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、 で使用される GUI と CLI インターフェイス、および 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、 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。

ユーザ インターフェイス	インターフェイスの説明	ユーザ タイプ
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、 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）]：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 （7 ページ）を参照してください。 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 （6 ページ）を参照してください。 （注） Web GUI ルート ユーザは、Linux CLI ルート ユーザと同じではなく、CLI 管理者ユーザとも異なります。 .

ユーザ インターフェイス	インターフェイスの説明	ユーザ タイプ
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、 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。	**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、 管理 CLI と 構成 CLI の切り替え （4 ページ）内の手順を使用します。 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 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。
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、 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。	
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、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。 この管理者ユーザは、Linux CLI ルート ユーザとしてのログインおよびログアウト （4 ページ）に記載されている手順に従って、ルート レベル権限を取得できます。ルート レベル権限が必要なタスクは、シスコ サポート チームだけが製品に関連した動作上の問題をデバッグするために実行する必要があります。セキュリティの目的で、Linux CLI 管理者ユーザとルート ユーザは無効にする必要があります。での Linux CLI ユーザの無効化および有効化 （5 ページ）を参照してください。

で CLI ユーザ インターフェイスを切り替える方法

次の図に、 を実行している展開上で と Linux の CLI ユーザ インターフェイスを切り替える方法を示します。

管理 CLI と 構成 CLI の切り替え

管理 CLI から 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)#
```

Linux CLI ルート ユーザとしてのログインおよびログアウト

Linux CLI のシェル ユーザは、管理アクセス権を持つユーザ（Linux CLI 管理者ユーザ）と、ルート アクセス権を持つユーザ（Linux CLI ルート ユーザ）の 2 つです。で CLI ユーザ インターフェイスを切り替える方法 （4 ページ）に、さまざまな CLI ユーザとしてログインおよびログアウトするためのフロー図を示しています。

Linux CLI ルート ユーザとしてログインするには、CLI 管理者ユーザから Linux CLI 管理者ユーザに移行し、さらに Linux CLI ルート ユーザに移行する必要があります。次に、実行する必要がある具体的な手順を示します。

始める前に

Linux CLI ユーザが無効になっている場合は、再度有効にします。での Linux CLI ユーザの無効化および有効化 （5 ページ）を参照してください。

ステップ 1 Linux CLI ルート ユーザとしてログインするには、次の手順を実行します。

a) サーバで SSH セッションを開始して、 CLI 管理者ユーザとしてログインします。

b) CLI 管理者ユーザが Linux CLI 管理者ユーザとしてログインします。

```
shell
Enter shell access password:  password
```

c) Linux CLI ルート ユーザとしてログインします。

```
sudo -i
```

デフォルトでは、Linux CLI のシェル プロンプトは Linux CLI 管理者およびルート ユーザに対するものと同じです。**whoami** コマンドを使用して、現在のユーザを確認できます。

ステップ 2 終了するには、次の手順を実行します。

a) Linux CLI ルート ユーザとしてログアウトします。

```
exit
```

b) Linux CLI 管理者ユーザとしてログアウトします。

```
exit
```

これで CLI 管理者ユーザとしてログインしていることになります。

次のタスク

セキュリティ上の理由から、Linux CLI ユーザを無効にします。での Linux CLI ユーザの無効化および有効化 （5 ページ） を参照してください。

Linux CLI および 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、で CLI ユーザ インターフェイスを切り替える方法 （4 ページ）の説明に従って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、 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 （6 ページ）を参照してください。

Linux CLI ルート ユーザは、インストール後に無効になります。再度有効にする必要がある場合は、での Linux CLI ユーザの無効化および有効化 （5 ページ）の手順に従います。

での Linux CLI ユーザの無効化および有効化

この手順では、 で稼働している展開環境で Linux CLI 管理シェルを無効化および有効化する方法を説明します。シェルを無効にすると、Linux CLI 管理ユーザまたはルート ユーザとしてログインできなくなります。シェルが有効にされている場合、ユーザはで CLI ユーザ インターフェイスを切り替える方法 （4 ページ）で説明している手順に従ってログインできます。

始める前に

Linux CLI 管理ユーザのパスワードが必要です。

ステップ 1 CLI 管理ユーザとして にログインします。サーバとの SSH セッションの確立を参照してください。

ステップ 2 Linux CLI 管理シェルを無効にするには（Linux CLI 管理ユーザおよびルート ユーザが無効になります）、次のコマンドを実行します。

```
shell disable
Enter shell access password: passwd
shell access is disabled
```

ステップ 3 Linux CLI管理シェルを再び有効にするには、次のコマンドを実行します（このコマンドは、CLI管理ユーザとして実行する必要があります）。

