。アイデンティティ ソースは、ユーザ情報が格納されている内部または外部データベースです。

Cisco ISE で作成できる認証ポリシーには、次の 2 つのタイプがあります。

- シンプルな認証ポリシー：このタイプのポリシーでは、ユーザの認証に使用できるプロトコルとアイデンティティ ソースを選択できます。
- ルールベースの認証ポリシー：このタイプのポリシーでは、許可するプロトコルとアイデンティティ ソースを Cisco ISE に動的に選択させるための条件を定義できます。

認証ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authentication Policies」の章を参照してください。

Cisco ISE で認証ポリシーを作成するには、次の手順に従います。

ステップ 1 上級管理ユーザまたはシステム管理ユーザとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [認証（Authentication）]** の順に選択します。

ステップ 3 必要な認証ポリシーを作成するために、[ポリシー タイプ（Policy Type）] として [シンプル（Simple）] または [ルールベース（Rule-Based）] を選択します。

ステップ 4 選択したポリシー タイプに基づいて、必要な情報を入力します。

ステップ 5 [保存（Save）] をクリックします。

Cisco ACS と RADIUS または TACACS+ による外部認証

Cisco Secure Access Control System（ACS）は販売されなくなりました。詳細については、「Cisco Secure Access Control System の販売終了およびライフサイクル終了のお知らせ」を参照してください。Cisco Evolved Programmable Network Manager と Cisco ACS との統合については、今後新たな開発は予定されていません。ACS との統合のサポート終了日は、2020 年 8 月 31 日に予定されており、同日に ACS 製品が廃止される予定です。

Cisco Secure Access Control System（ACS）は、認証、認可、およびアカウンティング（AAA）に RADIUS および TACACS+ プロトコルを使用します。Cisco ACS に Cisco EPN Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco EPN Manager ユーザを認証できます。外部認証を使用する場合は、ユーザ、ユーザ ロール、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ACS データベースから保存および確認する必要があります。

Cisco ACS で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ACS を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ACS のサポートされるバージョンを使用していることを確認します。	Cisco EPN Manager でサポートされる Cisco ACS のバージョン （56 ページ）
Cisco ACS で Cisco EPN Manager を AAA クライアントとして追加します。	Cisco ACS にクライアントとして Cisco EPN Manager を追加する （56 ページ）
Cisco ACS でユーザ グループを作成します。	Cisco ACS でのユーザ グループの作成 （57 ページ）
Cisco ACS でユーザを作成し、そのユーザを Cisco ACS のユーザ グループに追加します。	Cisco ACS でのユーザの作成とユーザ グループへのユーザの追加 （57 ページ）

（RADIUS を使用する場合）Cisco ACS でネットワーク アクセスの認証プロファイルを作成し、Cisco EPN Manager で作成したユーザ ロールと仮想ドメインの RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザ タスクの属性を追加する必要はありません。これらはユーザ ロールに基づいて自動的に追加されます。	Cisco ACS での RADIUS 用の認証プロファイルの作成 （57 ページ）
（TACACS+ を使用する場合）Cisco ACS でデバイス管理の認証プロファイルを作成し、Cisco EPN Manager で作成したユーザ ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 （注） TACACS+ では、ユーザ タスクの属性を追加する必要はありません。これらはユーザ ロールに基づいて自動的に追加されます。	Cisco ACS での TACACS+ の認証プロファイルの作成 （59 ページ）
Cisco ACS でアクセス サービスを作成し、アクセス サービスのポリシー構造を定義します。	Cisco ACS での Cisco EPN Manager 用アクセス サービスの作成 （60 ページ）
Cisco ACS で認証ポリシー規則を作成し、アクセス タイプ（ネットワーク アクセスまたはデバイス管理）に基づいて認証またはシェル プロファイルをマッピングします。	Cisco ACS での認証ポリシー ルールの作成 （60 ページ）
Cisco ACS でサービス選択ポリシーを設定し、着信要求にアクセス サービスを割り当てます。	Cisco ACS でのサービス セレクション ポリシーの設定 （61 ページ）
Cisco EPN Manager で RADIUS または TACACS+ サーバとして Cisco ACS を追加します。	Cisco EPN Manager への RADIUS または TACACS+ サーバの追加 （47 ページ）
Cisco EPN Manager サーバで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバ上で RADIUS または TACACS+ モードを設定する （48 ページ）

