ユーザの管理

ユーザー プロファイルについて

ユーザープロファイルで、ユーザーのログイン、パスワード、およびロール（権限）を定義します。

ユーザーの内部プロファイルと外部プロファイルの両方を設定できます。内部ユーザープロファイルは Cisco DNA Center に配置され、外部ユーザープロファイルは外部 AAA サーバーに配置されます。

Cisco DNA Center をインストールすると、SUPER-ADMIN-ROLE 権限を持つデフォルトのユーザープロファイルが作成されます。

ユーザ ロールの概要

実行できる機能を指定する次のユーザロールがユーザに割り当てられます。

- **管理者（SUPER-ADMIN-ROLE）**：このロールを持つユーザは、Cisco DNA Center のすべての機能へのフルアクセスが可能です。管理者は、SUPER-ADMIN-ROLE を含むさまざまなロールを持つ他のユーザプロファイルを作成できます。
- **ネットワーク管理者（NETWORK-ADMIN-ROLE）**：このロールを持つユーザは、Cisco DNA Center のすべてのネットワーク関連機能へのフルアクセスが可能です。ただし、バックアップと復元など、システム関連の機能へのアクセス権はありません。
- **オブザーバ（OBSERVER-ROLE）**：このロールを持つユーザは、Cisco DNA Center の機能への表示専用アクセスが可能です。オブザーバ ロールを持つユーザは、Cisco DNA Center やそれが管理するデバイスを設定または制御する機能にはアクセスできません。

内部ユーザーの作成

ユーザーを作成し、このユーザーにロールを割り当てることができます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （1 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 新しいユーザーの姓、名、電子メールアドレス、およびユーザー名を入力します。

電子メールアドレスは、標準の Apache EmailValidator クラスの要件を満たしている必要があります。

ステップ 4 [Role List] で、SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、または OBSERVER-ROLE のいずれかのロールを選択します。

ステップ 5 パスワードを入力し、確認します。パスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 6 [Save] をクリックします。

ユーザーの編集

一部のユーザープロパティは編集できますが、ユーザー名は編集できません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （1 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 編集するユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Edit] をクリックします。

ステップ 4 必要に応じて、姓名または電子メールアドレスを編集します。

ステップ 5 [Role List] で、必要に応じて新しいロール（[SUPER-ADMIN-ROLE]、[NETWORK-ADMIN-ROLE]、または [OBSERVER-ROLE]）を選択します。

ステップ 6 [Save] をクリックします。

ユーザーの削除

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （1 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 削除するユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Delete] をクリックします。

ステップ 4 確認のプロンプトで、[Continue] をクリックします。

ユーザーパスワードのリセット

別のユーザーのパスワードをリセットできます。

セキュリティ上の理由から、パスワードは、どのユーザーに対しても（管理者権限を持つユーザーに対しても）表示されません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （1 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 パスワードをリセットするユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Reset Password] をクリックします。

ステップ 4 パスワードを入力し、確認します。新しいパスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 5 [Save] をクリックします。

自身のユーザーパスワードの変更

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、「ユーザ ロールの概要」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Change Password]** の順にクリックします。

ステップ 2 必要なフィールドに情報を入力します。

ステップ 3 [更新（Update）] をクリックします。

管理者権限なしでのユーザーパスワードの変更

次の手順では、管理者権限なしでパスワードを変更する方法について説明します。

ステップ 1 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings]** > **[My Account]** の順に選択します。

ステップ 2 [Password] フィールドで、[Update Password] をクリックします。

ステップ 3 [Update Password] ダイアログボックスで、現在のパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

ステップ 4 [更新（Update）] をクリックします。

思い出せないパスワードのリセット

パスワードを忘れた場合は、CLI を使用してパスワードをリセットできます。

ステップ 1 システムでそのユーザーが作成されているかどうかを確認するには、次のコマンドを入力します。

```
magctl user display <username>
```

