Cisco Nexus Dashboard 管理タスク、リリース 3.1.x

目次

Nexus DashboardのGUIにログインするユーザーの認証方法を選択できます。今回のリリースでは、ローカル認証に加えて、LDAP、RADIUS、およびTACACSリモート認証サーバーもサポートしています。ユーザーのロールと権限についてはこのセクションで、リモート認証の設定については「リモート認証」で、ローカルユーザーの設定については「ユーザー」で説明します。

ロールとアクセス許可

Cisco Nexus Dashboardでは、ロールベース アクセス コントロール(RBAC)で定義されているロールに応じて、ユーザーはアクセスが許可されます。ロールはローカル認証と外部認証の両方で使用され、Nexus Dashboardやそこで実行されているサービスに適用されます。すべてのロールに、読み取り専用または書き込み権限を割り当てることができます。読み取り専用アクセスではユーザーはオブジェクトと設定を表示でき、書き込みアクセスではユーザーは変更を加えることができます。

次のセクションに、Nexus Dashboardで使用可能なユーザーロールとプラットフォーム内で関連付けられている権限、および個々のサービスを示します。

リモート認証サーバーで同じロールを設定し、そのサーバーを使用してNexus Dashboardユーザーを認証できます。リモート認証の詳細については、「リモート認証」セクションを参照してください。

Nexus Dashboard Insights および Orchestrator のロール

ユーザロール	NDプラットフォーム	オーケストレータサービス
管理者	すべての設定、機能、タスクへのフルアクセスが許可されます。 サービスの追加と削除を実行できる唯一のロールです。	フルアクセス。
承認者	Dashboard ロールと同じです。	|テンプレート設定の承認または拒否を実行できます。テンプレートの編集や展開は実行できません。
Dashboard ユーザー	ダッシュボードビューへのアクセスとアプリケーションの起動を実行できますが、Nexus Dashboardの設定は変更できません。	アクセス権なし。
展開担当者	Dashboard ロールと同じです。	テンプレートをサイトに展開できますが、テンプレートの編集や承認は実行できません。
ポリシー マネージャ	Dashboard ロールと同じです。	アクセス権なし。
サイト管理者	サイトのオンボーディングと構成に関連する設定にアクセスできます。	managed と unmanaged の間でサイトステータス、ファブリック リソース テンプレート、ファブリック ポリシー テンプレート、およびモニタリング テンプレート（アクセス SPAN）を変更できるようにします。

ユーザロール	NDプラットフォーム	オーケストレータサービス
サイト マネージャ	サイトへのポリシーの展開へのアクセスを許可します。	ポリシー、スキーマ、およびモニタリング テンプレート（テナント SPAN）の構成を許可します。
テナントマネージャ	Dashboard ロールと同じです。	ポリシー、スキーマ、およびモニタリング テンプレート（テナント SPAN）の構成を許可します。
ユーザーマネージャ	ユーザーの作成、権限の変更、リモート認証プロバイダーの追加などのユーザー設定にアクセスできます。	アクセス権なし。

上記の各ロールは、一連の権限に関連付けられています。これらの権限は、関連する要素を表示し、関連しない要素をユーザーのビューから非表示にするために使用されます。

Nexus Dashboard Insights

Insights サービスは RBAC をサポートしておらず、Nexus ダッシュボードにログインできるアカウントはすべて、Insights に完全にアクセスできます。

Nexus Dashboard Fabricファブリック コントローラ ロール

ユーザロール	**Nexus Dashboard** ファブリック コントローラ
NDFC アクセス管理者	NDFC の インターフェイス マネージャ画面で、ネットワーク インターフェイスに関連する操作を実行できます。 アクセス管理者は、次のアクションを実行できます。 ・レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。 ・ホスト vPC、およびイーサネット インターフェイスを編集します。 ・管理インターフェイスからの保存、プレビュー、および展開。 ・LAN クラシックのインターフェイス、およびポリシーに関連付けられていない場合は外部ファブリックを編集します。nve、管理、トンネル、サブインターフェイス、SVI、インターフェイスグループ化、およびループバック インターフェイスを除く ただし、アクセス管理者は次のアクションを実行できません。 ・レイヤ 3 ポートチャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。 ・レイヤ 3、ST FEX、AA FEX のメンバーインターフェイスおよびポートチャネルは編集できません。 ・アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。 ・ポートチャネルのようなピアは編集できません。 ・管理インターフェイスを編集できません。 ・トンネルを編集できません。
|NDFC デバイス アップグレード管理者	NDFC のイメージ管理画面でデバイスのアップグレードに関連する操作を実行できます。 **[**イメージ管理（**Image Management**）**]** 画面。
NDFC ネットワーク管理者	完全な管理アクセスを許可します。

ユーザロール	**Nexus Dashboard** ファブリック コントローラ
NDFC ネットワークオペレータ	次の NDFC メニューへの読み取り専用アクセスを許可します。 ・ダッシュボード ・トポロジ ・モニタ（Monitor） ・アプリケーション ネットワークオペレータのユーザーは、以下を表示できます。 ・ファブリックビルダー ・ファブリックの設定 ・設定のプレビュー ・ポリシー ・テンプレート （Templates） ただし、ネットワークオペレータは次の操作を実行できません。 ・ファブリック内のスイッチの予期される構成を変更できません。 ・スイッチに構成を展開できません。 ・ライセンス、追加ユーザーの作成などの管理オプションにアクセスできません。

ユーザロール	**Nexus Dashboard** ファブリック コントローラ
NDFC ネットワークステージャ	構成の変更を行うことができますが、ネットワーク管理者ユーザーがその変更を後で展開する必要があります。 ネットワークステージャのユーザーは、次のアクションを実行できます。 ・インターフェイス構成の編集 ・ポリシーの表示または編集 ・インターフェイスの作成 ・ファブリック設定の変更 ・テンプレートの編集または作成 ただし、ネットワークステージャは次のアクションを実行できません。 ・スイッチに設定を展開できません。 ・DCNM Web UI または REST API から展開関連のアクションを実行できません。 ・ライセンス、追加ユーザーの作成などの管理オプションにアクセスできません。 ・スイッチをメンテナンスモードに入れるか解除するかの切り替えはできません。 ・ファブリックを展開フリーズモードに入れるか解除するかの切り替えはできません。 ・パッチをインストールできません。 ・スイッチをアップグレードできません。 ・ファブリックを作成または削除できません。 ・スイッチをインポートまたは削除できません。  ネットワーク ステージャ は、 既存の ファブリックを使用できますが、これらの構成を展開することはできません 。ネットワーク管理者は、ネットワークステージャー ロールを持つユーザーによってステージングされた変更と編集を展開できます。

デフォルト認証ドメインの選択

デフォルトでは、ログイン画面でのユーザー認証でローカル ドメインが選択されます。ドロップダウン メニューから使用可能なログインドメインのいずれかを選択して、ログイン時にドメインを手動で変更できます。