Cisco EPN Manager でサポートされる Cisco ACS のバージョン

Cisco EPN Manager は Cisco ACS 5.*x* リリースをサポートしています。

Cisco ACS にクライアントとして Cisco EPN Manager を追加する

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [ネットワーク デバイスおよび AAA クライアント（Network Devices and AAA Clients）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [作成（Create）] をクリックします。

ステップ 4 Cisco EPN Manager サーバのデバイス名と IP アドレスを入力します。

ステップ 5 認証オプションで [RADIUS] または [TACACS+] を選択し、共有秘密を入力します。

（注） この共有秘密は、Cisco EPN Manager で Cisco ACS サーバを RADIUS または TACACS+ サーバとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS でのユーザ グループの作成

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザと ID ストア（Users and Identity Stores）] > [アイデンティティ グループ（Identity Groups）]** の順に選択します。

ステップ 3 [アイデンティティグループ（Identity Groups）] ページで [作成（Create）] をクリックします。

ステップ 4 グループの名前と説明を入力します。

ステップ 5 ユーザ グループの親ネットワーク デバイス グループを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS でのユーザの作成とユーザ グループへのユーザの追加

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザとIDストア（Users and Identity Stores）] > [内部IDストア（Internal Identity Stores）] > [ユーザ（Users）]** の順に選択します。

ステップ 3 [内部ユーザ（Internal Users）] ページで [作成（Create）] をクリックします。

ステップ 4 次の必須詳細情報を入力します。

ステップ 5 [アイデンティティ グループ（Identity Group）] フィールドで [選択（Select）] を選択して、ユーザを割り当てるユーザ グループを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での RADIUS 用の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN接続を介してネットワークへのアクセスを試みるユー

ザには、有線接続を介してネットワークへのアクセスを試みるユーザよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザ ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザ ロールの属性を追加できます。タスクはユーザ ロールによって自動的に追加されます。

Cisco ACS 認証プロファイルおよびポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素およびアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で RADIUS 用の認証プロファイルを作成するには、次の手順に従います。

始める前に

RADIUS 用の次の Cisco EPN Manager カスタム属性を完全に網羅したリストを用意しておきます。次の手順では、この情報を Cisco ACS に追加する必要があります。

- Cisco EPN Manager ユーザ ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート （26 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （44 ページ）を参照してください。

ステップ 1 管理ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）] > [認証と許可（Authorizations and Permissions）] > [ネットワーク アクセス（Network Access）] > [認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [RADIUS 属性（RADIUS Attributes）] タブをクリックし、以下についての RADIUS カスタム属性の完全なリストを貼り付けます。

- ユーザ ロール
- 仮想ドメイン

（注） ユーザ タスクを追加する場合は、必ずホーム メニュー アクセス タスクを追加してください。これは必須です。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での TACACS+ の認証プロファイルの作成

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager で作成されたユーザ ロールおよび仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

（注） TACACS+ では、ユーザ タスクの属性を追加する必要はありません。これらはユーザ ロールに基づいて自動的に追加されます。

Cisco ACS 認証プロファイルとポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素とアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で TACACS+ の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示すすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ACS に追加する必要があります。

- Cisco EPN Manager ユーザ ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザ グループとロール属性のエクスポート （26 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （44 ページ）を参照してください。

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）]** > **[認証と許可（Authorizations and Permissions）]** > **[デバイス管理（Device Administration）]** > **[シェル プロファイル（Shell Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [カスタム属性（Custom Attributes）] タブをクリックし、次のアイテムのずべての TACACS+ カスタム属性のリストを貼り付けます。