```
shell
Shell access password is not set
Configure password for shell access

Password: passwd
Password again: passwd

Shell access password is set
Run the command again to enter shell
```

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 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 （37 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 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、 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 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 （52 ページ）」を参照してください。

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 （7 ページ）

ユーザ グループのタイプ

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 （2 ページ）を参照してください）。

ユーザ グループ：Web UI

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 （35 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 （2 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 （6 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（root に似ています）。このグループの権限は編集できます。
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。

ユーザ グループ	グループ タスク フォーカス
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。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	：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

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 （35 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 Credential	
NBI Read	
NBI Write	

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 （59 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、 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 （35 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 （7 ページ） とユーザ 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 （10 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 （35 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 （34 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 （39 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 （7 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、 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 （7 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 （35 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 （10 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
APIC-EM コントローラ	APIC コントローラの読み取りアクセス（Apic Controller Read Access）	ユーザは APIC-EM コントローラの詳細を読み取ることができます。
	APIC コントローラの書き込みアクセス（Apic Controller Write Access）	ユーザは APIC-EM コントローラの詳細を作成または更新できます。
	APIC グローバル PnP の読み取りアクセス（Apic Global PnP Read Access）	ユーザは APIC グローバル PnP/Ztd の設定を読み取ることができます。
	APIC グローバル PnP の書き込みアクセス（Apic Global PnP Write Access）	ユーザは APIC グローバル PnP/Ztd の設定を作成または更新できます。
アクティブ セッション（Active Sessions）	アクセスの強制ログアウト（Force Logout Access）	ユーザは、アクティブなセッションからその他のユーザを強制的にログアウトさせることができます。

タスクグループ名	タスク名	説明
Administrative Operations	アプライアンス	ユーザは [管理（Administration）] > [設定（Settings）] > [アプライアンス（Appliance）] メニューにアクセスできます。
	アプリケーションサーバの管理アクセス（Application Server Management Access）	ユーザは NAM サーバリストを管理できます。
	アプリケーションおよびサービスへのアクセス（Application and Services Access）	ユーザはカスタムのアプリケーションとサービスを作成、変更、削除できます。
	データの移行	
	設計エンドポイントサイトの関連付けアクセス（Design Endpoint Site Association Access）	ユーザは保証サイトの分類ルールを作成できます。
	デバイス詳細 UDF（Device Detail UDF）	ユーザはデバイス詳細 UDF にアクセスできます。
	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）	

タスクグループ名	タスク名	説明
		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	ユーザは製品の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）	[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。
	ツール	ユーザは [管理（Administration）] > [システム設定（System Settings）] メニューにアクセスできます。
	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。
	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。
	Syslog ポリシー	[Syslog ポリシー（Syslog Policies）]ページへのアクセス権を付与します。
	Syslog ポリシーの編集へのアクセス（Syslog Policies Edit Access）	Syslog ポリシーを作成、変更、削除できます。
	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。

タスクグループ名	タスク名	説明
設定アーカイブ（Configuration Archive）	設定アーカイブの読み取り専用タスク（figuration Archive Read-Only Task）	ユーザはアーカイブされた設定の表示と、設定のアーカイブ収集ジョブのスケジュールができます。
	設定アーカイブの読み取り/書き込みタスク（Configuration Archive Read-Write Task）	ユーザはすべての設定アーカイブ操作を実行できます。
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。
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エクスポートできます。
	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
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）	ユーザはジョブをスケジュールできます。
	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。

タスクグループ名	タスク名	説明
マップ（Maps）	クライアント ロケーション	ユーザは地図上にクライアントの場所を表示できます。
	地図の読み取り専用（Maps Read Only）	ユーザは地図を読み取り専用モードで表示できます。
	地図の読み取り/書き込み（Maps Read Write）	ユーザは AP 配置などの地図内の要素を表示し、操作することもできます。
	プランニング モード（Planning Mode）	ユーザはプランニングモードツールを起動できます。
	不正位置	ユーザは地図上に不正な AP の場所を表示できます。
モビリティ サービス	モビリティサービス管理（Mobility Service Management）	ユーザはモビリティサービスエンジンのプロパティとパラメータを編集し、セッションとトラップの宛先を表示し、ユーザとグループアカウントを管理し、ステータス情報を管理できます。
	CAS の通知のみの表示（View CAS Notifications Only）	ユーザは CAS の通知を表示できます。

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 Prime Infrastructure 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。
	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。
	アクセスポイントの設定	ユーザはアクセスポイントを設定できます。
	Autonomous アクセス ポイント テンプレートの設定（Configure Autonomous Access Point Templates）	Prime Infrastructure の 自律型 APテンプレートにアクセスして設定できます。
	チョークポイントの設定（Configure Choke Points）	ユーザはチョークポイントにアクセスして設定できます。
	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。
	コントローラの設定	ユーザはワイヤレスコントローラの機能を設定できます。
	イーサネットスイッチポートの設定（Configure Ethernet Switch Ports）	DWC でデバイスのイーサネットの詳細を表示するときの設定機能へのアクセスを制御します。
	イーサネットスイッチの設定（Configure Ethernet Switches）	DWC でデバイスのイーサネットの詳細を表示するときの設定機能へのアクセスを制御します。
	ISE サーバの設定	ユーザは Prime Infrastructure で ISE サーバを管理できます。
	Lightweight アクセス ポイント テンプレートの設定（Configure Lightweight Access Point Templates）	Prime Infrastructure の Lightweight アクセス ポイント テンプレートを設定できます。
	モビリティデバイスの設定（Configure Mobility Devices）	ユーザはCAS、WIPS、モバイル コンシェルジュ サービス、ロケーション分析サービスを設定してモビリティ手順を示すことができます。

タスクグループ名	タスク名	説明
	Spectrum Expert の設定（Configure Spectrum Experts）	ユーザは Spectrum Expert を設定できます。
	スイッチ位置設定テンプレートの設定（Configure Switch Location Configuration Templates）	ユーザは設定テンプレートを変更できます。
	テンプレートの設定（Configure Templates）	ユーザは DWC で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。
	サードパーティ製コントローラおよびアクセスポイントの設定（Configure Third Party Controllers and Access Point）	ユーザは Prime Infrastructure でサードパーティ製コントローラとアクセスポイントを設定できます。
	WIPS プロファイルの設定（Configure WIPS Profiles）	ユーザは WIPS プロファイルにアクセスできます。