または、次のように、最も一般的に使用される別のデフォルトログインドメインを設定できます。

デフォルトドメインとして設定できるのは、既存のドメインに限られます。リモート認証ドメインの追加については、「リモート認証」を参照してください。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. デフォルトのログインドメインを選択します。
   a. メイン ナビゲーション メニューから、**[管理] > [認証]（Administrative > Authentication）** の順に選択します。
   b. **[デフォルト認証（Default Authentication）]** タイルの右上にある

      [編集（Edit）] アイコンをクリックします。**[デフォルト認証**

      （Default Authentication）] ウィンドウが開きます。
3. **[デフォルト認証（Default Authentication）]** が開いたら、ドロップダウンから **[ログインドメイン（Login Domain）]** を選択します。

リモート認証

Cisco Nexus Dashboardは、LDAP、TACACS、Radiusなどの多数のリモート認証プロバイダーをサポートしています。

外部認証サーバーを設定する場合は、次のことに注意してください。

- リモート認証サーバーの各ユーザーごとに設定を行う必要があります。
- すべてのLDAP設定は、大文字と小文字が区別されます。

  たとえば、LDAP サーバーに OU=Cisco Users、Nexus Dashboard に OU=cisco users がある場合、認証は機能しません。

- LDAP 設定のベストプラクティスは、属性文字列として CiscoAVPair を使用することです。何らかの理由でオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用できない場合は、追加のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 を LDAP サーバーで使用することもできます。

  または、各ユーザーのCisco AVPair値を設定する代わりに、Nexus DashboardでLDAPグループマップを作成できます。

- Nexus Dashboard、サイト、およびアプリケーション間のシングルサインオン(SSO)は、リモートユーザーのみが使用できます。
- SSOを使用してNexus Dashboardの[サイト]ページからAPICサイトにクロス起動する場合、Nexus Dashboardユーザーに対して定義されたAVペアは、APIC へのログイン時にも使用されます。

  たとえば、Nexus Dashboard クラスタの 管理者 として定義されたユーザーは、APICでの 管理者 権限も付与されます。

リモート認証サーバーの設定

Nexus Dashboardユーザーのリモート認証サーバーを設定する際、ユーザー名とそのユーザーに割り当てられたロールを指定して、カスタム属性値(AV)のペアを追加する必要があります。

ユーザーロールとその権限は、「ロールと権限」で説明されているように、Nexus Dashboard GUIで直接設定するローカルユーザーと同じです。

次の表に、Nexus Dashboardのユーザーロールと、LDAPなどのリモート認証サーバーでロールを定義するために使用するAVペアを示します。

表 1. Nexus Dashboard AVペア

ユーザロール	**AV**ペア値
管理者	admin
Approver	approver
ダッシュボードユーザー	app-user
展開担当者	deployer
ポリシー マネージャ	config-manager
サイト管理者	site-admin

ユーザロール	AVペア値
サイト マネージャ	site-policy
テナントマネージャ	tenant-policy
ユーザーマネージャ	aaa

表 2. Nexus Dashboard Fabric Controller AVペア

ユーザロール	AVペア値
NDFC アクセス管理者	access-admin
NDFC デバイスアップグレード管理者	device-upg-admin
NDFC ネットワーク管理者	ネットワーク管理者
NDFC ネットワークオペレータ	network-operator
NDFC ネットワークステージャ	network-stager

AV ペアの文字列形式は、特定のユーザに読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかで異なります。通常の文字列にはドメインが含まれており、その後にスラッシュ（/）で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ（|）文字で区切られています。

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

たとえば次の文字列を使用すると、テナント マネージャロールとポリシー マネージャロールがユーザーに割り当てられると同時に、ユーザーマネージャユーザーに表示されるオブジェクトを参照できます。

```
shell:domains=all/tenant-policy|site-policy/aaa
```

読み取り専用権限のみ、または読み取り/書き込み権限のみをユーザーに設定する場合にも、スラッシュ（/）を含める必要があります。次の例は、サイト管理者ロールで使用可能なオブジェクトへの読み取り/書き込みアクセス権または読み取り専用アクセス権のみを設定する方法を示しています。

- 読み取り専用：shell:domains=all//site-admin
- 読み取り/書き込み：shell:domains=all/site-admin/

リモート認証プロバイダーとしての LDAP の追加

はじめる前に

- 「リモート認証サーバーの設定」の説明に従って、LDAP サーバーに 1 人以上のユーザーを設定しておく必要があります。

  LDAP設定のエンドツーエンドの検証には、既存のユーザーを使用する必要があります。

LDAPリモート認証プロバイダーを追加するには、次の手順を実行します。

1. Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。
2. 認証ドメインを追加します。
   a. メイン ナビゲーション メニューから、[管理] > [認証]（**Administrative > Authentication**） の順に選択します。
   b. メイン ペインの右上で、[アクション（**Actions**）] メニューをクリックし、[ログイン ドメインの作成（**Create Login Domain**）] を選択します。
3. [ログインドメインの作成（**Create Login Domain**）] 画面が開いたら、ドメインの詳細を入力します。
   a. [名前（**Name**）] にドメインの名前を入力します。
   b. （任意）[説明（**Description**）] にドメインの説明を入力します。
   c. [レルム（**Realm**）] ドロップダウンから [Ldap] を選択します。
   d. 次に、[+プロバイダーの追加（**+Add Provider**）] をクリックして、

      リモート認証サーバーを追加します。[プロバイダーの追加（**Add**

      Provider）] ウィンドウが開きます。

4. リモート認証サーバーの詳細を入力します。
   a. サーバーのホスト名を [ホスト名（**Hostname**）] に入力するか、サーバーの [IPアドレス（**IP Address**）] に入力します。
   b. （オプション）サーバーの説明を [説明（**Description**）] に入力します。
   c. [ポート（**Port**）] 番号を入力します。

      LDAP のデフォルトのポートは 389 です。

   d. ベース DN を [ベース**DN**（**Base DN**）] に、バインド DN を [バインド **DN**（**Bind DN**）] に入力します。

      ベースDNとバインドDNは、LDAPサーバーがどのように設定されているかによって異なります。LDAPサーバーで作成されたユーザーの識別名から、ベースDNとバインドDNの値を取得できます。

      ベースDNは、サーバーがユーザーを検索するポイントです。例：DC=nd,DC=local。

      バインド DN は、サーバに対する認証に使用されるログイン情報です。例：CN=admin、CN=Users、DC=nd、DC=local。

   e. キーを [キー（**Key**）] に入力して確認します。

      これは、バインドDNユーザーのパスワードです。匿名バインドはサポートされていないため、フィールドに有効な値を入力する必要があります。

   f. 認証サーバーに接続する際のタイムアウトを [タイムアウト（**Timeout**）] に、再試行回数を [試行回数（**Retries**）] に指定します。
   g. [**LDAP**属性（**LDAP Attribute**）] フィールドに入力して、グループメンバーシッ

      プとロールを指定します。次の2つのオプションがサポートされています。

      - ciscoAVPair（デフォルト）：ユーザー ロールの Cisco AVPair 属性で設定した LDAP サーバーに使用されます。
      - memberOf：LDAP グループマップで設定した LDAP サーバーに使用されます。グループマッ