- タスクを含むユーザ ロール
- 仮想ドメイン

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での Cisco EPN Manager 用アクセス サービスの作成

アクセス サービスには、アクセス要求の認証および認可ポリシーが含まれています。使用事例（デバイス管理（TACACS+）やネットワーク アクセス（RADIUS）など）ごとに異なるアクセス サービスを作成できます。

Cisco ACS でアクセス サービスを作成するときに、サービスに含まれるポリシーのタイプとポリシー構造を定義します。たとえば、デバイス管理やネットワーク アクセス用のポリシーがあります。

（注） サービス選択ルールを定義する前に、アクセス サービスを作成する必要がありますが、サービスにポリシーを定義する必要はありません。

Cisco EPN Manager の要求用にアクセス サービスを作成するには、次の手順を実行します。

ステップ 1 管理ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）] > [アクセス サービス（ Access Services）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 アクセス サービスの名前と説明を入力します。

ステップ 5 アクセス サービスのポリシー構造を定義するために、次のいずれかのオプションを選択します。

- [サービス テンプレート ベース（Based on service template）]：定義済みテンプレートに基づいたポリシーを含むアクセス サービスを作成します。
- [既存のサービス ベース（Based on existing service）]：既存のアクセス サービスに基づいたポリシーを含むアクセス サービスを作成します。ただし、新しいアクセス サービスには既存のサービスのポリシー ルールは含まれません。
- [ユーザ選択のサービス タイプ（User selected service type）]：ユーザがアクセス サービスのタイプを選択できます。選択可能なオプションには、ネットワーク アクセス（RADIUS）、デバイス管理（TACACS+）、外部プロキシ（外部 RADIUS または TACACS+ サーバ）があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サービス アクセスに使用できる認証プロトコルを選択します。

ステップ 8 [終了（Finish）] をクリックします。

Cisco ACS での認証ポリシー ルールの作成

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセスポリシー（Access Policies）] > [アクセスサービス（Access Services）] > [サービス（service）] > [認証（Authorization）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 ルールの必須条件を設定します。

たとえば、ロケーション、デバイス タイプ、または作成したユーザ グループに基づいてルールを作成できます。

ステップ 6 ネットワーク アクセス（RADIUS）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須認証プロファイルを選択します。

あるいは、デバイス管理（TACACS+）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須シェル プロファイルを選択します。

（注） 複数の認証プロファイルまたはシェル プロファイルを使用する場合は、優先順位の高い順に並べる必要があります。

ステップ 7 [OK] をクリックします。

Cisco ACS でのサービス セレクション ポリシーの設定

サービス セレクション ポリシーでは、着信要求に適用するアクセス サービスを決定します。たとえば、TACACS+ プロトコルを使用するアクセス要求にデバイス管理アクセス サービスを適用するサービス セレクション ポリシーを設定できます。

次の 2 種類のサービス セレクション ポリシーを設定できます。

- 単純なサービス セレクション ポリシー：すべての要求に同じアクセス サービスを適用します。
- ルール ベースのサービス セレクション ポリシー：1 つ以上の条件とその結果（着信要求に適用されるアクセス サービス）が設定されています。

サービス セレクション ポリシーを設定するには、次の手順を実行します。

ステップ 1 admin ユーザとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）]** > **[アクセス サービス（Access Services）]** > **[サービス セレクション ルール（Service Selection Rules）]** の順に選択します。

ステップ 3 単純なサービス セレクション ポリシーを設定するには、[単一結果の選択（Single result selection）] オプション ボタンをクリックし、すべての要求に適用するアクセス サービスを選択します。

または、ルールベースのサービス セレクション ポリシーを設定するには、[ルールベースの結果選択（Rule based result selection）] オプション ボタンをオンにし、[作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 サービス セレクション ポリシーのプロトコルとして [RADIUS] または [TACACS+] を選択します。

