ユーザー権限とデバイス アクセス

ユーザーインターフェイス、ユーザータイプ、およびそれらの間の遷移

これらのトピックでは、Cisco Evolved Programmable Network Manager で使用される GUI と CLI インターフェイス、および Cisco Evolved Programmable Network 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。

ユーザー インターフェイスとユーザー タイプ

次の表に、Cisco Evolved Programmable Network Manager （CEPNM）によって採用されたユーザー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ーのタイプの説明を示します。

CEPNM ユーザーインターフェイス	インターフェイスの説明	**CEPNM** ユーザー 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。これらのユーザーは、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 Evolved Programmable Network Manager の CLI 管理ユーザーと CLI 構成ユーザーによって提供される操作のサブセットを提供します。	[Cisco Evolved Programmable Network Manager Web GUI通常ユーザー（Cisco EPN Manager web GUI everyday users）]：Web GUI のルートユーザーによって作成されます。このユーザーは、さまざまなレベルの権限を持ち、ユーザー グループ（管理者、スーパーユーザー、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。ユーザー グループについては、ユーザーグループのタイプ （6 ページ）を参照してください。 **Cisco Evolved Programmable Network Manager** Web GUI ルート ユーザー：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ー 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 ユーザー、つまり、管理者ユーザーまたはスーパー ユーザー ユーザー グループに属している Web GUI ユーザーの作成後に無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （5 ページ）を参照してください。 （注） Cisco Evolved Programmable Network Manager Web GUI ルート ユーザーは、Linux CLI ルート ユーザーと同じではなく、Cisco Evolved Programmable Network Manager CLI 管理者ユーザーとも異なります。

CEPNM ユーザー インターフェイス	インターフェイスの説明	CEPNM ユーザー タイプ
[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 ユーザーは、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ユーザー（Cisco EPN Manager NBI users）]：Web GUI ルートユーザーによって作成されます。これらのユーザーには、3種類の異なる権限があり、ロールベース アクセス コントロール（RBAC）クラスと NBI ユーザーグループというサブクラス（NBI 読み取りおよび NBI 書き込み）に分類されます。ユーザーグループの詳細については、次の項を参照してください。ユーザー グループ - NBI （8 ページ）

CEPNMユーザーインターフェイス	インターフェイスの説明	CEPNM ユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager CLI 管理者ユーザー 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 Evolved Programmable Network Manager CLI 管理者ユーザー**：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 で使用できます）。 このユーザー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 Evolved Programmable Network Manager 管理 CLI と Cisco Evolved Programmable Network Manager 構成 CLI の切り替え （5 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 Evolved Programmable Network 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ー アクセス権を持っている必要があります（この表の [ユーザー タイプ（User Types）] 列内の情報を参照）。管理者 CLI シェルでこのシェルにアクセスできます。	管理者 CLI ユーザーは、次のコマンドを使用して、さまざまな理由で他の CLI ユーザーを作成できます。 `(config) username username password role {admin|user} password` これらのユーザーには、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 Evolved Programmable Network Manager CLI ユーザーを作成するには、**admin** キーワードを指定して **username** コマンドを実行します。それ以外のユーザーを作成する場合は、**user** キーワードを使用します。パスワードの制限については、管理者ユーザーの作成を参照してください。
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 Evolved Programmable Network Manager 管理者シェルと CLI を経由する必要があります。	**Linux CLI 管理ユーザー**：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 Evolved Programmable Network Manager で CLI ユーザー 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 Evolved Programmable Network Manager 管理 CLI と Cisco Evolved Programmable Network Manager 構成 CLI の切り替え

Cisco Evolved Programmable Network Manager 管理 CLI から Cisco Evolved Programmable Network 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

インストール後、管理者権限またはスーパーユーザー権限を持つ他の Web GUI ユーザーを 1 人以上作成したら、Cisco EPN Manager Web GUI **root** ユーザーを無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （5 ページ）を参照してください。

Web GUI ルート ユーザー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 ユーザー（つまり、管理ユーザー グループまたはスーパー ユーザー グループに属する Web GUI ユーザー）を作成します。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 ユーザー 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
```

ユーザーが実行できるタスクWebインターフェイスの制御

Web インターフェイス ユーザーの場合、Cisco EPN Manager では、ユーザー認証はユーザーグループを使用して実装されます。ユーザー グループには、ユーザーがアクセスできる Cisco EPN Manager の部分およびユーザー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。

ユーザー グループはユーザーの操作を制御しますが、仮想ドメインはユーザー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ー アクセスを制御するための仮想ドメインの作成 （37 ページ）」を参照してください。

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

次のトピックでは、ユーザー認証の管理方法について説明します。

ユーザー グループのタイプ

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

CLI ユーザーについては、ユーザー インターフェイスとユーザー タイプ （2 ページ）を参照してください）。

ユーザー 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 ユーザーグループを提供します。Monitor Lite ユーザーグループに属するユーザーを除き、ユーザーを複数のグルー

プに割り当てることができます（Monitor Lite は、権限が制限されているユーザー向けであるためです）。

各ユーザー 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 （26 ページ）を参照してください。

ユーザー 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 ユーザーが使用可能になります。ユーザー インターフェイスとユーザー タイプ （2 ページ）を参照してください。Web GUI ルート ユーザーの無効化および有効化 （5 ページ）に説明されているとおり、Admin または Super Users 権限で別のユーザーを作成し、root Web UI ユーザーを無効にすることをお勧めします。
Super Users	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。ルートユーザーの権限に類似した権限を有効にすることができます。
Admin	システムとサーバーを管理します。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ーします（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ーします（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ー設定関連のページにしかアクセスできません。これは、ユーザー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 ユーザーのみのユーザー管理。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
User–Defined 1 ～ 50	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ー 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。このユーザー グループのメンバーは、他のユーザー 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 ユーザー管理のみ。このユーザー グループのメンバーは、他のユーザー 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。

ユーザー 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 ユーザー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。

各ユーザー 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 （26 ページ）を参照してください。

ユーザー グループ	アクセス対象：
NBI Read	RESTCONF NBI 読み取り操作（HTTP GET）。他の NBI または Web UI ユーザー 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 ユーザー グループに属することもできます。

ユーザーが実行できるタスクの表示と変更