プの追加については、次の手順で説明します。

h. （任意）LDAP 通信の場合は **[SSL]** を有効にします。
SSL を有効にする場合は、**[SSL** 証明書（**SSL Certificate**）**]** と **[SSL** 証明書検証 タイプ（SSL Certificate Validation）] も指定する必要があります。

- [許可（Permissive）]：任意の認証局（CA）によって署名された証明書を受け入れ、暗号化に使用します。
- [厳格（Strict）]：使用する前に証明書チェーン全体を確認します。

i. （任意）**[**サーバーのモニタリング（**Server Monitoring**）**]** を有効にします。

モニタリングを有効にする場合は、[ユーザー名（Username）] と [パスワード（Password）] も指定する必要があります。

j. **[**検証（**Validation**）**]** フィールドに、追加する LDAP サーバーですでに設定されているユーザーの **[**ユーザー名（**Username**）**]**と **[**パスワード（**Password**）**]** を入力します。

Nexus Dashboardはこのユーザー情報に基づいてエンドツーエンドの認証を検証し、入力した設定が妥当であるかを確認します。

k. **[**保存（**Save**）**]** をクリックしてプロバイダー設定を完了します。

l. このドメインで使用するLDAP認証サーバーが他にもあれば、この手順を繰り返します。

5. （任意）**[LDAP**グループマップルール（**LDAP Group Map Rules**）**]** を有効にして設定します。

Cisco AVペア文字列を使用してLDAPユーザーを認証する場合は、この手順をスキップしてください。

a. **[LDAP**認証の選択（**LDAP Auth Choice**）**]** で、[LDAPグループマップルール（LDAP Group Map Rules）] を選択します。

b. **[LDAP** グループ マップ ルールの追加（**Add LDAP Group Map Rule**）**]** をクリックします。

[LDAPグループマップルールの追加（**Add LDAP Group Map Rule**）**]** ウィンドウが開きます。

c. グループの **[**グループ**DN**（**Group DN**）**]** を指定します。

d. LDAP グループの **[**ロール（**Roles**）**]** を 1 つ以上選択します。

e. **[**保存（**Save**）**]** をクリックしてグループ設定を保存します。

f. 追加のLDAPグループがあれば、この手順を繰り返します。

6. **[**作成（**Create**）**]** をクリックして、ドメインの追加を終了します。

リモート認証プロバイダーとしての **RADIUS** または **TACACS** の追加

はじめる前に

- 「リモート認証サーバーの設定」の説明に従って、リモート認証サーバーに 1 人以上のユーザーを設定しておく必要があります。

プロバイダー構成の設定のエンドツーエンドの検証には、既存のユーザーを使用する必要があります。

RadiusまたはTACACSリモート認証プロバイダーを追加するには、次の手順を実行します。

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。

2. 認証ドメインを追加します。
   a. メイン ナビゲーション メニューから、**[管理] > [認証]**（**Administrative > Authentication**） の順に選択します。
   b. メイン ペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[ログイン ドメインの作成（Create Login Domain）]** を選択します。
3. **[ログインドメインの作成（Create Login Domain）]** 画面が開いたら、ドメインの詳細を入力します。
   a. **[名前（Name）]** にドメインの名前を入力します。
   b. （任意）**[説明（Description）]** にドメインの説明を入力します。
   c. **[レルム（Realm）]** ドロップダウンから [Radius] または [Tacacs] を選択します。
   d. 次に、**[+プロバイダーの追加（+Add Provider）]** をクリックして、

      リモート認証サーバーを追加します。**[プロバイダーの追加（Add**

      Provider）] ウィンドウが開きます。

4. リモート認証サーバーの詳細を入力します。
   a. サーバーのホスト名を入力するか、IP アドレスを入力します。
   b. （オプション）サーバーの説明を **[説明（Description）]** に入力します。
   c. サーバーが使用する認証プロトコルを選択します。

      [PAP]、[CHAP]、または [MS-CHAP] から選択しま

      す。

   d. ポート番号を入力します。

      デフォルトのポートは RADIUS に対して 1812、TACACS に対して 49 です。

   e. キーを **[キー（Key）]** に入力して確認します。

      これはプロバイダーサーバーへの接続で使用するパスワードです。

   f. （任意）**[サーバーのモニタリング（Server Monitoring）]** を有効にするかを選択します。

      モニタリングを有効にする場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** も指定する必要があります。

   g. **[検証（Validation）]** フィールドに、追加するリモートサーバーですでに設定されているユーザーの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。

      Nexus Dashboardはこのユーザー情報に基づいてエンドツーエンドの認証を検証し、入力した設定が妥当であるかを確認します。

   h. **[保存（Save）]** をクリックしてプロバイダー設定を完了します。
   i. 追加のリモート認証サーバーがあれば、この手順を繰り返します。
5. **[作成（Create）]** をクリックして、ドメインの追加を終了します。

リモートユーザーログインの検証

Nexus Dashboard では、特定のユーザーのクレデンシャルを使用してログインを試行することで、リモー

ト認証プロバイダーの到達可能性を検証できます。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. テストするドメインに移動します。
   a. メイン ナビゲーション メニューから、**[管理] > [認証]（Administrative > Authentication）** の順に選択します。
   b. 特定のドメインをクリックします。
   c. 右側のプロパティサイドバーで、詳細アイコンをクリックします。ドメインの **[概要（Overview）]** ページが開きます。
3. **[概要（Overview）]** ページで、テストするプロバイダーの横にある **[検証（Validate）]** をクリックします。
4. **[プロバイダーの検証（Validate Provider）]** ウィンドウで、この認証プロバイダーで定義されているユーザーの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力し、**[検証（Validate）]** をクリックします。

   認証が成功したかどうかを示すメッセージが表示されます。

   認証失敗メッセージが表示された場合は、認証プロバイダーのサーバーに到達可能であること、およびテストに使用したユーザーのクレデンシャルが有効になっており、プロバイダーで設定されていることを確認してください。

リモート認証ドメインの編集

作成したドメインに変更を加える場合は、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理] > [認証]（Administrative > Authentication）** の順に選択します。
3. ドメインの **[アクション（Actions）]** メニューから、**[ログイン ドメインの編集（Edit Login Domain）]** を選択します。

   認証ドメインの名前とタイプは変更できませんが、説明とプロバイダー設定は変更できます。

   単に説明を更新するなど、ログインドメインに変更を加えた場合は、既存のすべてのプロバイダーに対してキーを再入力する必要があります。

リモート認証ドメインの削除

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理] > [認証]（Administrative > Authentication）** の順に選択します。
3. ドメインの **[アクション（Actions）]** メニューから、**[ログイン ドメインの削除（Delete Login Domain）]** を選択します。
4. **[削除の確認（Confirm Delete）]** プロンプトで、**[OK]** をクリックして確定します。