このコマンドは、パスワードをリセットするために使用できるテナント名を返します。出力は、次のようになります。

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

ステップ 2 パスワードをリセットするには、次のコマンドにテナント名を入力します。次のコマンドを入力します。

```
magctl user password update <username> <tenant-name>
```

新しいパスワードを入力するように求められます。

ステップ 3 新しいパスワードを入力します。

確認のために新しいパスワードを再入力するよう求められます。

ステップ 4 新しいパスワードを入力します。パスワードがリセットされ、新しいパスワードを使用して Cisco DNA Center にログインできます。

ロールベース アクセス コントロールの設定

Cisco DNA Center は、ロールベース アクセス コントロール（RBAC）をサポートしています。これにより、SUPER-ADMIN-ROLE 権限を持つユーザーは、特定の Cisco DNA Center 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 カスタムロールを定義します。

a) 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Role Based Access Control]** の順に選択します。

b) [Create a New Role] をクリックします。
[Create a Role] ウィンドウが表示されます。これが RBAC の最初のイテレーションである場合、新しいロールを作成した後に、ユーザーを新しいロールに割り当てるように求められます。

c) タスクの概要ウィンドウが開いたら、[Let's do it] をクリックして、ワークフローに直接移動します。
[Create a New Role] ウィンドウが開きます。

d) ロール名を入力し、[Next] をクリックします。
[Define the Access] ウィンドウが開き、オプションのリストが表示されます。デフォルトでは、Cisco DNA Center のすべての機能に対してオブザーバロールが設定されています。

e) 目的の機能に対応する [>] アイコンをクリックして、関連付けられている機能を表示します。

f) それぞれの機能の権限レベルを必要に応じて [Deny]、[Read]、または [Write] に設定します。

機能の権限レベルを [Deny] に設定すると、このロールを割り当てられたユーザーは該当する機能を GUI で表示できなくなります。

g) [Next] をクリックします。
[Summary] ウィンドウが開きます。

h) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
[Done, Role-Name] ウィンドウが開きます。

ステップ 2 作成したカスタムロールにユーザーを割り当てるには、[Add Users] をクリックします。

[User Management] > **[Internal Users]** ウィンドウが開きます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。

  1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザーの横にあるオプションボタンをクリックし、次に [Edit] をクリックします。

     [Update Internal User] スライドインペインが開きます。

  2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。

- カスタムロールを新規ユーザーに割り当てるには、次の手順を実行します。

  1. [Add] をクリックします。

     [Create Internal User] スライドインペインが開きます。

  2. 表示されるフィールドに氏名とユーザー名を入力します。

3. [Role List] ドロップダウンリストから、新規ユーザーに割り当てるカスタムロールを選択します。
4. 新しいパスワードを入力し、確認のために再度入力します。
5. [Save] をクリックします。

ステップ 3 既存のユーザーのログイン中に管理者がそのユーザーのアクセス権限を更新した場合、新しい権限設定を有効にするには、ユーザーが Cisco DNA Center からログアウトして、ログインし直す必要があります。

Cisco DNA Center ユーザー ロール権限

表 *1 : Cisco DNA Center* ユーザー ロール権限

機能	説明
アシュアランス	ネットワークのあらゆる側面を完全に可視化して一貫したサービスレベルを維持できます。
モニターリングおよびトラブルシューティング	問題のトラブルシューティングと修復、プロアクティブなネットワークモニタリング、および AI ネットワーク分析 から得られるインサイトにより、ネットワークの正常性のモニタリングと管理を行います。 このロールでは次のことが可能です。 • 問題の解決、クローズ、無視。 • 機械推論エンジン（MRE）のワークフローの実行。 • トレンドとインサイトの分析。 • パストレース、センサーダッシュボード、不正管理などの問題のトラブルシューティング。 • 不正および Cisco Advanced Wireless Intrusion Prevention System（aWIPS）のワークフローの実行。これらのワークフローには、AP 許可リスト、ベンダー許可リスト、aWIPS プロファイルの作成、aWIPS プロファイルの割り当てなどが含まれます。
モニターリングの設定（Monitoring Settings）	問題の設定と管理を行います。ネットワーク、クライアント、およびアプリケーションの正常性のしきい値を更新します。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。