ユーザーが実行できるタスクは、ユーザーが所属するユーザー グループによって制御されます。ユーザーグループと、ユーザー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） ユーザーがアクセスできるデバイスを確認する場合は、ユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択します。

ステップ 2 [ロール（Roles）] タブを選択し、左ペインの [ロール（Roles）] でユーザーグループを見つけます。

ステップ 3 ユーザーグループを選択し、[タスク権限（Task Permissions）] タブを選択します。グループメンバーが実行できるタスクと実行できないタスクが一覧表示されます。

- チェックボックスがオンの場合は、グループメンバーがそのタスクを実行できることを示します。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。たとえば、Cisco EPN Manager では、Monitor Lite ユーザーグループの [タグの表示（View tags）] タスクを削除できません。これは、そのユーザー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、そのユーザー 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。

- すべてのユーザー 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 （26 ページ）を参照してください。
- 別のユーザー グループにユーザーを追加します。事前定義されたユーザー グループについては、ユーザー グループ：Web UI （6 ページ） とユーザー グループ - NBI （8 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、ユーザーが事前定義済みの Monitor Lite ユーザー グループに属している場合、そのユーザー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ーを削除します。ユーザーが属しているグループを表示して変更する （9 ページ）を参照してください。
- カスタマイズされたユーザー グループを使用し、ユーザー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 （26 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 ユーザー グループの作成 （26 ページ）を参照してください。

ユーザーが属しているグループを表示して変更する

ユーザーが実行可能なタスクは、そのユーザーが属しているユーザー グループによって決定されます。通常は、ユーザー アカウントの作成時に設定されます（ユーザーの追加および削除 （30 ページ）を参照）。ユーザー グループについては、ユーザー グループのタイプ （6 ページ）で説明します。

この手順では、ユーザーが属しているグループを表示し、必要に応じて、ユーザー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）]>[ユーザーとロール（Users and Roles）] の順に選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザー名（User Name）] 列で、ユーザー名のチェックボックスを見つけて選択します。[編集（Edit）] オプションをクリックします。[ユーザーの編集（Edit User）] ウィンドウが表示されます。

- オンになっているチェックボックスは、ユーザー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ーを削除できないことを意味します。たとえば、Cisco EPN Manager では、ルートユーザーグループから **root** という名前のユーザーを削除できません。

ステップ 3 ユーザーが属しているグループを変更するには、[ロールの詳細（Role Details）] ドロップダウンリスト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。

ユーザー グループとそのメンバーの表示

ユーザーは、Monitoring Lite などの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、既存のユーザー 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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ロール（Roles）] を選択します。

[ロール（Roles）] ページには、既存のすべてのユーザー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、ユーザー グループのタイプ （6 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、グループ名を選択し、[メンバー（Members）] タブを選択します。

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 （26 ページ）
- ユーザーが属しているグループを表示して変更する （9 ページ）

ユーザーグループの権限とタスクの説明

次の表に、ユーザーグループの権限とタスクの説明を示します。

表 *1*:ユーザー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	ユーザー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	ユーザー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）	ユーザーは [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
	ヘルスモニターの詳細（Health Monitor Details）	ユーザー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	ユーザーはプライマリサーバーとセカンダリサーバーのペアリングに [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）	ユーザー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）	ユーザー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	ユーザー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
	ユーザー定義フィールド	ユーザーはユーザー定義フィールドを作成できます
	ユーザー設定	[管理（Administration）] > [ユーザー設定（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）	ユーザーは [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）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザーはアラームで 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）	ユーザー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）	ユーザー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	ユーザー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	ユーザー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	ユーザーは、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	ユーザーは、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）	ユーザーは 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）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザー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）	ユーザー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）	ユーザーはグループをインポートできます
	グループの変更（Modify Groups）	ユーザーは名前、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	ユーザーは [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	ユーザー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）	ユーザーは別のユーザー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）	ユーザー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）]	ユーザーは [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）]	ユーザーは [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）	ユーザー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）	ユーザーはジョブをスケジュールできます
	ジョブの表示（Schedule Job）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザーはシステムジョブを表示できます
[モニター（Monitor）] メニュータスク	[モニター（Monitor）] メニューアクセス	ユーザーは [モニター（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）	ユーザーは 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）	ユーザー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
	アラームモニターポリシー	アラームモニター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）	ユーザー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）	ユーザーは「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）	ユーザー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）	ユーザー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）	ユーザー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
	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 サーバーの設定	ユーザーは Cisco EPN Manager で ISE サーバーを管理できます