	WiFi TDoA レシーバの設定（Configure WiFi TDOA Receivers）	ユーザは WiFi TDoA レシーバを設定できます。
	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 Prime Infrastructure 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編集（Edit 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。
	グローバル SSID グループ（Global SSID Groups）	ユーザはグローバル SSID グループを設定できます。
	移行テンプレート（Migration Templates）	ユーザは自律型 AP の移行テンプレートを作成できます。
	[ネットワーク デバイス（Network Devices）]	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。
	スケジュール済みの設定タスク（Scheduled Configuration Tasks）	ユーザは設定テンプレート、設定グループ、ソフトウェアダウンロード タスクおよびテンプレートを作成してスケジュールできます。
	TrustSec 準備状況評価（TrustSec Readiness Assessment）	ユーザがネットワーク内の TrustSec を設定できる TrustSec メニューにアクセスできます。
	コンピューティングデバイスの表示	

タスクグループ名	タスク名	説明
		データセンターのコンピューティングサーバと、Prime Infrastructure で管理されているホストや仮想マシンなどの仮想要素にアクセスします。
	WIPS サービス（WIPS Service）	ユーザは WIPS サービスを設定できます。
	ワイヤレス セキュリティ	ユーザは、ワイヤレスセキュリティ設定ウィザードを使用して不正ポリシー、不正ルール、WIPS プロファイルを設定できます。

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	セキュリティインデックスの問題のACKおよびUNACK（Ack and Unack Security Index Issues）	ユーザはセキュリティインデックス侵害を確認応答または確認応答解除できます。
	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。
	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 [保証データソース（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。
	クライアントの無効化（Disable Clients）	ユーザは [無効なクライアント（Disabled Clients）] ページにアクセスできます。
	不明ユーザの識別（Identify Unknown Users）	ユーザは [不明ユーザの識別（Identify Unknown Users）] ページ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。
	Lync モニタリングアクセス（Lync Monitoring Access）	ユーザは [Lync モニタリング（Lync monitoring）] ページにアクセスして表示できます。
	モニタ アクセス ポイント	ユーザは [アクセスポイントのモニタ（Monitor Access Points）] ページを表示できます。
	チョークポイントのモニタ	ユーザは [チョークポイントのモニタ（Monitor Chokepoints）] ページにアクセスできます。
	クライアントのモニタ（Monitor Clients）	

タスクグループ名	タスク名	説明
		ユーザは[クライアントのモニタ（Monitor Clients）] ページにアクセスできます。
	イーサネットスイッチのモニタ（Monitor Ethernet Switches）	ユーザはイーサネットインターフェイス、VLAN スイッチポート、およびイーサネットスイッチの VLAN トランクをモニタできます。
	干渉源のモニタ（Monitor Interferers）	ユーザは [干渉源のモニタ（Monitor Interferers）] ページにアクセスできます。
	[モニタ（Monitor）] [メディアストリーム（Media Streams）]	ユーザは名前、開始アドレスと終了アドレス、最大帯域幅、動作ステータス、平均パケットサイズ、RRC の更新、優先度、違反など、メディアストリームの設定情報をモニタできます。
	モバイルデバイスのモニタ（Monitor Mobility Devices）	ユーザはモビリティ統計情報、モビリティレスポンダの統計情報、モビリティイニシエータの統計情報などのモビリティグループのイベントをモニタできます。
	モニタのセキュリティ	ユーザは RADIUS 認証、RADIUS アカウンティング、管理フレーム保護、不正 AP ルール、ゲストユーザなど、コントローラのセキュリティ情報をモニタできます。
	Spectrum Expert のモニタ（Monitor Spectrum Experts）	ユーザは Spectrum Expert をモニタできます。
	タグのモニタ	ユーザはタグをモニタできます。
	サードパーティ製コントローラおよびアクセスポイントのモニタ（Monitor Third Party Controllers and Access Point）	

タスクグループ名	タスク名	説明
		ユーザは[サードパーティ製コントローラとアクセスポイントのモニタ（Monitor Third Party Controllers and Access Point）]ページにアクセスできます。
	WiFi TDOA レシーバのモニタ	ユーザは[WiFi TDoAレシーバのモニタ（Monitor WiFi TDOA Receivers）]ページにアクセスできます。
	モニタリング ポリシー	ユーザは最も使用されたルールを特定し、特定のルールをトラブルシューティングして、選択したルールのヒットを確認できます。
	ネットワーク トポロジ（Network Topology）	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。
	パケットキャプチャアクセス（Packet Capture Access）	ユーザはNAMおよびサポートされているルータのパケットキャプチャを開始できます。
	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。
	PfR モニタリングアクセス（PfR Monitoring Access）	ユーザは[PfR モニタリング（PfR Monitoring）]ページにアクセスして表示できます。
	RRM ダッシュボード	ユーザはRRMダッシュボードページにアクセスできます。
	クライアントの削除（Remove Clients）	ユーザは[クライアントの削除（Remove Clients）]ページにアクセスできます。
	サービス状態へのアクセス（Service Health Access）	

タスクグループ名	タスク名	説明
		ユーザは [サービスの状態（Service Health Access）] ページにアクセスして表示できます。
	サイト可視性へのアクセス（Site Visibility Access）	ユーザはサイトの可視性にアクセスできます。
	クライアントの追跡（Track Clients）	ユーザは[クライアントの追跡（Track Clients）] ページにアクセスできます。
	セキュリティインデックスの問題の表示（View Security Index Issues）	ユーザは [セキュリティインデックスの問題（Security Index Issues）] ページにアクセスできます。
	音声診断（Voice Diagnostics）	ユーザは音声診断情報にアクセスできます。
	ワイヤレスダッシュボードへのアクセス（Wireless Dashboard Access）	ユーザはワイヤレスダッシュボードを表示できます。
オペレーションセンタータスク（Operations Center Tasks）	[サーバの管理とモニタ（Manage and Monitor Servers）] ページでの管理者権限（Administrative privileges under Manage and Monitor Servers page）	M&M ページでサーバの追加/削除/編集/アクティブ化/非アクティブ化などの管理タスクを実行できます。
	NBI 読み取りアクセス権だけを持つユーザがレポートおよびダッシュレットを使用できます。	レポートを生成し、すべてのダッシュレットに入力できるよう、NBI 読み取りアクセス権を持つユーザ向けにこのオプションを有効にします。
	[サーバの管理とモニタ（Manage and Monitor Servers）] ページへのアクセス（Manage and Monitor Servers Page Access）	[サーバの管理とモニタ（Manage & Monitor Servers）] 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
プラグアンドプレイの設定（Plug n Play Configuration）	PnP 展開履歴への読み取りアクセス（PnP Deploy History Read Access）	ユーザはプロビジョニング済みのデバイスのステータスを読み取ることができます。
	PnP 展開履歴への読み取り/書き込みアクセス（PnP Deploy History Read-Write Access）	ユーザはプロビジョニング済みデバイスで操作の読み取りおよび削除を実行できます。
	PnP ユーザ設定への読み取りアクセス	ユーザはプラグアンドプレイのユーザ設定を表示できます。
	PnP ユーザ設定への読み取り/書き込みアクセス（PnP Preferences Read-Write Access）	ユーザはプラグアンドプレイのユーザ設定を編集できます。
	PnP プロファイル展開への読み取りアクセス（PnP Profile Deploy Read Access）	ユーザはプラグアンドプレイのプロビジョニング プロファイルを表示できます。
	PnP プロファイル展開への読み取り/書き込みアクセス（PnP Profile Deploy Read-Write Access）	ユーザはプラグアンドプレイのプロビジョニング プロファイルを作成、変更、削除できます。
	PnP プロファイルへの読み取りアクセス（PnP Profile Read Access）	ユーザはプラグアンドプレイのプロファイルを表示できます。
	PnP プロファイルへの読み取り/書き込みアクセス（PnP Profile Read-Write Access）	ユーザはプラグアンドプレイのプロファイルを作成、削除、変更できます。
	WorkflowsReadWriteAccess	ユーザはシスコの IOS スイッチおよびアクセスデバイスを設定できます。
製品使用状況レポート	製品のフィードバック	ユーザは [フィードバック（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	Autonomous AP レポート	ユーザは新しい自律型 AP レポートを作成できます。
	読み取り専用自律型 AP レポート（Autonomous AP Reports Read Only）	ユーザは自律型 AP レポートを表示できます。
	CleanAir レポート	ユーザは新しい CleanAir レポートを作成できます。
	読み取り専用 CleanAir レポート（CleanAir Reports Read Only）	ユーザは CleanAir レポートを表示できます。
	クライアント レポート	ユーザはクライアントレポートを作成できます
	読み取り専用クライアントレポート（Client Reports Read Only）	ユーザはクライアントレポートを表示できます。
	コンプライアンス レポート	ユーザは設定監査、ネットワーク一の不一致、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、ネットワーク一の不一致、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。
	コンテキスト認識型レポート（Context Aware Reports）	ユーザはコンテキスト認識型/ロケーション固有のレポートを実行できます。
	読み取り専用コンテキスト認識型レポート（Context Aware Reports Read Only）	ユーザはコンテキスト認識型/ロケーション固有のレポートを実行できます。
	カスタムコンポジットレポート（Custom Composite Report）	

タスクグループ名	タスク名	説明
		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。
	カスタム NetFlow レポート（Custom NetFlow Reports）	ユーザは NetFlow カスタムレポートにアクセスできます。
	読み取り専用 NetFlow カスタムレポート	ユーザは NetFlow カスタム レポートを表示できます。
	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。
	ゲスト レポート	ユーザはゲストレポートを作成できます。
	読み取り専用ゲストレポート（Guest Reports Read Only）	ユーザはゲストレポートを表示できます。
	MSAP レポート	ユーザはモバイルコンシェルジュのレポートを実行できます。
	読み取り専用 MSAP レポート（MSAP Reports Read Only）	ユーザはモバイルコンシェルジュのレポートを実行できます。