機能	説明
トラブルシューティング ツール	センサーテストの作成と管理を行います。クライアントのトラブルシューティングのためのオンデマンドのフォレンジック パケットキャプチャ（インテリジェントキャプチャ）をスケジュールします。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。
ネットワーク分析	ネットワーク分析関連のコンポーネントを管理します。
データアクセス	クエリエンジン API へのアクセスを有効にします。グローバル検索、不正管理、aWIPS などの制御機能。 注：許可を [Deny] に設定すると、検索と アシュアランス 機能に影響します。
ネットワーク設計	ネットワーク階層の設定、ソフトウェア イメージ リポジトリの更新、サイトやネットワークデバイスの管理に使用するネットワークプロファイルと設定の構成を行います。
詳細ネットワーク設定	• グローバルデバイスログイン情報、認証サーバーとポリシーサーバー、証明書、信頼できる証明書、クラウドアクセスキー、Stealthwatch、Umbrella、データ匿名化などのネットワーク設定を更新します。 • デバイスインベントリとそのクレデンシャルをエクスポートします。 注：このタスクを完了するには、[Network Settings] に対する書き込み権限が必要です。
イメージリポジトリ	ソフトウェアイメージを管理し、物理および仮想ネットワークエンティティのアップグレードと更新を促進します。
ネットワーク階層	サイト、ビルディング、フロア、およびエリアのネットワーク階層を地理的な場所に基づいて定義および作成します。このロールを持つユーザーは、**[System]** > **[Settings]** で CMX サーバーを追加することもできます。
ネットワーク プロファイル	ルーティング、スイッチング、およびワイヤレスのネットワークプロファイルを作成します。サイトへプロファイルを割り当てます。このロールには、テンプレートハブ、タギング、モデル設定エディタ、および認証テンプレートが含まれます。 注：SSID を作成するには、[Network Settings] に対する書き込み権限が必要です。
ネットワーク設定	AAA、NTP、DHCP、DNS、Syslog、SNMP、テレメトリなど、サイト全体の共通のネットワーク設定。このロールを持つユーザーは、**[System]** > **[Settings]** で SFTP サーバーの追加とネットワーク再同期間隔の変更が可能です。 注：ワイヤレスプロファイルを作成するには、[Network Profiles] に対する書き込み権限が必要です。CMX サーバーをサイト、ビルディング、またはフロアに割り当てるには、[Network Hierarchy] に対する書き込み権限が必要です。

機能	説明
仮想ネットワーク	仮想ネットワーク（VN）を管理します。トラフィックの分離やVN間通信の制御のために、物理ネットワークを複数の論理ネットワークにセグメント化します。
ネットワーク プロビジョニング	ネットワークデバイスの設定、アップグレード、プロビジョニング、および管理を行います。
コンプライアンス	コンプライアンス プロビジョニングを管理します。
EoX	ネットワーク内のハードウェアおよびソフトウェアの [End of Life]、[End of Sales]、または [End of Support] に関連する公開情報の詳細について、ネットワークをスキャンします。 注：EoX スキャンを表示するには、[Compliance] に対する読み取り権限が必要です。EoX スキャンを実行するには、[Compliance] に対する書き込み権限が必要です。
イメージの更新	完全なアップグレード ライフサイクルの後で、ゴールデンイメージ設定に一致しないデバイスのソフトウェアイメージをアップグレードします。
インベントリ管理	ネットワーク上のデバイスの検出、追加、置換、削除、およびデバイス属性と設定プロパティの管理を行います。 注：デバイスを交換するには、**[Network Provision]** > **[PnP]** に対する書き込み権限が必要です。
[Inventory Management] > [Device Configuration]	デバイス設定：デバイスの実行構成を表示します。
[Inventory Management] > [Discovery]	ディスカバリ：ネットワーク内の新しいデバイスを検出します。
[Inventory Management] > [Network Device]	ネットワークデバイス：インベントリからデバイスを追加し、デバイスの詳細を表示し、デバイスレベルのアクションを実行します。
	インベントリインサイト：速度/デュプレックス設定の不一致やVLANの不一致などのデバイスの問題や、各問題が発生した回数を表示します。問題を解決するためにユーザーが実行する詳細なアクションを提供します。この情報には、可能な設定変更を含むアクションが必要であるため、読み取り専用ロールのユーザーには表示されません。
[Inventory Management] > [Port Management]	ポート管理：デバイスでポートアクションを許可します。
[Inventory Management] > [Topology]	トポロジ：ネットワークデバイスとリンク接続を表示します。デバイスロールの管理、デバイスのタグ付け、表示のカスタマイズ、およびカスタムトポロジレイアウトの保存を行います。 注：[SD-Access Fabric] ウィンドウを表示するには、少なくとも**[Network Provision]** > **[Inventory Management]** > **[Topology]**に対する読み取りアクセス許可が必要です。