	テンプレートの設定（Configure Templates）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザー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）	ユーザーは 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）	ユーザーは設定と 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）	ユーザーは、[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）	ユーザーは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）	ユーザー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編集（Edit Device Access）	ユーザー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）	ユーザー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	ユーザー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）	ユーザー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	ユーザー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）	ユーザー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）	ユーザー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）	ユーザーは [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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザー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）	ユーザーはパフォーマンス 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	ユーザーは 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	ユーザーは 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	ユーザーは [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	デバイス レポート	ユーザー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）	ユーザー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	ユーザーはネットワーク 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）	ユーザー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	ユーザー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	ユーザー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	ユーザーはパフォーマンスレポートを作成できます
	読み取り専用パフォーマンスレポート（Performance Reports Read Only）	ユーザー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	ユーザーは [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）	ユーザー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）	ユーザー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）	ユーザー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	ユーザーはシステム モニタリング レポートを表示できます

タスクグループ名	タスク名	説明
	仮想ドメインリスト（Virtual Domains List）	ユーザー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ーの追加（Add Software Image Management Servers）	ユーザーはソフトウェアイメージ管理サーバーを追加できます
	イメージ詳細ビュー	ユーザーはイメージの詳細を表示できます
	プロトコルの管理	ユーザー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 のユーザー設定の保存	ユーザーは [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	ユーザーは最小 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	ユーザーは 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	ユーザー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
ユーザー管理	監査証跡	ユーザーはユーザー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 サーバー（LDAP Server）	ユーザーは [LDAPサーバー（LDAP Server）] メニューにアクセスできます
	RADIUS サーバー	ユーザーは [RADIUSサーバー（RADIUS Servers）] メニューにアクセスできます
	SSO サーバー AAA モード（SSO Server AAA Mode）	ユーザーは [AAA] メニューにアクセスできます。
	SSO サーバー	ユーザーは [SSO] メニューにアクセスできます。
	TACACS+ サーバー	ユーザーは [TACACS+サーバー（TACACS+ Servers）] メニューにアクセスできます。
	ユーザーとグループ	ユーザーは[ユーザーとグループ（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）	ユーザーは[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、ユーザーは[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	ユーザーはオンラインヘルプにアクセスできます

カスタム ユーザー 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ーグループを利用してユーザーの権限を制御できます。これらの定義済みグループ（ユーザー グループのタイプ （6 ページ）を参照）に含まれているユーザー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ー 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ー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ロール（Roles）] を選択します。

ステップ 2 左側の [ロール（Roles）] ペインで、メンバーのないユーザー定義グループを見つけて選択します。

ステップ 3 [ロールの権限（Role Permissions）] 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。ユーザー定義グループ名の前にある [編集（Edit）] アイコンをクリックすると、ユーザーグループの名前を変更できます。

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、該当するユーザー アカウントを編集して、そのユーザーを新しいグループに追加します。ユーザー アカウントの調整の詳細については、ユーザーの追加および削除 （30 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

既存のユーザー 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ー グループの詳細については、「ユーザー グループとそのメンバーの表示 （10 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、「ユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ロール（Roles）] を選択します。

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

ステップ 2 ユーザ グループを選択します。[タスク権限（Tasks Permissions）] ウィンドウに、タスク権限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、そのユーザー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、[ユーザー定義（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 ユーザー グループの作成 （26 ページ）」を参照してください。

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

Cisco EPN Manager に存在するユーザー グループを認識するように、RADIUS または TACACS+ サーバーを設定する必要があります。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート （27 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 ユーザー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 ユーザー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）サーバー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 サーバーにエクスポートしない場合、Cisco EPN Manager は、ユーザー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 サーバー用に事前に書式設定されています。

（注） 外部サーバー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ーで必須です。

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

a) **[管理（Administration）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）] > [ロール（Roles）]** の順に選択します。

b) [ロール（Roles）] リストからユーザーグループを選択し、[タスクリスト（Task List）] アイコン（[ロール権限（Role Permissions）] の前）をクリックして、各ユーザー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 サーバーに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザー 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 （57 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （50 ページ）

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

b) 該当するユーザーまたはグループの [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。

ユーザーの追加およびユーザー アカウントの管理

管理者権限を持つ Web GUI ユーザーの作成

インストール後、Cisco EPN Manager には **root** という名前の Web 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、サーバー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 ユーザー
- その他すべてのユーザーアカウント。

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 ユーザーを作成した後には 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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザー（Users）] ウィンドウで、＋をクリックして、新しいユーザーエントリをテーブルに表示します。

ステップ 3 [ユーザー名（User Name）] テキストボックスにユーザー名を入力します。

ステップ 4 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。

ステップ 5 （オプション）ユーザーの [名（First Name）]、[姓（Last Name）]、および [説明（Description）] を入力します。

ステップ 6 [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 7 [ロール（Role）] ドロップダウンリストで、[管理者（Admin）] を選択します。