多要素認証

リリース2.1.2以降、ユーザーログインに多要素認証(MFA)を使用するようにNexus Dashboardを設定できます。

多要素認証を設定する場合、次を実行します。

- 「MFA プロバイダーとしての Okta アカウントの構成」で説明されているように、MFA プロバイダーの各ユーザーを構成します。

  このリリースでは、MFAプロバイダーとしてOktaのみがサポートされています。

- 「MFA クライアントの構成」で説明されているように、MFA プロバイダーとクライアントの統合

  を確立します。このリリースでは、MFAクライアントとしてDuoのみがサポートされています。

- 「Okta をリモート認証プロバイダーとして追加する」で説明されているように、MFA プロバイダーを Nexus Dashboard の外部認証ドメインとして追加します。

MFA プロバイダーとしての Okta アカウントの構成

次の手順では、Oktaをプロバイダーとして使用してNexus DashboardのMFAを有効にするために必要な基本設定を示します。詳細なOkta設定は、このドキュメントの範囲外です。使用可能なすべてのオプションについては、Oktaのドキュメントを参照してください。

Nexus Dashboard MFA用にOktaを設定するには、次を実行します。

1. Oktaアカウントにログインします。

   アカウントを作成するには、https://developer.okta.com にアクセスします。

2. 新しいアプリ統合を作成します。
   a. 左側のナビゲーションメニューから、**[**アプリケーション **>** アプリケーション（**Application > Application**）**]** を選択します。
   b. **[**アプリケーション統合の作成（**Create App Integration**）**]** をクリックします。
   c. **[**サインイン方法（**Sign-in method**）**]** は、[OIDC - OpenID接続（OIDC - OpenID Connect）] を選択します。
   d. **[**アプリケーション タイプ（**Application Type**）**]** は、[Webアプリケーション（Web Application）] を選択します。
   e. **[**次へ（**Next**）**]** をクリックします。
   f. **[**アプリケーション統合名（**App integration name**）**]** を指定します。たとえば nd-mfa です。

      次の手順では、アプリ統合名として nd-mfa を使用していることを前提としています。別の名前を選択する場合は、必要に応じて nd-mfa を置き換えます。

   g. **[**サインインリダイレクト**URI**（**Sign-in redirect URIs**）**]** には、https://<nd-node1-ip>/oidccallback を入力します。

      <nd-node1-ip> はクラスタ ノードの IPアドレスに置き換え、**[+URI** を追加（**Add URI**）**]** をクリックして、クラスタのすべてのノードの URI を指定します。

h. **[制御されたアクセス（Controlled Access）]** で、[今はグループの割り当てをスキップ（Skip group assignment for now）] を選択します。

i. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。

3. 必要な属性をデフォルトユーザーに追加します。

a. 左側のナビゲーションメニューから、**[ディレクトリ > プロファイル エディタ（Directory > Profile Editor）]** を選択します。

b. **[Okta ユーザー（デフォルト）]** のプロファイルをクリックします。

c. **[+属性の追加（+Add Attribute）]** をクリックします。

d. **[データ型（Data type）]** では、文字列（string）を選択します。

e. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、CiscoAVPair と入力します。

f. **[属性が必要（Attribute required）]** がオフ（unchecked）になっていることを確認します。

g. 他のフィールドはデフォルト値のままにして、**[保存してさらに追加（Save and Add Another）]** をクリックします。

h. **[データ型（Data type）]** では、文字列（string）を選択します。

i. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、nduser と入力します。

j. **[属性が必要（Attribute required）]** がオフ（unchecked）になっていることを確認します。

k. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。

4. 作成した nd-mfa ユーザーに必要な属性を追加します。

a. 左側のナビゲーション メニューから、**[ディレクトリ > プロファイル エディタ（Directory > Profile Editor）]** を選択します。

b. **nd-mfa ユーザー（デフォルト）** のプロファイルをクリックします。

c. **[+属性の追加（+Add Attribute）]** をクリックします。

d. **[データ型（Data type）]** では、文字列（string）を選択します。

e. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、CiscoAVPair と入力します。

f. **[属性が必要（Attribute required）]** がオンになっていることを確認します。

g. 他のフィールドはデフォルト値のままにして、**[保存してさらに追加（Save and Add Another）]** をクリックします。

h. **[データ型（Data type）]** では、文字列（string）を選択します。

i. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、nduser と入力します。

j. **[属性が必要（Attribute required）]** がオンになっていることを確認します。

k. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。

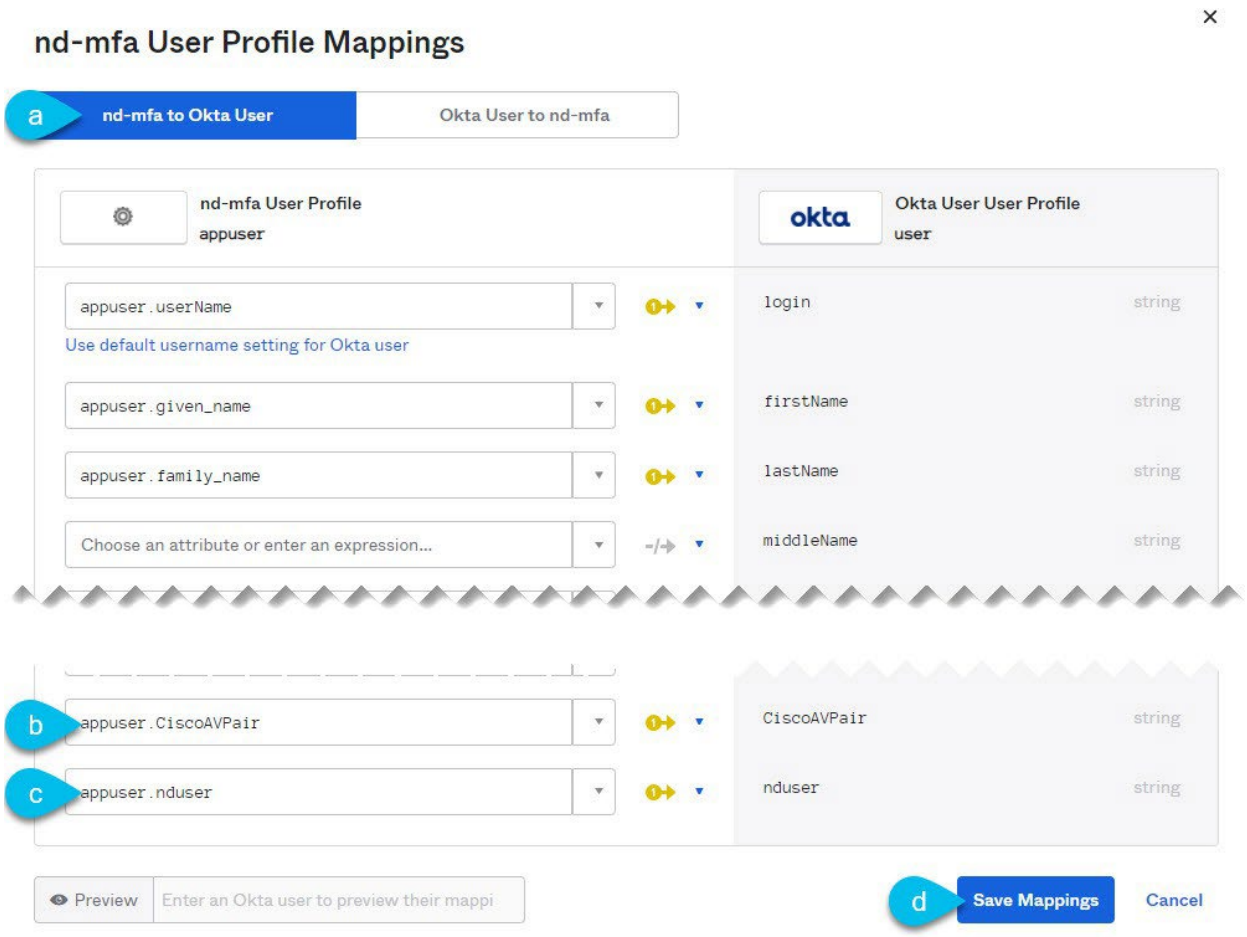
5. 属性をマッピングします。

a. 左側のナビゲーション メニューから、**[ディレクトリ > プロファイル エディタ（Directory > Profile Editor）]** を選択します。