機能	説明
ライセンス	ソフトウェア資産やネットワーク資産のライセンス使用状況とコンプライアンスに関する情報を一元管理します。このロールは、cisco.com、シスコのクレデンシャル、デバイスの EULA、およびスマートアカウントの権限も管理します。
ネットワークテレメトリ	デバイスからのアプリケーションテレメトリの収集を有効または無効にします。サイトテレメトリレシーバ、ワイヤレスサービスアシュアランス、コントローラ証明書などの関連設定をデバイスに展開します。 注：アプリケーションテレメトリの収集を有効または無効にするには、[Provision] に対する書き込み権限が必要です。
PnP	新しいデバイスを自動的にオンボードしてサイトに割り当て、サイト固有のコンテキスト設定に基づいて設定します。
プロビジョニング	サイト固有の設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。このロールには、ファブリック、アプリケーションポリシー、アプリケーションの可視性、クラウド、サイト間 VPN、ネットワーク/アプリケーションテレメトリ、Stealthwatch、同期開始と実行設定、および Umbrella プロビジョニングが含まれます。 不正および aWIPS のメインダッシュボードでは、不正封じ込めなどの特定のアクションを有効または無効にできます。 デバイスをプロビジョニングするには、[Network Design] と [Network Provisioning] に対する書き込み権限が必要です。
ネットワーク サービス	基本的なネットワーク接続とアクセスの枠を超えたネットワークの追加機能を設定します。
アプリケーション ホスティング	ネットワークデバイスで実行される仮想化されたコンテナベースのアプリケーションを展開、管理、およびモニターします。
Bonjour	ポリシーベースのサービス検出を有効にするために、ネットワーク全体で Wide Area Bonjour サービスを有効にします。
Stealthwatch	暗号化されたトラフィックに含まれる脅威も検出して軽減できるようにするために、ネットワーク要素から Cisco Stealthwatch にデータを送信するように設定します。 Stealthwatch をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。 • **[Network Design]** > **[Network Settings]** • **[Network Provision]** > **[Provision]** • **[Network Services]** > **[Stealthwatch]** • **[Network Design]** > **[Advanced Settings]**