ステップ 8 [仮想ドメイン（Virtual Domains）] で、ユーザー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 ユーザー（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ー アクセスを制御するための仮想ドメインの作成 （37 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 9 [保存（Save）] をクリックします。

（注） 新しいユーザーを作成するときは、ブラウザにユーザー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

セキュリティ上の理由から、Web GUI ルート ユーザーの無効化および有効化 （5 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。

ユーザーの追加および削除

ユーザー 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場合は、ユーザーアカウントを編集してドメインアクセスを追加する必要があります。デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （37 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、ユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ユーザー（Users）] を選択します。

ステップ 2 ＋ をクリックすると、新しいユーザーエントリが表示されます。

ステップ 3 ユーザー アカウントを設定します。

a) ユーザー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、ユーザー名と電子メールアドレスを入力します。詳細については、ユーザーのパスワードの自動生成 （31 ページ）を参照してください。

b) ユーザーの名、姓、説明を入力します。

c) ユーザーが実行できるアクションを制御するために、1 つ以上のユーザーグループを選択します。ユーザー グループについては、ユーザー グループとそのメンバーの表示 （10 ページ）を参照してください。

d) [仮想ドメイン（Virtual Domains）] スペースからユーザーがアクセスできるデバイスを制御し、ドメインをユーザーに割り当てます。（デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （37 ページ） を参照）。

ステップ 4 **[保存（Save）]** をクリックします。

（注） 新しいユーザーを作成するときは、ブラウザにユーザー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 ユーザーアカウントを削除するには、ユーザーを選択して 🗑 をクリックします。

ステップ 6 [削除（Delete）] をクリックして、ユーザーの削除を確定します。

ユーザー アカウントの無効化（ロック）

一時的にユーザーが Cisco EPN Manager GUI にログインできないようにするには、ユーザーアカウントを無効にします。ユーザー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。ユーザー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。

ユーザー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。ユーザーアカウントを削除する場合は、ユーザーの追加および削除 （30 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、自動的にユーザー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。ユーザーのパスワードを変更する （31 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 （34 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ユーザー（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ーを選択します。

ステップ 3 ユーザーをロックするには、  クリックします（またはユーザーのロックを解除するには、  [ユーザーのロック解除（Unlock User(s)）]）をクリックします）。

ユーザーのパスワードを変更する

パスワードルールを設定して、ユーザー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 （34 ページ）を参照）。ユーザーは、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。ユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択し、[ユーザー（Users）] をクリックします。

ステップ 2 ユーザー名を選択して  アイコンをクリックすると、[ユーザーの編集（Edit User）] ウィンドウが開きます。

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、[保存（Save）] をクリックします。

ユーザーのパスワードの自動生成

Cisco EPN Manager には、電子メールサーバーの可用性に基づいて新規および既存のユーザー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ーに送信します。

（注） [パスワードの自動生成（Auto-generate Passwords）] オプションは、電子メールサーバー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ー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

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

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** の順に選択し、[設定（Settings）] を選択して、[ローカルパスワードポリシー（Local Password Policy）] ドロップダウンを展開します。

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 [すべての変更を保存（Save All Changes）] をクリックして、変更を保存します。

ステップ 4 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザーとロール（Users and Roles）]** の順に移動し、[ユーザー（Users）] をクリックします。

a) 新しいユーザーの場合は、ユーザー名と電子メールアドレスを入力します。

b) 既存のユーザーの場合は、パスワードをリセットします。

ステップ 5 [保存（Save）] をクリックして変更を保存し、ユーザー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ーの確認

現在 Cisco EPN Manager サーバーにログインしているユーザーを確認するには、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ー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 [設定（Settings）] アイコンをクリックし、**[マイ設定（My Preferences）]** > **[一般（General）]** > **[ページあたりのリストの項目数（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）]** > **[ユーザー（Users）]** > **[ユーザーとロール（Users and Roles）]** を選択し、[アクティブなセッション（Active Sessions）] タブを選択します。Cisco EPN Manager により、Cisco EPN Manager サーバーに現在ログインしているすべてのユーザーと、各ユーザーのクライアントマシンの IP アドレスがリストされます。

ステップ 2 このユーザー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、ユーザー名に対応する アイコンをクリックし、[監査証跡（Audit Trail）] を選択します。ユーザー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（ユーザー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 3 アクティブなユーザーセッションを終了する場合は、 をクリックし、[セッションの終了（Terminate Session）] を選択します。

（注） [セッションの終了（Terminate Session）] は、アクティブなユーザーセッションのみを終了します。ユーザーが再度ログインしないようにするには、ユーザー 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。

ユーザー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ーが実行したすべてのアクションの履歴を保持します。特定のユーザーまたは特定のユーザー 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、ユーザー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（ユーザーが新しいデバイスを追加した場合や [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、ユーザー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ーを確認するには、現在ログイン中のユーザーの確認 （32 ページ）を参照してください。

ユーザー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。

- ユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）]** の順に選択します。

ステップ 2 特定のユーザーが実行するタスクを表示するには：

1. [ユーザー（Users）] を選択します。
2. ユーザー名を見つけて  アイコンをクリックし、[監査ログ（Audit Log）] を選択します。

ステップ 3 ユーザー 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. [ロール（Roles）] を選択します。
2. ユーザーグループ名を見つけて、[メンバー（Members）] タブをクリックします。そのグループに対応する  アイコンをクリックし、[監査証跡（Audit Trail）] を選択します。

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ーに電子メールを送信し、そ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、ウィンドウの右上にある [ジョブ承認（Job Approval）] リンクをクリックします。

- ロールバック ジョブの場合は、実行コンフィギュレーションとスタートアップ コンフィギュレーションの詳細が表示されます。
- 上書きジョブの場合は、実行される操作の説明が表示されます。

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。このチェックボックスを有効にすると、ジョブタイプの順序リストから選択できます。必要なオプションを選択します。

ステップ 3 [ジョブ承認用のメールを有効にする（Enable Mail for Job Approval）] チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。ジョブ承認者の電子メールアドレスを入力します。

ステップ 4 [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 ユーザー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、ユーザーは、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）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** を選択し、[設定（Settings）] を

選択して、[ローカルパスワードポリシー（Local Password Policy）] ドロップダウンを展開します。