b. **nd-mfa ユーザー（nd-mfa User）** のプロファイルをクリックします。

c. メイン ウィンドウの [属性（Attributes）] 領域で、[マッピン

グ（Mappings）] をクリックします。**[nd-mfa**ユーザー プロファイル マッピング（**nd-mfa User Profile Mappings**）] ウィンドウが開きます。



d. **[nd-mfaユーザー プロファイル マッピング（nd-mfa User Profile Mappings）]** ウィンドウの上部で、**[nd-mfa を Okta ユーザーに]** をクリックします。

e. [CiscoAVPair] の横にあるドロップダウンメニューから app.CiscoAVPair を選択します。

f. [nduser] の横にあるドロップダウンメニューから app.nduser を選択します。

g. **[マッピングの保存（Save Mappings）]** をクリックします。

h. **[今すぐ更新を適用（Apply Update now）]**をクリックします。

6. ユーザを作成します。

a. 左側のナビゲーションメニューから、**[ディレクトリ > ユーザー（Directory > People）]** を選択します。

b. **[+ユーザーの追加（+Add person）]** をクリックします。

c. ユーザー情報を入力します。

d. **[保存してさらに追加（Save and Add Another）]** をクリックして別のユーザーを追加するか、**[保存（Save）]** をクリックして終了します。

Nexus Dashboarにログインできるようにするすべてのユーザーを追加する必要があります。

7. ユーザーをアプリに割り当てます。

a. 左側のナビゲーションメニューから、**[アプリケーション > アプリケーション（Applications > Application）]** を選択します。

b. 作成したアプリケーション（nd-mfa）をクリックします。

c. **[課題（Assignments）]** タブを選択します。

d. **[割り当て > ユーザーに割り当て（Assign > Assign to People）]** を選択します。

[ユーザーへのnd-mfaの割り当て（**Assign nd-mfa to People**）] ウィンドウが開きます。

e. **[ユーザーへのnd-mfaの割り当て]** ウィンドウで、ユーザーの横にある **[割り当て（Assign）]** をクリックし、ユーザーが Nexus Dashboard にログインできるようにします。

f. ユーザーの詳細ウィンドウが開いたら、**[CiscoAVPair]** および **[nduser]** フィールドに値を入力します。

CiscoAVPair の値は、「Configuring Remote Authentication Server（リモート認証サーバーの構成）」で説明されています（例：shell:domains=all/admin/）。

nduser の値は、Nexus Dashboard にログインするときにこのユーザーのユーザー名として使用されます。

g. **[保存して戻る（Save and Go Back）]** をクリックします。

h. 別のユーザーを割り当てるか、**[完了（Done）]** をクリックして終了します。

前の手順で作成したすべてのユーザーを追加する必要があります。

8. アプリの **[要求（Claims）]** を設定します。

a. 左のナビゲーションメニューから **[セキュリティ > API（Security > API）]** を選択します。

b. デフォルトの名前をクリックします。

c. **[要求（Claims）]** タブを選択します。

d. **[+要求の追加（+Add Claim）]** をクリックして、CiscoAVPair 要求を追加します。

e. **[名前（Name）]** フィールドに、CiscoAVPair と入力します。

f. **[トークン タイプに含める（Include in token type）]** ドロップダウンから、[IDトークン（ID Token）] を選択します。

[IDトークン（ID Token）] の使用をお勧めしますが、[アクセス トークン（Access Token）] もサポートされています。

g. **[値（Value）]** フィールドに、appuser.CiscoAVPair と入力します。

h. **[保存（Save）]** をクリックします。

i. **[+要求の追加（+Add Claim）]** をクリックして、nduser の要求を追加します。

j. **[名前（Name）]** フィールドに、nduser と入力します。

k. **[トークン タイプに含める（Include in token type）]** ドロップダウンから、[IDトークン（ID Token）] を選択します。