	メッシュレポート（Mesh Reports）	ユーザはメッシュレポートを作成できます。
	読み取り専用メッシュレポート（Mesh Reports Read Only）	ユーザはメッシュレポートを表示できます。
	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。
		ユーザはすべてのサマリー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
	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）	
	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。
	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。
	Raw NetFlow レポート	ユーザは NetFlow レポートを表示できます。
	読み取り専用 Raw NetFlow レポート（Raw NetFlow Reports Read Only）	ユーザは Raw NetFlow 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。
	読み取り専用保存済みレポートリスト（Saved Reports List Read Only）	ユーザは保存済みレポートを表示できます。
	セキュリティ レポート	ユーザはセキュリティレポートを作成できます。
	読み取り専用セキュリティレポート（Security Reports Read Only）	ユーザは不正な AP、WIPS などに関連するワイヤレス セキュリティ 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。
	音声監査レポート（Voice Audit Report）	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。
	ソフトウェアイメージのアクセス権限（Software Image Access Privilege）	ユーザは [インベントリ（Inventory）]>[ソフトウェアイメージ（Software Images）] にアクセスできます。
	ソフトウェアイメージの有効化（Software Image Activation）	ユーザはネットワーク内のデバイスを管理するソフトウェアバージョンをアップグレードおよびダウングレードできます。
	ソフトウェアイメージの収集（Software Image Collection）	ユーザは、デバイス、Cisco.com、またはURLなど、さまざまな場所からイメージを収集できます。
	ソフトウェアイメージの削除（Software Image Delete）	ユーザはプラグアンドプレイのプロファイルに含まれるイメージを除き、[ソフトウェアイメージ（Software Images）] ページからイメージを削除できます。
	ソフトウェアイメージの詳細の表示（Software Image Details View）	ユーザはイメージの詳細を表示できます。
	ソフトウェアイメージの配布（Software Image Distribution）	ユーザはネットワーク内の管理対象デバイスにソフトウェアバージョンを配布できます。
	ソフトウェアイメージ情報の更新（Software Image Info Update）	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。
	ソフトウェアイメージ管理サーバ管理プロトコル（Software Image Management Server-Manage Protocols）	ユーザはプロトコルを管理できます。

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ユーザ設定の保存（Software Image Preference Save）	ユーザは[ソフトウェアイメージ（Software Images）]ページでユーザ設定のオプションを保存できます。
	推奨ソフトウェアイメージ（Software Image Recommendation）	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。
	ソフトウェアイメージのアップグレード分析（Software Image Upgrade Analysis）	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。
	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メンバーを追加する場合、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 Prime Infrastructure の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

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 （7 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。グループ名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 （39 ページ）を参照してください。

ワイヤレス ペルソナを使用したユーザの追加

ワイヤレス ペルソナを使用してローカル ユーザを追加することで、ユーザにワイヤレス関連のナビゲーション メニュー項目だけが表示されるようにすることができます。

（注） ワイヤレス ペルソナを使用して AAA ユーザまたはリモート ユーザを追加することはできません。

ステップ 1 Cisco Prime Infrastructure に管理者としてログインします。

ステップ 2 **[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 3 [コマンドの選択（Select a command）] ドロップダウン リストから、[ユーザの追加（Add User）] を選択し、[実行（Go）] をクリックします。

ステップ 4 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。

b) 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 （10 ページ）を参照してください。

c) 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。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 （52 ページ）を参照してください。

ステップ 5 [ペルソナ（Persona）] ペインで、[ワイヤレス（Wireless）] チェックボックスをオンにします。マウスのカーソルをヘルプ テキストの疑問符の上に重ねて、ナビゲーションから削除されるメニュー項目を確認します。

ステップ 6 [保存（Save）] をクリックします。

（注） 次のユーザ グループはワイヤレス ペルソナ ベースのメニューをサポートしていません。

1. Root
2. Lobby Ambassador
3. Lobby Ambassador + NBI Credential
4. Lobby Ambassador + NBI Read
5. Lobby Ambassador + NBI Write
6. Lobby Ambassador + (NBI Credential + NBI Read)
7. Lobby Ambassador + (NBI Read + NBI Write)
8. Lobby Ambassador + (NBI Credential + NBI Write)
9. Lobby Ambassador + (NBI Credential + NBI Read +NBI Write)
10. Help Desk Admin
11. Help Desk Admin + NBI Credential
12. Help Desk Admin + NBI Read
13. Help Desk Admin + NBI Writer
14. Help Desk Admin + (NBI Credential + NBI Read)
15. Help Desk Admin + (NBI Read + NBI Write)
16. Help Desk Admin + (NBI Credential + NBI Write)
17. Help Desk Admin + (NBI Credential + NBI Read +NBI Write)
18. mDNS Policy Admin

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 （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、「ユーザへの仮想ドメインの割り当て （59 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。

RADIUS および TACACS+ での ユーザ グループの使用

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 ユーザ グループとロール属性のエクスポート （36 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 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 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、 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、 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 （62 ページ）の説明に従って AAA サーバをすでに追加し、AAA モードを設定したことを確認します。

ステップ 1 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+ による外部認証 （71 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （65 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

ユーザ グループ メンバーシップの変更

ユーザが属しているユーザ グループを変更することによって、Prime Infrastructure 内のユーザの権限を簡単に変更できます。

仮想ドメインからアクセス可能なサイトまたはデバイスを割り当てることもできます。詳細については、「関連項目」の「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」を参照してください。

Prime Infrastructure では、許可されないユーザ グループ メンバーシップの特定の組み合わせがあります。たとえば、ユーザは「Root」ユーザ グループと「Lobby Ambassador」ユーザ グループに同時に属することはできません（詳細については、「ユーザが実行できるタスクの制御（ユーザ グループ）」の表を参照してください）。Prime Infrastructure ユーザの認証に RADIUS を使用している場合、RADIUS ユーザ属性/値ペアに無効なユーザ グループ メンバーシップの組み合わせを挿入しないようにしてください。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [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 3 メンバーシップを変更するユーザのユーザ名をクリックします。[ユーザ詳細（User Details）] ページが表示されます。

ステップ 4 [一般（General）] タブの [このユーザに割り当てられたグループ（Groups Assigned to This User）] で、以下を行います。

- そのユーザを追加する各ユーザ グループの横にあるチェックボックスをオンにします。
- そのユーザを削除する各ユーザ グループの横にあるチェックボックスをオフにします。

ステップ 5 完了したら、[保存（Save）] をクリックします。

関連トピック

ユーザが実行できるタスクの制御（ユーザグループ） （6 ページ）
グループで実行できるタスクを表示および変更する （35 ページ）
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 （52 ページ）

管理者権限を持つ Web GUI ユーザの作成

インストール後、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

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

（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 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 [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 6 [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 （52 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