（注） 新しいユーザーが 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、初回ログインチェックボックスで [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）] > [サーバー（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。

アイドルユーザー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 ユーザー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。

- [ユーザー 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ー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）] : [ユーザー 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ーのみが [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、ユーザー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、ユーザーにキーストロークやマウスクリックがない場合、ユーザーは 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、ユーザーは 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、すべてのユーザー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。アイドルユーザーのタイムアウトを無効にするか変更するには、アイドル ユーザーのタイムアウトの無効化 （36 ページ） を参照してください。

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）] > [サーバー（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 ユーザーをログアウトする（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 ユーザーをログアウトする（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 ユーザー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ーは自動的にログアウトされます。これはすべてのユーザー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 ユーザー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、[ユーザー 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（Global Idle Timeout）] の設定を行うには、アイドル ユーザー用のグローバル タイムアウトを設定する （35 ページ） 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ーをログアウト（Logout all idle users）] を無効にするか、またはルートユーザーのマイプリファレンス設定で [アイドルユーザーをログアウト（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 サーバー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ー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）] > [サーバー（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 ユーザーをログアウトする（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 [ユーザー 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ーのログアウト（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ーのログアウト（Logout idle user）] チェックボックスをオンにし、[アイドルユーザー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ー 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ー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ーを選択します。仮想ドメインは、物理サイト、デバイス タイプ、ユーザー 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、ユーザー グループと連携します。仮想ドメインは、ユーザーがアクセスできるデバイスを制御しますが、ユーザー グループは、ユーザー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ーは、ユーザーの権限に応じて、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。オプションで説明、電子メール アドレス、およびタイム ゾーンを設定できます。Cisco EPN Manager は、指定されたタイム ゾーンと電子メール アドレスを使用して、ドメイン固有のレポートをスケジュールして電子メール送信します。

ユーザーは、一度に 1 つの仮想ドメインで作業します。ユーザーは、[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ーを決定します。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ー 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）のユーザー ビューがユーザー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 （39 ページ）
• 検索と仮想ドメイン （39 ページ）
• アラームと仮想ドメイン （39 ページ）
• マップおよび仮想ドメイン （39 ページ）
• 設定テンプレートと仮想ドメイン （39 ページ）

• グループおよび仮想ドメインの設定 （40 ページ）
• 電子メール通知と仮想ドメイン （40 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 サーバー、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ー、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 （40 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 （41 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 （41 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（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 [i]（情報）アイコンをクリックし、[サブドメインの作成（Create Sub Domain）] をクリックします。

ステップ 3 ドメインの名前と説明を入力します。

ステップ 4 [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 （40 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（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。）

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、[サブドメインを追加（Add a 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、[無題（Untitled）] という名前の子ドメインの上に親ドメインが表示されます。

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。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した後に [無題（Untitled）] から**指定した子ドメイン名**に変わります。

ステップ 4 （任意）説明を追加します。

ステップ 5 [作成（Create）] 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。

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）] > [ユーザー（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ーに対し、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）] > [ユーザー（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 左ペインで [追加（Add）] アイコンをクリックします。

ステップ 4 ネットワーク デバイスをグループ単位で追加したり、特定のロケーション グループにネットワーク デバイス グループを追加することができます。

ステップ 5 グループからデバイスを追加するには、[グループ（Groups）] タブで [追加（Add）] をクリックします。[グループの追加（Add Group）] ポップアップが表示され、適用可能なロケーションとユーザー定義グループの一覧が表示されます。デバイスを追加するグループを選択して [選択（Select）] をクリックし、グループを [グループ別の選択済みネットワークデバイス（Selected Network Devices by Group）] 表に追加します。

ステップ 6 個々のデバイスを追加する場合は、[ネットワークデバイス（Network Devices）] タブを選択し、[追加（Add）] をクリックすると、[ネットワークデバイスの選択（Select Network Devices）] ポップアップが表示されます。ここでは、[フィルタ条件（Filter By）] ドロップダウン リストを使用して、機能に基づいてネットワーク デバイスを絞り込むことができます。

ステップ 7 [フィルタ条件（Filter By）] ドロップダウン リストから、ネットワーク デバイスを選択します。[使用可能なネットワーク デバイス（Available Network Devices）] テーブルから必要なデバイスを選択して、[選択（Select）] をクリックし、[選択されたネットワーク デバイス（Selected Network Devices）] テーブルにデバイスを追加します。

（注） [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ます。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に追加されます。

（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 8 [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 9 [保存（Save）] をクリックして変更を確定します。

次のタスク

ユーザー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ーに付与します。

ユーザーへの仮想ドメインの割り当て

仮想ドメインをユーザーアカウントに割り当てると、そのユーザーが表示して操作を実行できるデバイスは、ユーザー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 サーバーの該当するユーザー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）] > [ユーザー（Users）] > [ユーザーとロール（Users and Roles）] > [ユーザー（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ーを選択します。 アイコンをクリックすると、[ユーザーの編集（Edit User）] ウィンドウが開きます。