両方の要求を同じトークンで作成する必要があります。ID トークンとアクセス トークンの混在はサポートされていません。

l. **[値（Value）]** フィールドに、appuser.nduser と入力します。

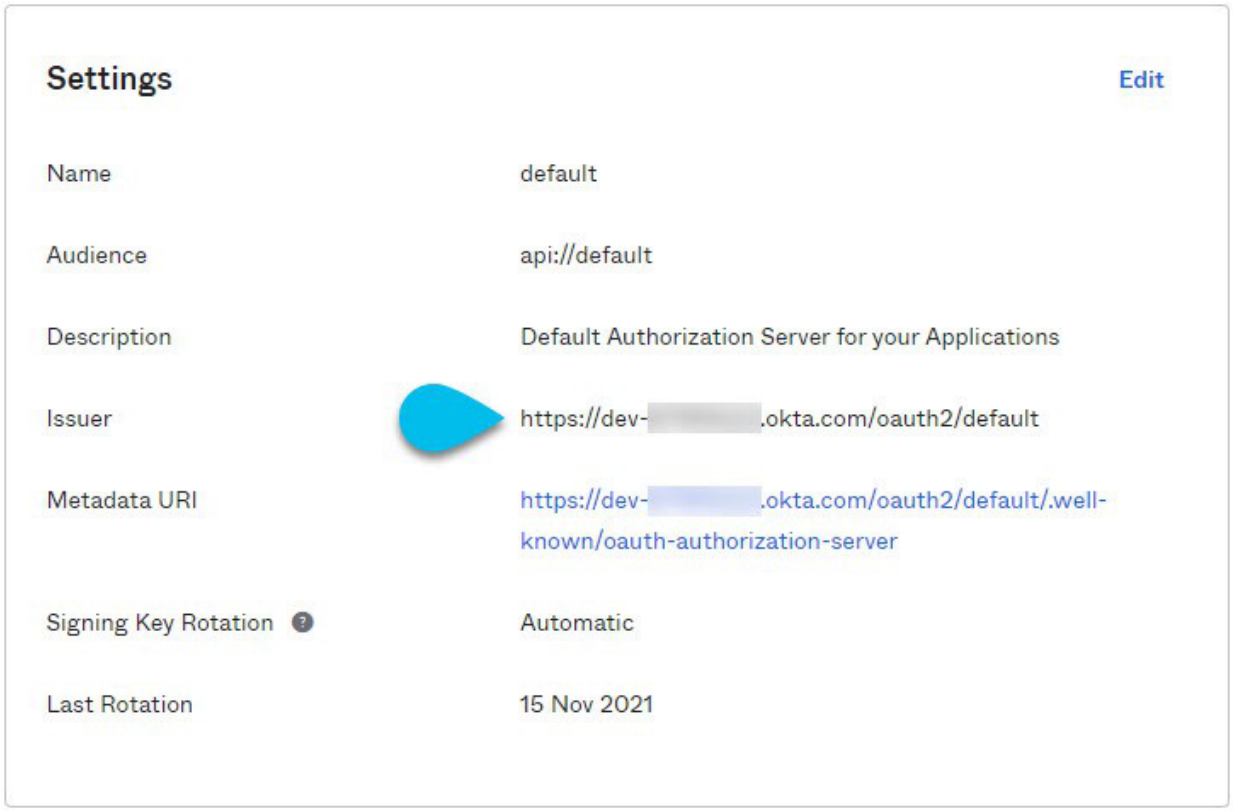
m. **[保存（Save）]** をクリックします。

9. Nexus ダッシュボードの認証プロバイダーとして追加するために必要な Okta アカウント情報を収集します。

a. 左のナビゲーションメニューから **[セキュリティ > API（Security > API）]** を選択します。

b. デフォルトの名前をクリックします。

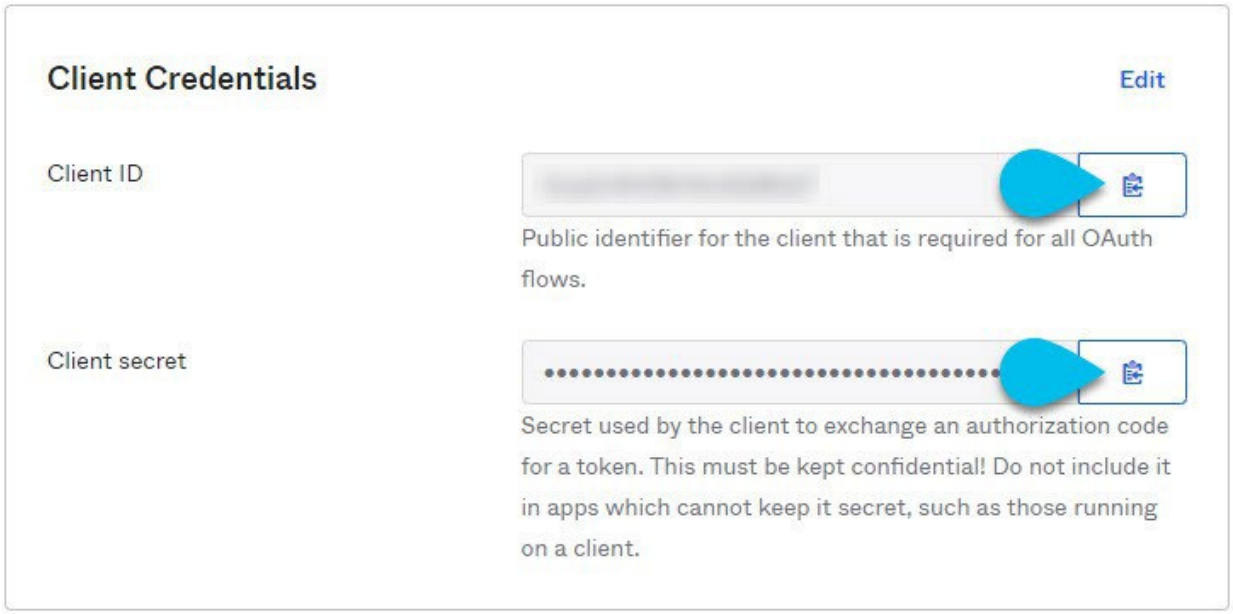
c. **[発行者（Issuer）]** の値を書き留めます。



d. 左側のナビゲーションメニューから、[アプリケーション > アプリケーション（**Application > Application**）] を選択します。

e. 作成したアプリケーション（nd-mfa）をクリックします。

f. [クライアント ID（**Client ID**）] と [クライアント シークレット（**Client Secret**）] の値を書き留めます。



MFAクライアントの設定

このリリースでは、MFAクライアントとしてCisco Duoのみがサポートされています。

次の手順では、Cisco Duo for Nexus Dashboard MFAを使用できるようにするために必要な基本設定を提供します。詳細なDuo設定は、このドキュメントの範囲外です。使用可能なすべてのオプションについては、Cisco Duoのドキュメントを参照してください。

Duoを設定するには、次を実行します。

1. Oktaアカウントにログインします。
2. DUOをMFAタイプとして追加します。
   a. 左のナビゲーションメニューから **[セキュリティ > 多要素（Security > Multifactor）]** を選択します。
   b. **[要素タイプ（Factor Types）]** タブで、[Duo セキュリティ（Duo Security）] を選択します。

      Duo Security オプションがない場合は、https://support.okta.com/help/s/opencase から Okta でサポートケースを開く必要があります。

   c. **[Duoセキュリティ（Duo Security）]** ウィンドウで、必要な情報を入力します。

      統合キー、秘密キー、API ホスト名を取得する方法の詳細については、https://duo.com/docs/okta を参照してください。

      Duo ユーザー名の形式が電子メールに設定されていることを確認します。

   d. **[保存（Save）]** をクリックします。
3. Duo ルールを作成します。
   a. 左側のナビゲーションメニューから、**[アプリケーション > アプリケーション（Applications > Application）]** を選択します。
   b. 作成したアプリケーション（nd-mfa）をクリックします。
   c. **[サインオン（Sign On）]** タブを選択します。
   d. **[サイン オン ポリシー（Sign On Policy）]** 領域で、**[+ルールの追加（+Add Rule）]** をクリックします。
   e. ルールの名前を入力します。
   f. **[アクセス（Access）]** 領域で **[要素のプロンプト（Prompt for factor）]** を有効にして、**[すべてのサインオン（Every sign on）]** を選択します。
   g. ユースケースの必要に応じて、他のオプションを指定します。
   h. **[保存（Save）]** をクリックします。
4. Okta と Duo の統合を構成します。

   Okta で構成したユーザーが MFA 用の Duo アプリを使用できるようにする方法は 2 つあります。Duo 管理者に Duo ダッシュボードと同じユーザーをすべて追加してもらうか、個々のユーザーが Okta にログインして自分で登録するかです。