機能	説明
Umbrella	サイバーセキュリティの脅威に対する最前線の防御策として、ネットワーク要素で Cisco Umbrella を使用するように設定します。 Umbrella をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。 • **[Network Design]** > **[Network Settings]** • **[Network Provision]** > **[Provision]** • **[Network Provision]** > **[Scheduler]** • **[Network Services]** > **[Umbrella]** また、[Advanced Network Settings] に対する読み取り権限も必要です。
プラットフォーム	アクセス可能なインテントベースのワークフロー、データ交換、通知、統合の設定、およびサードパーティ製アプリケーションの統合に使用できるオープンなプラットフォーム。
API	Cisco DNA Center に REST API を使用してアクセスできます。
バンドル	生産性の向上のために、ITSM との統合用に事前設定されたバンドルを設定およびアクティブ化します。
イベント	ネットワークやシステムの関心があるイベントに登録することで、それらのイベントについての通知をほぼリアルタイムで受け取り、修正処置を開始できます。 電子メールおよび Syslog ログの設定は、**[System]** > **[Settings]** > **[Destinations]** で設定できます。
レポート	事前定義されたレポーティングテンプレートを使用して、ネットワークのあらゆる側面についてのレポートを生成できます。 不正デバイスおよび aWIPS のレポートを生成します。 ウェブフックは、**[System]** > **[Settings]** > **[Destinations]** で設定できます。
セキュリティ	ネットワークへのセキュアなアクセスを管理および制御します。
グループベース ポリシー	シスコのセキュリティグループタグに基づいてネットワークのセグメンテーションとアクセス制御を適用するグループベースポリシーを管理します。このロールには、エンドポイント分析が含まれます。
IP ベースのアクセス制御	IP アドレスに基づいてネットワークのセグメンテーションを適用する IP ベースのアクセス制御リストを管理します。
セキュリティ アドバイザリ	ネットワークをスキャンしてセキュリティアドバイザリを検索します。シスコが公開しているセキュリティアドバイザリでネットワークに影響する可能性がある情報を確認および把握できます。

機能	説明
システム	Cisco DNA Center の構成管理、ネットワーク接続、ソフトウェアアップグレードなどを一元管理します。
機械推論	セキュリティの脆弱性を迅速に特定して問題の自動分析を改善するために、機械推論ナレッジベースの自動更新を設定します。
システム管理	システムのコア機能と接続の設定を管理します。ユーザーロールを管理し、外部認証を設定します。 このロールには、整合性検証、HA、ディザスタリカバリ、デバッグログ、テレメトリコレクション、システムの EULA、IPAM、vManage サーバー、Cisco AI Analytics、バックアップと復元、およびデータプラットフォームが含まれます。
ユーティリティ	広く使用されているトラブルシューティング ツールやサービスなど、生産性に役立つ情報がまとめられています。
監査ログ	UI または API インターフェイスを通じてネットワークデバイスや Cisco DNA Center に加えられた変更の詳細なログ。
イベント ビューア	トラブルシューティングのためのネットワークデバイスおよびクライアントイベントの表示。
ネットワーク推論機能	ネットワーク分野の専門家の知識に基づく、ネットワークの問題についての自動化された論理的なトラブルシューティングを開始します。
リモートデバイスのサポート	シスコサポートチームが Cisco DNA Center によって管理されているネットワークデバイスをリモートでトラブルシューティングできるようにします。このロールを有効にすると、Cisco Technical Assistance Center（TAC）のエンジニアは、トラブルシューティングのためにお客様の Cisco DNA Center のセットアップにリモートで接続できます。
スケジューラ	他のバックエンドサービスと統合されたスケジューラを使用して、ポリシーの展開、プロビジョニング、ネットワークのアップグレードなどのタスクやアクティビティの実行、スケジュール、および監視が行えます。 不正封じ込めをスケジュールすることもできます。
検索	サイト、ネットワークデバイス、クライアント、アプリケーション、ポリシー、設定、タグ、メニュー項目など、Cisco DNA Center のさまざまなオブジェクトを検索します。

ロールベース アクセス コントロール統計の表示

各ユーザーロールに属しているユーザーの数を示す統計を表示できます。ドリルダウンして、選択したロールを持つユーザーのリストを表示することもできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Role Based Access Control]** の順に選択します。

デフォルトのすべてのユーザーロールとカスタムロールが表示されます。

ステップ 2 各ユーザーロールに対応する番号をクリックすると、そのロールを持つユーザーのリストが表示されます。

外部認証の設定

外部ユーザーの認証と許可に外部サーバーを使用している場合、Cisco DNA Center で外部認証を有効にする必要があります。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （1 ページ）を参照してください。
- 少なくとも 1 つの認証サーバーを設定する必要があります。