ステップ 6 必要な複合条件を設定し、着信要求に適用するアクセス サービスを選択します。

ステップ 7 [OK] をクリックし、[変更の保存（Save Changes）] をクリックします。

SSO による外部認証

（RADIUS または TACACS+ サーバの有無にかかわらず）SSO をセットアップおよび使用するには、これらのトピックを参照してください。

- SSO サーバの追加 （62 ページ）
- SSO サーバの削除 （62 ページ）
- Cisco EPN Manager サーバ上で SSO モードを設定する （63 ページ）

Cisco EPN Manager では、SSO サインイン ページのローカリゼーションをサポートしていません。

SSO サーバの追加

プライマリ サーバとバックアップ サーバが含まれる高可用性環境に Cisco EPN Manager が導入されている場合は、HA 環境での SSO サーバの設定の手順を参照してください。

Cisco EPN Manager には最大 3 つの AAA サーバを設定できます。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[SSO サーバ（SSO Servers）] を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[SSO サーバの追加（Add SSO Server）] を選択し、[実行（Go）] をクリックします。

ステップ 3 SSO 情報を入力します。SSO サーバ認証要求のサーバ再試行回数は最大 3 回です。

ステップ 4 [保存（Save）] をクリックします。

（注） SSO サーバとして使用している EPNM サーバを追加することもできます。**[コマンドの選択（Select a command）]** ドロップダウンリストから、**[SSO サーバとして自身を追加（Add self as SSO Servers）]** を選択し、**[実行（Go）]** をクリックします。

SSO サーバの削除

EPNM に追加された SSO サーバを削除できます。SSO サーバを削除するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[SSO サーバ（SSO Servers）] を選択します。

ステップ 2 削除するサーバを選択します。

ステップ 3 **[コマンドの選択（Select a command）]** ドロップダウンリストから、**[SSO サーバの削除（Delete SSO Server(s)）]** を選択し、**[実行（Go）]** をクリックします。

ステップ 4 **[OK]** をクリックして、サーバの削除を確認します。

Cisco EPN Manager サーバ上で SSO モードを設定する

SSO サーバが SSO クライアントに追加されたときに、SSO 機能によって CA 証明書が配布されます。

Cisco EPN Manager は、CA および自己署名証明書をサポートしますが、その場合、SSO クライアントおよび SSO サーバの両方にあるサーバの完全修飾ドメイン名（FQDN）が証明書の Common Name（CN）フィールドに含まれていることが必要です。このサーバは、IP アドレスから FQDN に名前解決できることが必要です。さらに、ホスト名が FQDN の最も左のコンポーネントと一致する必要があります。SSO には正確な DNS 設定が必要です。完全修飾ドメイン名（FQDN）を使用して DNS を定義する必要があります。たとえば、FQDN を使用して DNS を設定する場合の nslookup コマンドと予想されるデータは次のとおりです。

```
hostname CUSTOMER_HOSTNAME
nslookup CUSTOMER_HOSTNAME
Server:...
Address:...
Name: CUSTOMER_HOSTNAME.example.com
Address:....
```

SSO 操作の場合、Cisco EPN Manager は、SSL/TLS 証明書の CN フィールドに FQDN が含まれていることを必要とします。Cisco EPN Manager サーバが使用する証明書の CN フィールドに FQDN が含まれていることを確認するには、ブラウザを使用して証明書を表示します。証明書の CN フィールドに FQDN が含まれていない場合は、証明書を再生成して、古い証明書を使用しているすべてのユーザに再配布する必要があります。

（注） 次の手順を使用して SSO を設定するが、ローカル認証を使用する場合は、ステップ 2 で [ローカル（Local）] を選択します。

ステップ 1 **[管理（Administration）]** > **[ユーザ（Users）]** > **[ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[SSO サーバの設定（SSO Server Settings）] を選択します。

ステップ 2 使用する SSO サーバ AAA モードを選択します。一度に 1 つのみ選択できます。

ステップ 3 [OK] をクリックします。