ステップ 3 [仮想ドメイン（Virtual Domains）] スペースから、チェックボックスをオンまたはオフにしてドメインを追加または削除し、[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）] > [ユーザー（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 [保存（Save）] をクリックして変更内容を適用、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。

- ユーザー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 ユーザー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ーがいない場合。

ステップ 1 **[管理（Administration）] > [ユーザー（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+ サーバーは、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 Evolved Programmable Network Manager 仮想ドメイン属性のエクスポート （45 ページ）」の手順を使用します。

RADIUS または TACACS+ サーバーにユーザー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 がユーザー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、ユーザーがログインできなくなります。

RADIUS および TACACS+ の Cisco Evolved Programmable Network 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 Evolved Programmable Network Manager 仮想ドメイン情報をすべて Cisco ACS または Cisco ISE サーバーにコピーする必要があります。Cisco Evolved Programmable Network 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 サーバーにデータをエクスポートしない場合、Cisco Evolved Programmable Network Manager ではユーザー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 サーバー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） 外部サーバー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ーで必須です。

始める前に

外部認証の設定 （47 ページ）の説明に従い、AAA サーバーを追加し、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 Evolved Programmable Network Manager で、次の手順を実行します。

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

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+ を使用する場合は、[TACACS+カスタム属性（TACACS+ 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。

ステップ 2 Cisco ACS または Cisco ISE サーバーに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザー 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 （57 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （50 ページ）

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

ユーザーベースで仮想ドメインを指定する場合、すべてのカスタム属性情報（たとえば、タスク、ロール、仮想ドメインなど）を [ユーザー（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) 該当するユーザーまたはグループの [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、ユーザーパスワードが 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。

認証モードを確認するには、次の手順を実行します。

手順の概要

1. **[管理（Administration）] > [ユーザー（Users）] > [AAA（AAA）] > [設定（Settings）]** の順に選択します。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、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 （34 ページ）を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**[管理（Administration）] > [ユーザー（Users）] > [AAA（AAA）] > [設定（Settings）]** の順に選択します。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、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 （34 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 （47 ページ）を参照してください。 外部認証については、「」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 サーバーを追加し、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 サーバーとバックアップ サーバーが存在するハイ 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 サーバー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 サーバーで 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 サーバーの追加 （64 ページ）
- Cisco EPN Manager サーバーでの SSO モードの設定 （65 ページ）

外部認証の設定

Web GUI のルートユーザーまたはスーパーユーザー権限を持つユーザーは、外部認証、認可、およびアカウンティング（AAA）のために外部 RADIUS、TACACS+、SSO サーバーと通信するように 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、ユーザーグループ、ユーザー、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ーで作成済みである必要があります。

最大 3 つの AAA サーバーを使用できます。ユーザーは、最初のサーバー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 番目のサーバーで認証されます。

（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 サーバーを一緒に使用できます。プロトコルが異なるサーバー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 サーバーを使用する場合は、Cisco ISE または ACS を EPNM と AAA サーバー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 からの外部 AAA 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。

- 外部認証での RADIUS または TACACS+ の使用
- Cisco ISE と RADIUS または TACACS+ による外部認証
- Cisco ACS と RADIUS または TACACS+ による外部認証
- SSO による外部認証

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+ サーバーを使用するように 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+ サーバーの追加 （48 ページ）
- Cisco EPN Manager サーバーでの RADIUS または TACACS+ モードの設定 （49 ページ）

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

RADIUS または TACACS+ サーバーを 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）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** の順に選択し、[サーバー（Servers）] を選択します。このウィンドウからは、新し RADIUS/TACACS+ サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 追加するサーバーのタイプを選択します。

- RADIUS の場合、[RADIUS（RADIUS）] タブをクリックします。 ⊞ アイコンをクリックします。
- TACACS+ の場合、[TACACS+] タブをクリックします。 ⊞ アイコンをクリックします。

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 が外部認証サーバーと通信するためには、このページで入力された共有秘密が RADIUS また TACACS+ サーバー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 サーバー用の共有秘密

キーを入力する際は、アルファベット、数字、および特殊文字（'（一重引用符）と "（二重引用符）を除く）を使用できます。再送信タイムアウトと再試行の回数を入力します。

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プロトコルでは、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に使用する必要があります。
- 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ー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 [テスト（Test）] をクリックして、AAA サーバーの接続を確認します。接続テストは、入力したポート、認証タイプ、および共有キーが TACACS または RADIUS サーバーと一致する場合にのみ合格します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 RADIUS/TACACS+ サーバーを編集するには、次の手順を実行します。

a) RADIUS/TACACS+ サーバーの横にあるチェックボックスをクリックし、  をクリックします。変更を加えたら、[保存（Save）] をクリックします。

ステップ 8 RADIUS/TACACS+ サーバーを削除するには、次の手順を実行します。

a) RADIUS/TACACS+サーバーの横にあるチェックボックスをクリックし、  をクリックします。[削除（Delete）] ダイアログボックスが開きます。[削除（Delete）] をクリックして確認します。

Cisco EPN Manager サーバーでの RADIUS または TACACS+ モードの設定

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** の順に選択し、[設定（Settings）] 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（Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバー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+ サーバー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（Fallback to Local）] を選択します。

b) 次のいずれかのフォールバック条件を指定します。

- [サーバー無応答時のみ（Only on no server response）]：外部サーバーに到達できない、または、ネットワークに問題がある場合のみ。このオプションを選択すると、AAA ユーザーとしてのみログインできます。