（注） 2.1.x 以前のリリースでは、外部認証が有効になっている場合、Cisco DNA Center は AAA サーバーに到達できないか、AAA サーバーが不明なユーザー名を拒否すると、ローカルユーザーにフォールバックしていました。現在のリリースでは、AAA サーバーに到達できない場合や AAA サーバーが不明なユーザー名を拒否した場合に Cisco DNA Center がローカルユーザーにフォールバックすることはありません。

外部認証フォールバックが有効になっている場合、外部ユーザーとローカル管理者は Cisco DNA Center にログインできます。

外部認証フォールバックを有効にするには、Cisco DNA Center インスタンスに SSH 接続し、次の CLI コマンドを入力します。

```
magctl rbac external_auth_fallback enable
```

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[External Authentication]** の順に選択します。

ステップ 2 Cisco DNA Center で外部認証を有効にするには、[Enable External User] チェックボックスをオンにします。

ステップ 3 （任意） AAA 属性を設定します。

TACACS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	TACACS
Empty	cisco-av-pair

Cisco DNA Center	TACACS
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

RADIUS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) 前の表で説明されているように、[AAA Attribute] フィールドに、ユースケースに適した属性を入力します。[AAA Attribute] フィールドのデフォルト値は Null です。
b) [更新（Update）] をクリックします。

ステップ 4 （任意） AAA サーバーを設定します。

これらの設定は、現在のプライマリ AAA サーバーとセカンダリ AAA サーバーを交換したり、異なる AAA サーバーを定義したりする場合にのみ行います。左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** の順に選択して **[Authentication and Policy Servers]** ウィンドウを開きます。

a) [Primary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。
b) [Secondary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。
c) （任意） Cisco ISE サーバーを使用している場合は、必要に応じて設定を更新できます。

Cisco ISE ポリシーの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Configure and Manage Policies」を参照してください。

表 *2 : Cisco ISE*サーバーの設定

名前	説明
Shared Secret	デバイスの認証キー。共有秘密の長さは、最大 100 文字です。 AAA アドレスを更新する前に、共有秘密を指定する必要があります。
Username	Cisco ISE CLI にログインするために使用する名前。
Password	Cisco ISE CLI ユーザー名のパスワード。
FQDN	Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。 *hostname.domainname.com* たとえば Cisco ISE サーバーの FQDN は、ise.cisco.com である可能性があります。

名前	説明
Subscriber Name	一意のテキスト文字列（acme など）。これは Cisco DNA Center から Cisco ISE への統合中に、Cisco ISE に新しい pxGrid クライアントを設定するために使用されます。
Virtual IP Address	Cisco ISE ポリシーサービスノード（PSN）が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

d) （任意） 詳細設定を更新するには、[View Advanced Settings] をクリックして、必要に応じて設定を更新します。

表 *3 : AAA* サーバー詳細設定

名前	説明
Protocol	TACACS または RADIUS。
Authentication Port	AAA サーバーへの認証メッセージのリレーに使用されるポート。 • RADIUS の場合、デフォルトは UDP ポート 1812 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Accounting Port	AAA サーバーへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。 • RADIUS の場合、デフォルトの UDP ポートは 1813 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Retries	Cisco DNA Center が Cisco ISE との接続を試行できる回数。
Timeout	Cisco DNA Center が Cisco ISE からの応答を待機する時間の長さ。タイムアウトの最大値は 60 秒です。

e) [更新（Update）] をクリックします。

二要素認証

二要素認証（2FA）は、ユーザー名とパスワードに加えて識別子手法を使用することで、ユーザー認証のセキュリティを強化するものです。識別子手法は、一般に、実際の対象ユーザーだけが所持し（スマホアプリやキーフォブなど）、元のログイン方法と意図的に異なるものを使用します。

Cisco DNA Center の二要素認証の実装では、トークンクライアント（適切な PIN が入力された後に使い捨てトークンコードを生成）、トークンサーバー（トークンコードを検証）、およびユーザーのアクセスを管理する認証サーバーを使用できます。認証処理には、RADIUS または TACACS+ プロトコルが使用されます。