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 （6 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 （52 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） （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）] > [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 。

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。

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 （10 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 （52 ページ）を参照）。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 ユーザ アカウントを削除するには、

ユーザ アカウントの無効化（ロック）

一時的にユーザが 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、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 （39 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 （40 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 （49 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 [コマンドの選択（Select a command）] ドロップダウンリストから [ユーザのロック（Lock User(s)）]（または [ユーザのアンロック（Unlock User(s)）]）を選択し、次に [実行（Go）] 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使用して、ユーザにパスワードを定期的に変更するように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 （49 ページ）を参

照）。ユーザは、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すぐに変更する必要がある場合は、次の手順を使用します。

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。

ゲスト アカウントの設定

Prime Infrastructure 管理者は次の選択ができます。

- 期限切れのゲスト アカウントをすべて強制的に自動削除する。
- Lobby Ambassador のゲスト アカウントに対する制御を、その Lobby Ambassador が作成したアカウントのみに制限する。

これらの選択肢はいずれも、Lobby ambassador がこれらの一時ゲスト アカウントの管理する必要がある範囲に制限を加えることになります。Lobby ambassador の使用に関する詳細については、「関連項目」の「Lobby Ambassador を使用したゲスト ユーザ アカウントの管理」を参照してください。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [ゲスト アカウント（Guest Account）] の順に選択します。

ステップ 3 次のように、オプション ボタンの選択を変更します。

- [期限切れのゲスト アカウントを自動削除する（Automatically remove expired guest accounts）] を選択して、ライフタイムが終了したゲスト アカウントが [期限切れ（Expired）] 状態に移行されるようにします。[期限切れ（Expired）] 状態のゲスト アカウントは Prime Infrastructure から自動的に削除されます。
- [この Lobby Ambassador が作成したゲスト アカウントのみを検索して一覧表示（Search and List only guest accounts created by this lobby ambassador）] を選択して、作成したゲスト アカウントしか変更できないように Lobby Ambassador を制限します。デフォルトでは、Lobby Ambassador は、どのユーザが作成したかに関係なく、任意のゲスト アカウントを変更または削除できます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

Lobby Ambassadors を使用したゲスト ユーザ アカウントの管理 （42 ページ）
ユーザが実行できるタスクの制御（ユーザグループ） （6 ページ）

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 （52 ページ）

Lobby Ambassadors を使用したゲスト ユーザ アカウントの管理

Lobby Ambassador アカウントは、特殊な Prime Infrastructure 管理アカウントであり、一時ゲスト ユーザ アカウントの追加、管理、廃棄に使用されます。Lobby Ambassador アカウントは、Lobby Ambassador プロファイルで規定されるきわめて限定的なネットワーク設定権限を持ち、ゲスト アカウントの管理に使用される Prime Infrastructure 機能のみにアクセスできます。

通常、企業によって提供されるゲスト ネットワークは、企業のホストを危険にさらすことなく、ゲストがインターネットにアクセスできるようにします。Web 認証は専用クライアントなしで提供されるのが普通であるため、大半のゲストはそれらの目的の宛先への VPN トンネルを開始する必要があります。

Prime Infrastructure では、有線および無線の両方のゲスト ユーザ アクセスを許可しています。有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスまたは会議室の特定のポート経由で利用可能にすることもできます。無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。

Lobby Ambassador では、次の種類のゲスト ユーザ アカウントを作成できます。

- ライフタイムの期限があるゲスト ユーザ アカウント。指定した時間が経過すると、ゲスト ユーザ アカウントは自動的に失効します。
- ライフタイムの期限がないゲスト ユーザ アカウント。このアカウントには有効期限がありません。
- 事前に定義された将来の時刻にアクティブ化されるゲスト ユーザ アカウント。Lobby Ambassador では、有効期間の開始と終了が定義されています。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ゲスト ユーザ アカウントの管理：ワークフロー

Lobby Ambassador は、次のワークフローに従ってゲスト ユーザ アカウントを管理できます。

1. ゲスト ユーザ アカウントの作成：Lobby Ambassador としてログインし、ゲスト ユーザ アカウントを必要に応じて作成します。
2. ゲスト ユーザ アカウントのスケジュール設定：Lobby Ambassador としてログインし、ゲスト ユーザ アカウントの自動作成のスケジュールを設定します。

3. ゲストユーザ詳細の印刷または電子メール送信：Lobby Ambassador としてログインし、ゲスト ユーザ アカウントの詳細を印刷したり、ゲストを受け入れるホストや個人にこの情報を電子メールで送信します。

フル アクセスが可能な Prime Infrastructure 管理者は、次のワークフローを使用して、Lobby Ambassador とそれらの作業を管理できます。

1. Lobby Ambassador アカウントの作成：Prime Infrastructure 管理者としてログインし、Lobby Ambassador アカウントを必要に応じて作成します。
2. Lobby Ambassador アクティビティの表示：Prime Infrastructure 管理者としてログインし、ログを使って Lobby Ambassador のアクティビティを管理します。

Lobby Ambassador アカウントの作成 （43 ページ）
ロビー アンバサダーとしてのゲスト ユーザ アカウントの作成 （44 ページ）
ゲスト ユーザ アカウントのスケジュール設定 （44 ページ）
ゲスト ユーザの詳細の印刷または電子メールでの送信 （45 ページ）
Lobby Ambassador アクティビティの表示 （46 ページ）

Lobby Ambassador アカウントの作成

Lobby Ambassador アカウントの作成を開始する前に、デバイスで正しく時間設定が行われていることを確認する必要があります（正しくない場合、ゲスト ユーザ アカウントが検出された後のアカウント ライフタイムに誤りが生じます）。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [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 3 [コマンドの選択（Select a command）] > [ユーザの追加（Add User）] > [実行（Go）] の順に選択します。

ステップ 4 次のように必須フィールドに入力します。

a) [このユーザに割り当てられたグループ（Groups Assigned to this User）] セクションで、[Lobby Ambassador] チェックボックスをオンにすると、[Lobby Ambassador のデフォルト（Lobby Ambassador Defaults）] タブが表示されます。

b) [Lobby Ambassador のデフォルト設定（Lobby Ambassador Defaults）] タブの必須フィールドに入力します。

c) [仮想ドメイン（Virtual Domains）] タブをクリックし、この Lobby Ambassador アカウントの仮想ドメインを割り当てます。

d) [使用可能な仮想ドメイン（Available Virtual Domains）] リストで、このユーザにアクセスを許可する仮想ドメインをクリックしてハイライト表示します。続いて [追加（Add）] をクリックして、これを [選択済みの仮想ドメイン（Selected Virtual Domains）] リストに追加します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）

ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ロビー アンバサダーとしてログインする

Prime Infrastructure ユーザ インターフェイスにログインするには、Lobby Ambassador のユーザ名とパスワードを使用する必要があります。Lobby Ambassador としてログインすると、[ゲスト ユーザ（Guest User）] ページが開き、作成済みのすべてのゲスト ユーザのサマリが表示されます。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ロビー アンバサダーとしてのゲスト ユーザ アカウントの作成

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [コマンドの選択（Select a command）] > [ユーザ グループの追加（Add User Group）] > [実行（Go）] の順に選択します。

ステップ 3 [一般（General）] タブおよび [詳細設定（Advanced）] タブの必須フィールドに入力します。

フィールドの説明については、リファレンス ガイドを参照してください。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ゲスト ユーザ アカウントのスケジュール設定

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [コマンドの選択（Select a command）] > [ゲストユーザのスケジュール（Schedule Guest User）] > [実行（Go）] の順に選択します。

ステップ 3 **必須**パラメータを設定します。

[各スケジュールで新規パスワードを生成します（Generate new password on every schedule）] および [どの曜日にも生成しない（No days of the week）] チェックボックスがオンの場合、ユーザはアカウントが有効な期間全体に対して 1 つのパスワードを使用します。

[各スケジュールで新規パスワードを生成します（Generate new password on every schedule）] および [どの曜日にも生成する（Any days of the week）] チェックボックスがオンの場合、ユーザは毎日新しいパスワードを使用します。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ゲスト ユーザの詳細の印刷または電子メールでの送信

Lobby Ambassador では、ゲスト ユーザ アカウントの詳細を印刷したり、ゲストを受け入れるホストや個人にこの情報を電子メールで送信できます。電子メールや印刷済みシートには、次のアカウント詳細が示されます。

- ゲスト ユーザ アカウント名。