- [認証に失敗したかサーバーが応答しないとき（On authentication failure or no server response）]：外部サーバーに到達できない、または、ネットワークに問題がある場合と、外部 AAA サーバーでユーザーを認証できない場合のどちらか。このオプションを選択すると、ローカルユーザーと AAA ユーザーとしてログインできます。

ステップ 5 [すべての変更を保存（Save All Changes）] 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 Evolved Programmable Network Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco Evolved Programmable Network Manager ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager でサポートされる Cisco ISE のバージョン（51 ページ）
Cisco ISE で Cisco Evolved Programmable Network 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 Evolved Programmable Network Manager を追加する（52 ページ）
Cisco ISE でユーザー グループを作成します。	Cisco ISE でのユーザー グループの作成 （52 ページ）
Cisco ISE でユーザーを作成し、そのユーザーを Cisco ISE で作成したユーザー グループに追加します。	Cisco ISE でのユーザーの作成およびユーザー グループへのユーザーの追加 （53 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 Evolved Programmable Network Manager で作成したユーザー 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、ユーザー タスクの属性を追加する必要はありません。これらはユーザー 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 （53 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、で作成したユーザー 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 Evolved Programmable Network Manager （注） TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー 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 （54 ページ）
Cisco ISE で認証ポリシーを作成し、Cisco ISE で作成したユーザー 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 （51 ページ）
認証ポリシーを作成して、Cisco ISE が Cisco Evolved Programmable Network 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 Evolved Programmable Network Manager に対してユーザー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 （56 ページ）
Cisco Evolved Programmable Network Manager で RADIUS または TACACS+ サーバーとして Cisco ISE を追加します。	
Cisco Evolved Programmable Network Manager サーバーで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバーでの RADIUS または TACACS+ モードの設定 （49 ページ）

Cisco Evolved Programmable Network Manager でサポートされる Cisco ISE のバージョン

Cisco Evolved Programmable Network 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 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、ユーザー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、より大きなユーザーのグループ、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、限定数のユーザー、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 人のユーザーまたはユーザー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 管理者ユーザーとして 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、ユーザーグループを Cisco EPN Manager-System Monitoring-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、認証プロファイルを Cisco EPN Manager-System Monitoring-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こ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ーに、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 にクライアントとして Cisco Evolved Programmable Network Manager を追加する

ステップ 1 admin ユーザーとして 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 Evolved Programmable Network Manager サーバーのデバイス名と 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 Evolved Programmable Network Manager で Cisco ISE サーバーを RADIUS サーバー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 でのユーザー グループの作成

ステップ 1 管理ユーザーとして 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 [ユーザー 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、ユーザー 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 でのユーザーの作成およびユーザー グループへのユーザーの追加

ステップ 1 管理ユーザーとして 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 ユーザー（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、ユーザーを割り当てるユーザー 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ー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ーには、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ー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 Evolved Programmable Network Manager 内に作成したユーザー 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ー ロールの属性を追加できます。タスクはユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager ユーザー 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 ユーザーグループとロール属性のエクスポート （27 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco Evolved Programmable Network Manager 仮想ドメイン属性のエクスポート （45 ページ）を参照してください。

ステップ 1 管理ユーザーとして 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、次のアイテムのすべての RADIUS カスタム属性のリストを貼り付けます。

- ユーザー ロール
- 仮想ドメイン

（注） ユーザー 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ー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ーには、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ー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 Evolved Programmable Network Manager 内に作成したユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager ユーザー 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 ユーザーグループとロール属性のエクスポート （27 ページ）

- Cisco Evolved Programmable Network Manager 仮想ドメイン。参照先：RADIUS および TACACS+ の Cisco Evolved Programmable Network Manager 仮想ドメイン属性のエクスポート （45 ページ）

ステップ 1 管理ユーザーとして 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ー 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、ユーザー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、より大きなユーザーのグループ、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、限定数のユーザー、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 人のユーザーまたはユーザー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 管理者ユーザーとして 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、ユーザーグループを Cisco EPN Manager-System Monitoring-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、認証プロファイルを Cisco EPN Manager-System Monitoring-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こ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ーに、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 に対するユーザー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、ユーザー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、ユーザー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 上級管理ユーザーまたはシステム管理ユーザーとして 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 Evolved Programmable Network Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco Evolved Programmable Network Manager ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー 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 Evolved Programmable Network Manager でサポートされる Cisco ACS のバージョン（58 ページ）