二要素認証の前提条件

Cisco DNA Center で使用する二要素認証を設定するには、次の前提条件を満たしている必要があります。

- 認証された Cisco DNA Center ユーザーの RBAC ロール認可を伝達する属性値ペアを返すことができる認証サーバー。この例では、Cisco Identity Services Engine（Cisco ISE）2.3 パッチ 1 を使用しています。
- 認証サーバーと統合する二要素トークンサーバー。この例では、RSA Authentication Manager 7.2 を使用しています。
- ソフトウェアトークンを生成するクライアントのマシン上のトークン カード アプリケーション。この例では、RSA SecurID ソフトウェアトークンを使用しています。

二要素認証のワークフロー

以下に、二要素認証が設定されている Cisco DNA Center アプライアンスにユーザーがログインしたときの動作の概要を示します。

1. RSA SecurID トークンクライアントでは、ユーザーは PIN を入力してトークンコードを取得します。
2. Cisco DNA Center ログインページでは、ユーザー名とトークンコードを入力します。
3. Cisco DNA Center では、Cisco ISE へのログイン要求の送信に、RADIUS または TACACS+ プロトコルを使用します。
4. Cisco ISE RSA Authentication Manager サーバーに要求を送信します。
5. RSA Authentication Manager でトークンコードを検証し、ユーザーが正常に認証されたかどうかを Cisco ISE に通知します。
6. ユーザーが認証されている場合、Cisco ISE は認証されたユーザーと設定済みの認可プロファイルを照合し、**role=NETWORK-ADMIN-ROLE** 属性値ペアを返します。
7. Cisco DNA Center ユーザーのロールベース アクセス コントロール（RBAC）ロールに関連付けられている機能およびページへのアクセス権を付与します。

二要素認証の設定

Cisco DNA Center アプライアンスで二要素認証を設定するには、次の手順を実行します。

ステップ 1 RSA Authentication Manager を Cisco ISE と統合します。

a) RSA Authentication Manager で、2 つのユーザー、すなわち **cdnac_admin**（管理者ユーザーロール用）と **cdnac_observer**（オブザーバロール用）を作成します。

詳細については、RSA Self-Service Console Help の「Add a User to the Internal Database」のトピックを参照してください。このトピックにアクセスするには、次の手順を実行します。

1. *RSA Self-Service Console Help* を開きます。
2. [Search help] フィールドで、「**Add a User To the Internal Database**」と入力して、[Search help] をクリックします。

b) 新しい認証エージェントを作成します。

詳細については、*RSA Self-Service Console Help* の「Add an Authentication Agent」のトピックを参照してください。

c) 認証マネージャエージェント設定ファイル（sdconf.rec）を生成します。

1. RSA セキュリティコンソールで、**[Access]** > **[Authentication Agents]** > **[Generate Configuration File]** の順に選択します。

   [Configure Agent Timeout And Retries] タブが開きます。
2. [Maximum Retries] と [Maximum Time Between Each Retry] フィールドについては、デフォルト値を使用します。
3. [Generate Configuration File] をクリックします。

   [Download Configuration File] タブが開きます。
4. [Download Now] リンクをクリックします。
5. 画面に指示が表示されたら、[Save to Disk] をクリックして、zip ファイルのローカルコピーを保存します。
6. ファイルを解凍し、このバージョンの sdconf.rec ファイルを使用して、エージェントに現在インストールされているバージョンを上書きします。

d) 手順 1a で作成した **cdnac_admin** ユーザーと **cdnac_observer** ユーザーの PIN を生成します。

詳細については、*RSA Self-Service Console Help* の「Create My On-Demand Authentication PIN」のトピックを参照してください。

e) Cisco ISE を開始するには、**[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[RSA SecurID]** の順に選択して、[Add] を選択します。

f) [RSA SecurID Identity Sources] ページで、[Browse] をクリックし、ダウンロードした sdconf.rec ファイルを選択して、[Open] をクリックします。

g) [Reauthenticate on Change PIN] チェックボックスをオンにして、[Submit] をクリックします。

ステップ 2 2 つの許可プロファイルを作成します。1 つは Admin ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

a) Cisco ISE で、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

b) 両方のプロファイルについて、次の情報を入力します。

- [Name]：プロファイル名を入力します。
- [Access Type]：[ACCESS_ACCEPT] を選択します。
- [Advanced Attributes Settings] 領域：最初のドロップダウンリストから [Cisco:cisco-av-pair] を選択します。