- ゲスト ユーザ アカウントのパスワード。
- ゲスト ユーザ アカウントが有効化される日付と時刻。
- ゲスト ユーザ アカウントが期限切れになって終了する日付と時刻。
- ゲスト ユーザに割り当てられるプロファイル ID。使用する Profile ID については管理者に問い合わせてください。
- ゲスト ユーザに関する免責事項情報。

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [ゲスト ユーザ（Guest User）] ページで、アカウント詳細を送信するユーザ名の横にあるチェックボックスをオンにします。

ステップ 3 [コマンドの選択（Select a command）] > [ユーザ詳細を印刷/電子メールで送信（Print/E-mail User Details）] > [実行（Go）] の順に選択します。次のように続けます。

- 印刷する場合は、[印刷（Print）] **をクリックします。[印刷（Print）]** ページで、プリンタを選択して [印刷（Print）] をクリックします。
- 電子メールを送信する場合は、[電子メール（Email）] をクリックします。[電子メール（Email）] ページで、件名行に入力し、受信者の電子メールアドレスを入力して、[送信（Send）] をクリックします。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

Lobby Ambassador アクティビティの表示

Prime Infrastructure 管理者は、監査証跡機能を使用して Lobby Ambassador を管理できます。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles, & AAA）] > [ユーザ グループ（User Groups）] の順に選択します。

ステップ 3 表示する Lobby Ambassador アカウントの [監査証跡（Audit Trail）] アイコンをクリックします。Lobby Ambassador の [監査証跡（Audit Trail）] ページが表示されます。このページで、Lobby Ambassador アクティビティ一覧を時系列表示できます。

- ユーザのログイン名
- 監査された操作の種類
- 操作が監査された時刻
- ログインの成功または失敗
- ログイン失敗の理由（無効なパスワードなど）を示します。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ゲスト アカウントのデバイスへの保存

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [ゲスト ユーザ（Guest User）] ページの [デバイスにゲストアカウントを保存（Save Guest Accounts on Device）] チェックボックスをオンにして、ゲスト アカウントを Cisco Wireless LAN Controller（WLC）フラッシュに保存すると、WLC リブート時にもアカウントを保持できます。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト ユーザのクレデンシャルの編集 （46 ページ）

ゲスト ユーザのクレデンシャルの編集

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [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 3 クレデンシャルを編集するユーザ名をクリックします。

ステップ 4 対象のクレデンシャルに変更を加えます。

編集の際、[プロファイル（Profile）] の選択が削除されている場合（[プロファイルの選択（Select a profile）] に変更されている場合）、この Lobby Ambassador のデフォルト値は削除されています。デフォルト値を再び有効にするには、設定し直す必要があります。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザ アカウントの管理：ワークフロー （42 ページ）
ゲスト アカウントのデバイスへの保存 （46 ページ）

現在ログイン中のユーザの確認

現在 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。

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。 により、 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 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。

ユーザが実行するタスクを表示する（監査証跡）

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、 によって、各スイッチの監査エントリが表示されます。

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（47 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（）
- 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、が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。

ステップ 4 [保存（Save）] をクリックします。

ユーザ ジョブ用のジョブ通知メールを設定する

Last_Run_Status に次のステータスが表示される場合は、すべてのユーザジョブにジョブ通知メールを送信するように を設定できます。 [失敗（Failure）]、[一部成功（Partial Success）]、[成功（Success）] ユーザ ジョブに関するジョブ通知メールの設定を構成するには、次の手順を使用します。

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、**[メールと通知（Mail and Notification）] > [ジョブ通知メール（Job Notification Mail）]** を選択します。

ステップ 2 [ジョブ通知メールの有効化（Enable Job Notification Mail）] チェックボックスをオンにして、通知を有効にします。

ステップ 3 [宛先（To）] テキスト ボックスに、電子メール アドレスを入力します。デフォルトで、[メール サーバ設定（Mail Server Configuration）] で設定された電子メール アドレスまたは事前に設定された電子メール アドレスが [宛先（To）] テキスト ボックスに表示されます。で説明されている手順を実行することによって、電子メールサーバを設定できます。 電子メール サーバ設定の構成

ステップ 4 [件名（Subject）] テキスト ボックスに、ジョブ通知メールの件名を入力します。件名は、自動的にジョブ名が付加されます。

ステップ 5 [ジョブステータス（Job Status）] を選択します。[成功（Success）]、[一部成功（Partial Success）]、または [失敗（Failure）] のステータスオプションのいずれかか、または両方のオプションを選択して、受信者のアドレスを指定できます。

ステップ 6 [コンプライアンス監査ジョブ（Compliance Audit Job）] チェックボックスと [コンプライアンス修正ジョブ（Compliance Fix Job）] チェックボックスをオンにします。ジョブ通知メールは、選択したジョブに対してトリガーされます。

ステップ 7 [保存（Save）]をクリックします。ジョブ通知メールは、選択したジョブステータスに対してのみトリガーされ、ジョブの完了後にのみ送信されます。設定されたメールサーバに指定されているサイズをファイルサイズが超えた場合、ジョブ通知メールは受信されません。

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（ 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 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（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。

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

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。

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（51 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。

次のタスク

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。

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。

ユーザ当たりの最大セッション数の設定

Web GUI を使用してユーザあたりの最大セッション数を設定するには、次の手順に従います。

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

ステップ 2 ユーザあたりの最大セッション数を設定するには、[最大セッション数（Max Sessions）] テキスト ボックスに値を入力します。入力可能な値は 1 ～ 50 で、デフォルト値は 5 です。

ステップ 3 完了したら、[保存（Save）] をクリックします。

ステップ 4 サーバを再起動して、変更を適用します。

（注） このセッション制限は、ローカル サーバ、RADIUS サーバ、および TACACS+ サーバにのみ適用されます。このセッション制限は HA モードおよび SSO モードには適用されません。

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 （59 ページ）
• 仮想ドメインの削除 （60 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 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。 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。

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 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 （54 ページ）
• 検索と仮想ドメイン （54 ページ）
• アラームと仮想ドメイン （54 ページ）
• マップおよび仮想ドメイン （54 ページ）
• 設定テンプレートと仮想ドメイン （54 ページ）

• グループおよび仮想ドメインの設定 （55 ページ）
• 電子メール通知と仮想ドメイン （55 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 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 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 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 （55 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 （56 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 （57 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 （56 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 （58 ページ）の手順に従い、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 （55 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。

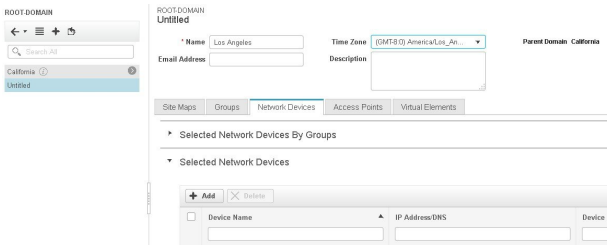
ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、次の手順を実行します。

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。

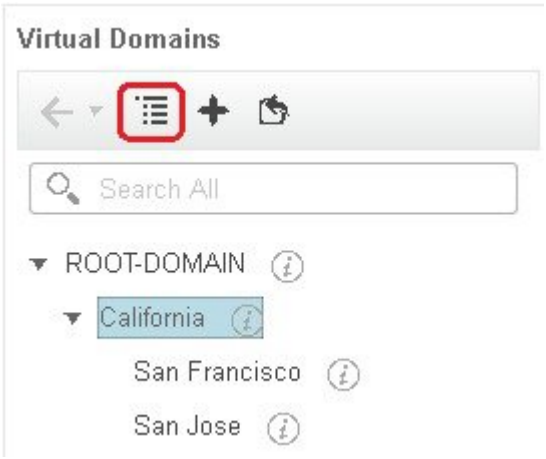
ステップ 3 [名前（Name）]テキストボックスに名前を入力します。これは必須です。この例では、新しい子ドメインに **Los Angeles** という名前を付けます。（ナビゲーション ペインに表示される名前は、新しい子ドメインを保存するまでは、[無題（Untitled）] から [Los Angeles] に変更されません。）



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 ペイに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 （58 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 （58 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 [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 4 [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 （59 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。