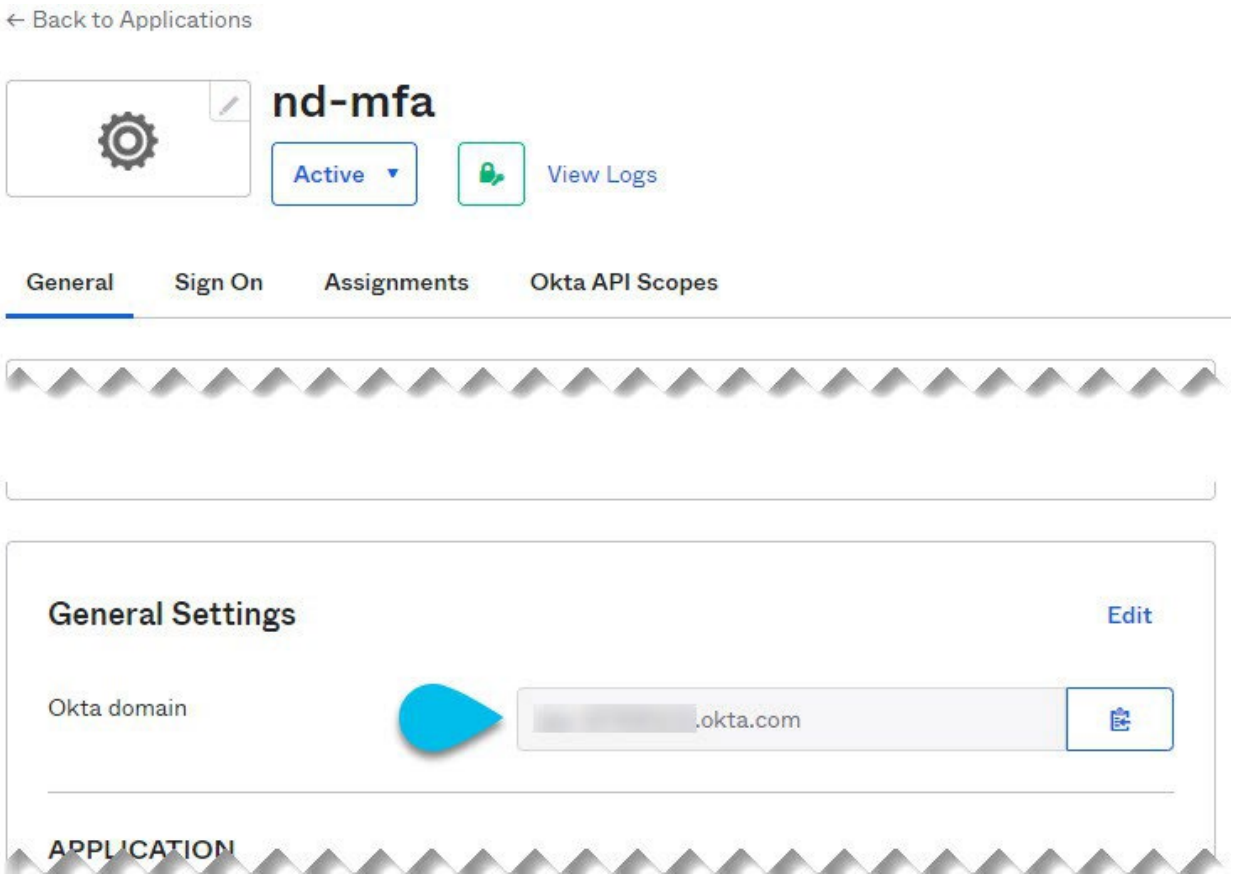
   Duoダッシュボードでユーザーを設定するには、次を実行します。

   a. 管理者ユーザーとしてDuoダッシュボードにログインします。
   b. 左のナビゲーション メニューから **[ユーザー（Users）]** を選択します。
   c. **[ユーザーの追加（Add User）]** をクリックし、Okta のユーザー情報と一致する詳細情報を入力します。
   d. Oktaに追加したすべてのユーザーについて、この手順を繰り返します。自己登録するには、次を実行します。

      a. 「MFA プロバイダーとしての Okta アカウントの構成」で作成したすべてのユーザーに、特定の

Okta ドメインを使用して自分で Okta にログインするように指示します。

使用する Okta ドメインを決定するには、**[**アプリケーション **>** アプリケーション（**Application > Application**）**]** に移動し、作成した nd-mfa アプリケーションをクリックして、**[Okta** ドメイン（**Okta domain**）**]** の URL をコピーします。



b. ログインすると、右上のユーザーメニューから **[設定（Settings）]** ページに移動できます。

c. **[Duoセキュリティ設定（Duo Security Setup）]** を選択し、画面の指示に従います。

リモート認証プロバイダーとしての Okta の追加

はじめる前に

- 「 Configuring Okta Account as MFA Provider」で説明されているように、Okta は 1 人以上のユーザーで構成されている必要があります。
- Okta アカウントからのクライアント **ID**、クライアントシークレット、発行者情報が手元にある必要があります。これについては、「Configuring Okta Account as MFA Provider」の最後の手順で説明されています。
- プロキシを使用して Okta アカウントに接続する場合は、「システム設定」で説明されているように、プロキシが構成済みである必要があります。

Oktaをリモート認証プロバイダーとして追加するには、次を実行します。

1. 管理者ユーザーとして Nexus Dashboard にログインします。
2. **[管理コンソール（Admin Console）]** に移動します。
3. 認証ドメインを追加します。
   a. メイン ナビゲーション メニューから、**[管理] > [認証]（Administrative > Authentication）** の順に選択します。
   b. メイン ペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[ログイン ドメインの作成（Create Login Domain）]** を選択します。
4. **[ログインドメインの作成（Create Login Domain）]** 画面が開いたら、ドメインの詳細を入力します。
   a. **[名前（Name）]** にドメインの名前を入力します。

b. （任意）**[**説明（**Description**）**]** にドメインの説明を入力します。
c. **[**レルム（**Realm**）**]** ドロップダウンから、[OIDC] を選択します。
d. **[**クライアント**ID**（**Client ID**）**]** フィールドに、Okta アカウントから取得したクライアント ID を入力します。
e. **[**クライアントシークレット（**Client Secret**）**]** フィールドに、Okta アカウントから取得したクライアントシークレットを入力します。
f. **[**発行者（**Issuer**）**]** フィールドに、Okta アカウントから取得した URI を入力します。
g. （任意）プロキシ経由で Okta に接続する場合は、**[**ユーザープロキシ（**User Proxy**）**]** オプションをオンにします。
h. **[**範囲（**Scopes**）**]** オプションはオフのままにします。

このリリースでは、openid の範囲のみがサポートされています。

5. **[**作成（**Create**）**]** をクリックして、ドメインの追加を終了します。

MFA を使用した Nexus Dashboard へのログイン

1. 通常どおり、Nexus DashboardのIPの1つに移動します。
2. **[**ログインドメイン（**Login Domain**）**]** ドロップダウンから、「リモート認証プロバイダーとしての Okta の追加 」で作成した OIDC ドメインを選択します。

ユーザー名とパスワードのフィールドは表示されません。

3. **[Login]** をクリックします。

Oktaログインページに移動します。

4. 「MFA プロバイダーとしての Okta アカウントの構成」の説明に従って、Okta で構成されたユーザーを使用してログインします。

Duoクライアントにプッシュ通知が送信されます。

5. Duoを使用してログインを承認します。

Nexus Dashboard UIにリダイレクトされ、Oktaユーザーを使用してログインします。

ユーザ

[ユーザー（**Users**）**]** の GUI ページでは、Nexus Dashboard にアクセスできるすべてのユーザーを表示および管理できます。

[ローカル（**Local**）**]** タブにはすべてのローカルユーザーが表示され、**[**リモート（**Remote**）**]** タブには、「リモート認証」セクションの説明に従って追加したリモート認証サーバーに設定されているユーザーが表示されます。