  Admin ユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=NETWORK-ADMIN-ROLE] を選択します。

  オブザーバユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=OBSERVER-ROLE] を選択します。

ステップ 3 Cisco DNA Center アプライアンスの認証ポリシーを作成します。

『*Cisco Identity Services Engine Administrator Guide*』の「Configure Authentication Policies」のトピックを参照してください。

ステップ 4 2 つの許可ポリシーを作成します。1 つは Admin ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

『*Cisco Identity Services Engine Administrator Guide*』の「Configure Authorization Policies」のトピックを参照してください。

ステップ 5 RSA Authentication Manager セキュリティコンソールで、ソフトウェアトークンが両方のユーザーに割り当てられていることを確認します。

詳細については、*RSA Self-Service Console Help* の「View a Token」のトピックを参照してください。

（注） トークンを割り当てる必要がある場合は、「Assign a Software Token to a User」のトピックで説明されている手順を実行します。

RADIUS を使用した二要素認証の有効化

RADIUS 用に設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE と Cisco DNA Center を連動させます。

『*Cisco DNA Center Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

ステップ 2 認証に Cisco ISE サーバーを使用するよう Cisco DNA Center を設定します。

「外部認証の設定」を参照してください。

重要 Cisco ISE と Cisco DNA Center の両方に同じ共有秘密を指定していることを確認します。

TACACS+ を使用した二要素認証の有効化

TACACS+ が設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE で、**[Administration]** > **[Network Resources]** > **[Network Devices]** の順に選択すると、[Network Devices] ウィンドウが開きます。

ステップ 2 [TACACS Authentication Settings] をクリックして、その内容を表示します。以前に追加した Cisco DNA Center デバイスに対して共有秘密がすでに設定されていることを確認します。

ステップ 3 **[Work Centers]** > **[Device Administration]** > **[Policy Elements]** を選択すると、[TACACS Profiles] ウィンドウが開きます。

ステップ 4 cdnac_admin および cdnac_observer ユーザーロールの TACACS+ プロファイルを作成します。

a) [Add] をクリックします。

b) 次のタスクを実行します。

- プロファイル名を入力します。
- [Raw View] タブをクリックした後、[Profile Attributes] テキストボックスに次のテキストを入力します。
  - cdnac_admin ユーザーロールの場合は、**`Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`** と入力します。
  - cdnac_observer ユーザーロールの場合は、**`Cisco-AVPair=ROLE=OBSERVER-ROLE`** と入力します。

c) **[保存（Save）]** をクリックします。

ステップ 5 Cisco ISE と Cisco DNA Center を連動させます。

『*Cisco DNA Center Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

ステップ 6 認証に Cisco ISE サーバーを使用するよう Cisco DNA Center を設定します。

「外部認証の設定」を参照してください。

重要 Cisco ISE と Cisco DNA Center の両方に同じ共有秘密を指定していることを確認します。

二要素認証を使用したログイン

二要素認証を使用して Cisco DNA Center にログインするには、次の手順を実行します。

ステップ 1 Cisco DNA Center のログインページで、適切なユーザー名を入力します。

ステップ 2 RSA SecurID トークンクライアントを開き、以前設定した PIN を入力して使い捨てトークンを生成します。

ステップ 3 このトークンをコピーして、Cisco DNA Center のログインページの [Password] フィールドに貼り付けます。

ステップ 4 [Log In] をクリックします。

外部ユーザーの表示

RADIUS/TACACS を使用して初めてログインした外部ユーザーのリストを表示できます。表示される情報には、ユーザー名とロールが含まれます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[External Authentication]** の順に選択します。

ステップ 2 ウィンドウの下部までスクロールします。[External Users] 領域に外部ユーザーのリストが表示されます。

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。