仮想ドメインへのグループの追加

デバイス グループを仮想ドメインに追加するには、次の手順に従います。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [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 3 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、ロケーション グループを追加する仮想ドメインをクリックします。

ステップ 4 [グループ（Group）] タブで [追加（Add）] をクリックして、使用可能なロケーションとユーザ定義グループのリストを表示します。

[グループの追加（Add Group）] ウィンドウが表示されます。

ステップ 5 [グループの追加（Add Group）] ウィンドウには、自分に該当するグループのみが表示されます。これらのグループは仮想ドメインに追加できます。[すべてのロケーション（All Locations）] で必要なグループの

チェック ボックスを選択し、[選択（Select）] をクリックして、デバイスを [選択されたグループ（Selected Groups）] テーブルに追加します。

（注） 選択したグループが親グループの場合、そのすべての子グループが自動的に仮想ドメインに追加されます。

ステップ 6 [送信（Submit）] をクリックして、仮想ドメインのサマリーを表示します。

ステップ 7 [保存（Save）] をクリックして、変更を確定します。

[グループ（Groups）] タブから追加されたこれらのグループには、作成、読み取り、更新、削除の各権限が設定されます。

ステップ 8 ユーザ アカウントの作成に進みます。

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+ で仮想ドメインを使用する （60 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 （58 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 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 から削除されません（ネットワーク要素は引き続き 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、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 仮想ドメインを使用する

RADIUS または TACACS+ サーバは、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。RADIUS および TACACS+ の 仮想ドメイン属性のエクスポート （61 ページ）の手順を使用して、これを実行できます。

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、 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。

- 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。
- 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 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、 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。 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、 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 （62 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 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。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 （71 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （65 ページ）

ローカル認証の設定

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 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 （49 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 （62 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 （62 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 を設定する必要があります。

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、 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 （78 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 RADIUS、TACACS+、SSO サーバと通信するように 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、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。

CLI から外部認証を設定するには、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 （63 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （65 ページ）
- Cisco ACS と RADIUS または TACACS+ による外部認証 （71 ページ）
- SSO による外部認証 （78 ページ）

と LDAP サーバの統合

では、LDAP サーバを使用した外部認証がサポートされています。この設定に興味がある場合は、シスコ担当者までお問い合わせください。

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 を設定する方法について説明します。

- への RADIUS または TACACS+ サーバの追加 （63 ページ）
- サーバ上で RADIUS または TACACS+ モードを設定する （64 ページ）

への RADIUS または TACACS+ サーバの追加

RADIUS または TACACS+ サーバを 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。 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、プライマリ サーバの仮想 IP アドレスまたは物理 IP アドレスのいずれかを選択します。

（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。

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。

ステップ 5 [保存（Save）] をクリックします。

Prime Infrastructure の IP アドレス変更後の必須 TACACS+/RADIUS 設定

TACACS+ または RADIUS サーバを追加した後で、Prime Infrastructure サーバの IP アドレスを変更した場合は、手動で、Prime Infrastructure サーバの新しい IP アドレスで TACACS+ または RADIUS サーバを設定する必要があります。Prime Infrastructure は RADIUS または TACACS+ 要求が送信されるローカルインターフェイスをキャッシュに保存するため、Prime Infrastructure の IP アドレスが確実に更新されるように RADIUS または TACACS+ サーバの設定を手動で編集する必要があります。

関連トピック

への RADIUS または TACACS+ サーバの追加 （63 ページ）
新しい Prime Infrastructure バージョンのインストール後の AAA 設定の更新 （65 ページ）

新しい Prime Infrastructure バージョンのインストール後の AAA 設定の更新

既存のデータを Prime Infrastructure の新しいバージョンに移行する前に、外部 RADIUS または TACACS+ ユーザ認証を使用していた場合は、拡張した Prime Infrastructure ユーザ タスク リストを AAA サーバに転送する必要があります。Prime Infrastructure をアップグレードした後、TACACS+ または RADIUS サーバに権限を再度追加し、Prime Infrastructure サーバからのタスクで TACACS サーバのロールを更新する必要があります。

関連トピック

への RADIUS または TACACS+ サーバの追加 （63 ページ）
Prime Infrastructure の IP アドレス変更後の必須 TACACS+/RADIUS 設定 （64 ページ）

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 を統合し、RADIUS または TACACS+ プロトコルを使用して 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。

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。	でサポートされる Cisco ISE のバージョン （66 ページ）
Cisco ISE で 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 を追加する （66 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 （67 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 （67 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、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 （67 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。 （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 （69 ページ）
認証ポリシーを作成して、Cisco ISE が と通信するために使用する必要があるプロトコルと 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 （71 ページ）
で RADIUS または TACACS+ サーバとして Cisco ISE を追加します。	への RADIUS または TACACS+ サーバの追加 （63 ページ）
サーバで RADIUS または TACACS+ モードを設定します。	サーバ上で RADIUS または TACACS+ モードを設定する （64 ページ）

でサポートされる Cisco ISE のバージョン

。

Cisco ISE にクライアントとして 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 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、 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、 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 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。

- ユーザ ロールとタスク：を参照してください。RADIUSおよびTACACS+のユーザ グループとロール属性のエクスポート （36 ページ）
- 仮想ドメイン。参照先：RADIUS および TACACS+ の 仮想ドメイン属性のエクスポート（61 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 **[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+ 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、 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。
- リリース8.5.135.0では、認可サーバの作成は廃止されています。認可サーバを作成するには、認証サーバを作成して、認可サーバとして複製する必要があります。この機能変更により、Cisco Prime Infrastructure 3.2では次のようなアラームが生成されます。