Cisco ACS で Cisco Evolved Programmable Network 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 （58 ページ）
Cisco ACS でユーザー グループを作成します。	Cisco ACS でのユーザー グループの作成 （59 ページ）
Cisco ACS でユーザーを作成し、そのユーザーを Cisco ACS のユーザー グループに追加します。	Cisco ACS でのユーザーの作成とユーザー グループへのユーザーの追加 （59 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 Evolved Programmable Network Manager で作成したユーザー 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、ユーザー タスクの属性を追加する必要はありません。これらはユーザー 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 （59 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 Evolved Programmable Network Manager で作成したユーザー 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、ユーザー タスクの属性を追加する必要はありません。これらはユーザー 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 （60 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 （61 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 （62 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 （63 ページ）
Cisco Evolved Programmable Network Manager で RADIUS または TACACS+ サーバーとして Cisco ACS を追加します。	Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加 （48 ページ）
Cisco Evolved Programmable Network Manager サーバーで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバーでの RADIUS または TACACS+ モードの設定 （49 ページ）

Cisco Evolved Programmable Network Manager でサポートされる Cisco ACS のバージョン

Cisco Evolved Programmable Network 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 ユーザーとして 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 サーバーのデバイス名と 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 サーバーを RADIUS または TACACS+ サーバー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 でのユーザー グループの作成

ステップ 1 admin ユーザーとして 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、**[ユーザーと 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 ユーザー 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 でのユーザーの作成とユーザー グループへのユーザーの追加

ステップ 1 admin ユーザーとして 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、**[ユーザーとIDストア（Users and Identity Stores）]** > **[内部IDストア（Internal Identity Stores）]** > **[ユーザー（Users）]** の順に選択します。

ステップ 3 [内部ユーザー（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、ユーザーを割り当てるユーザー 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ー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ーには、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ー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 Evolved Programmable Network Manager 内に作成したユーザー 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ー ロールの属性を追加できます。タスクはユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager ユーザー 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 ユーザーグループとロール属性のエクスポート （27 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco Evolved Programmable Network Manager 仮想ドメイン属性のエクスポート （45 ページ）を参照してください。

ステップ 1 管理ユーザーとして 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。

- ユーザー ロール
- 仮想ドメイン

（注） ユーザー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 Evolved Programmable Network Manager で作成されたユーザー 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、ユーザータスクの属性を追加する必要はありません。これらはユーザー 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 Evolved Programmable Network 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 Evolved Programmable Network Manager ユーザー 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 ユーザーグループとロール属性のエクスポート （27 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco Evolved Programmable Network Manager 仮想ドメイン属性のエクスポート （45 ページ）を参照してください。

ステップ 1 admin ユーザーとして 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ー 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 管理ユーザーとして 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。
- [ユーザー選択のサービス タイプ（User selected service type）]：ユーザーがアクセス 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+ サーバー）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 ユーザーとして 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ー 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 ユーザーとして 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+ サーバー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 サーバーの追加 （64 ページ）
• SSO サーバーの削除 （64 ページ）
• Cisco EPN Manager サーバーでの SSO モードの設定 （65 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 サーバーの追加

プライマリ サーバーとバックアップ サーバー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 サーバー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 サーバーを設定できます。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** の順に選択し、[サーバー（Servers）] を選択します。[SSO（SSO）] タブを選択します。このウィンドウからは、新しい SSO サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 アイコンをクリックします。

ステップ 3 SSO 情報を入力します。SSO サーバー認証要求のサーバー再試行回数は最大 9 回です。

ステップ 4 **[保存（Save）]** をクリックします。

（注） SSO サーバーとして使用している Cisco EPN Manager サーバーを追加することもできます。追加するには、[自身をSSOサーバーとして追加（Add self as SSO）] チェックボックスを選択します。

SSO サーバーの削除

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

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[AAA（AAA）]** の順に選択し、[サーバー（Servers）] を選択します。[SSO（SSO）] タブを選択します。

ステップ 2 削除するサーバーを選択します。

ステップ 3 SSO サーバーの横にあるチェックボックスをクリックし、 をクリックします。[削除（Delete）] ダイアログボックスが開きます。[削除（Delete）] をクリックして確認します。

Cisco EPN Manager サーバーでの SSO モードの設定

SSO サーバーが 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 クライアントと SSO サーバーにあるサーバー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。このサーバーは、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 サーバー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ー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）] > [ユーザー（Users）] > [AAA（AAA）]** の順に選択し、[SSOの設定（SSO Settings）] を選択します。

ステップ 2 使用する [SSOサーバーAAAモード（SSO Server AAA Mode）] を選択します。一度に 1 つのみ選択できます。

ステップ 3 [シングルサインアウトの有効化（Enable Single Sign-Out）] チェックボックスをオンまたはオフにします。

ステップ 4 [チケット認可チケットタイムアウト（Ticket Granting Ticket Timeout）] ドロップダウンから期間を選択します。

ステップ 5 [すべての変更を保存（Save All Changes）] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。