  ```
  1.Successfully created Authentication server. 2.Failed to create
  authorization server:SNMP operation to Device failed: SetOperation
  not allowed for TACACS authorization server.1.Successfully
  createdAccounting server.
  ```

  Cisco Prime Infrastructureでの回避策は、テンプレート上で認可サーバをオフにすることです。詳細については、『CSCvm01415』を参照してください。

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。

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 Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）]** の順に選択します。

ステップ 3 左側のサイドバーから、[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 [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 6 [raw ビュー（Raw View）] 領域に、以下についての TACACS+ 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

ステップ 7 **[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、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 -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 -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、 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 TACACS 認証ポリシーの設定

Cisco ISE で TACACS 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 管理ユーザとして Cisco ISE にログインします。

ステップ 2 **[デバイス ワーク センター（Device Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** の順に選択します。

ステップ 3 左側のペインで [デフォルト（Default）] を選択します。

ステップ 4 [認証ポリシー（Authorization Policy）] 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 5 ルール名を入力し、アイデンティティ グループ、条件、認証ポリシーのシェル プロファイルを選択します。

たとえば、ユーザ グループを -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 -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、 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 6 [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 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、 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、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 を統合し、RADIUS または TACACS+ プロトコルを使用して 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。	でサポートされる Cisco ACS のバージョン （73 ページ）
Cisco ACS で 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 を追加する （73 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 （73 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 （73 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、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 （74 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、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 （75 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 用アクセス サービスの作成 （76 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 （77 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 （77 ページ）
で RADIUS または TACACS+ サーバとして Cisco ACS を追加します。	への RADIUS または TACACS+ サーバの追加 （63 ページ）

サーバで RADIUS または TACACS+ モードを設定します。	サーバ上で RADIUS または TACACS+ モードを設定する（64 ページ）

でサポートされる Cisco ACS のバージョン

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 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 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、 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、 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 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。

- 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 ユーザ グループとロール属性のエクスポート （36 ページ）
- 仮想ドメイン。参照先：RADIUS および TACACS+ の 仮想ドメイン属性のエクスポート（61 ページ）

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、 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 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。

- ユーザロールとタスク：を参照してください。RADIUS および TACACS+ のユーザ グループとロール属性のエクスポート （36 ページ）
- 仮想ドメイン：参照項目：RADIUS および TACACS+ の 仮想ドメイン属性のエクスポート（61 ページ）。

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 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。

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 （78 ページ）

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

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）]** の順に選択し、[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。

Prime Infrastructure サーバで SSO モードを設定する

シングル サインオン（SSO）認証は、マルチユーザ、マルチリポジトリ環境でのユーザの認証および管理に使用されます。SSO サーバは、異種のシステムへのログインに使用されるクレデンシャルの保存および取得を行います。 の他のインスタンス用の SSO サーバとして をセットアップできます。

（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）] > [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。オプションは次のとおりです。[ローカル（Local）]、[RADIUS]、または [TACACS+]。

ステップ 3 [保存（Save）] をクリックします。