- デフォルトのローカル 管理者ユーザーは削除できません。
- Nexus Dashboard、サイト、およびアプリケーション間のシングルサインオン(SSO)は、リモートユーザーのみが使用できます。リモートユーザーの設定の詳細については、「リモート認証」を参照してください。

ローカル ユーザの追加

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。
2. 新しいローカルユーザを作成します。
   a. メイン ナビゲーション メニューから、**[**管理（**Admin**）**] > [**ユーザー（**Users**）**]** を選択します。
   b. メイン ペインの右上で、**[**ローカル ユーザーの作成（**Create Local User**）**]** をクリックします。
3. **[**ローカルユーザーの作成（**Create Local User**）**]** 画面が開いたら、ユーザーの詳細を入力します。
   a. ログインに使用するユーザー **ID** を入力します。
   b. 最初のパスワードを入力して確認します。
   c. ユーザーの名、姓、電子メール アドレスを入力します。
   d. ユーザーのロールと権限を選択します。

      各ユーザーに対して1つ以上のロールを選択できます。使用可能なロールとその権限については、「ロールと権限」を参照してください。

      選択したすべてのユーザーロールに対して、読み取り専用アクセスと読み取り/書き込みアクセスのどちらを有効にするかを選択できます。読み取り専用アクセスの場合、ユーザーは自分のユーザーロールで許可されたオブジェクトと設定を表示できますが、変更することはできません。

   e. **[**作成（**Create**）**]** をクリックしてユーザーを保存します。

ローカル ユーザの編集

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。
2. ユーザの詳細画面を開きます。
   a. メイン ナビゲーション メニューから、**[**管理（**Admin**）**] > [**ユーザー（**Users**）**]** を選択します。
   b. メインペインで、ユーザーの名前をクリックします。
   c. 詳細ペインが開いたら、**[**詳細（**Details**）**]** アイコンをクリックします。
3. ***<user-name>*** の詳細画面が開いたら、**[**編集（**Edit**）**]** アイコンをクリックします。
4. **[**ユーザーの編集（**Edit User**）**]** 画面で、必要に応じて設定を更新します。

セキュリティ

[セキュリティ（**Security**）**]** の GUI ページでは、Nexus Dashboard で使用される証明書を表示および管理できます。

セキュリティ設定

[管理（**Administrative**）**] >** [セキュリティの構成（**Security Configuration**）] ページでは、Nexus Dashboard クラスタで使用される認証セッションのタイムアウトとセキュリティ証明書を設定できます。

はじめる前に

- Nexus Dashboard で使用する予定のキーと証明書がすでに生成されている必要があります。通常、これには次のファイルが含まれます。
  - 秘密キー（nd.key ）
  - 認証局（CA）パブリック証明書（ca.crt）
  - CA 署名付き証明書（nd.crt）

  自己署名証明書用の上記ファイルの生成については、「秘密キーと自己署名証明書の 生成」で説明されています。
- セキュリティの設定を変更する前に、Nexus Dashboard クラスタの構成バックアップを作成することをお勧めします。

  バックアップの詳細については、Nexus Dashboard Operations の「バックアップと復元」を参照してください。

セキュリティの設定を編集するには、次を実行します。

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。
2. セキュリティの設定を編集します。
   a. メイン ナビゲーション メニューから、**[**管理（**Admin**）**] > [**セキュリティ（**Security**）**]** を選択します。
   b. メイン ペインで、**[**セキュリティの設定（**Security Configuration**）**]** タブを選択します。
   c. メイン ペインの右上にある **[**編集（**Edit**）**]** アイコンをクリックします。
3. **[**セキュリティの構成（**Security Configuration**）**]** 画面で、必要に応じて詳細を更新します。

   キーと証明書ファイルのアップロードはサポートされていないため、次のフィールドに情報を貼り付ける必要があることに注意してください。

   a. **[**セッションタイムアウト（**Session Timeout**）**]** を更新します。

   このフィールドは、API トークンの持続時間を定義します。デフォルトは 20 分に設定されています。

   b. **[**アイドルタイムアウト（**Idle Timeout**）**]** を更新します。

   このフィールドは、UI セッションの持続時間を定義します。

   c. **[** ドメイン名（**Domain Name**）**]** フィールドで、ドメインを指定します。
   d. **SSL** 暗号 フィールドをクリックして、有効にする追加の暗号スイートをドロップダウンから選択

するか、既存の暗号スイートの **x** アイコンをクリックして削除します。
暗号スイートは、ネットワーク接続を保護するために使用されるアルゴリズム（キー交換、一括暗号化、メッセージ認証コードなど）を定義します。このフィールドを使用すると、Nexus ダッシュボード クラスタがネットワーク通信に使用する暗号スイートをカスタマイズし、安全性の低い TLS1.2 や TLS1.3 などの望ましくないスイートを無効にすることができます。

e. **[**キー（**Key**）**]** フィールドで、秘密キーを指定します。

f. **[RSA**証明書（**RSA Certificate**）**]** フィールドに、CA 署名または自己署名の証明書を指定します。

g. **[**ルート証明書（**Root Certificate**）**]** フィールドに、CA のパブリック証明書を指定します。

h. （オプション）CA が中間証明書を提供している場合は、それを 中間証明書 フィールドに入力します。

i. **[**保存 **(Save)]** をクリックして、変更内容を保存します。

変更を保存すると、新しい設定を使用してGUIがリロードされます。

セキュリティ ドメイン

制限付きセキュリティドメインを使用すると、管理者は、両方のグループのユーザーに同じ特権が割り当てられている場合でさえ、別のセキュリティドメインのユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。

たとえば、制限付きセキュリティドメイン（domain1）の管理者は、別のセキュリティドメイン（domain2）のサイト、サービス、クラスタ、ユーザー構成を閲覧できません。

ユーザーは、ユーザーが適切な権限を持っているシステムで作成された構成に対して、常に読み取り専用の可視性を持つことに注意してください。制限付きセキュリティドメインのユーザーには、そのドメイン内で幅広いレベルの特権を与えることができます。ユーザーが別のグループの物理環境に不注意で影響を与える心配はありません。

セキュリティ ドメインを作成する手順：

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。
2. 新しいセキュリティドメインを作成します。
   a. メイン ナビゲーション メニューから、**[**管理（**Admin**）**] > [**セキュリティ（**Security**）**]** を選択します。
   b. メイン ペインで、**[**セキュリティ ドメイン（**Security Domain**）**]** タブを選択します。
   c. メイン ペインの右上で、**[**セキュリティ ドメインの作成（**Create Security Domain**）**]** をクリックします。
3. **[**セキュリティドメインの作成（**Create Security Domain**）**]** 画面が開いたら、ドメインの詳細を入力します。
   a. **[**名前（**Name**）**]** にドメインの名前を入力します。
   b. （任意）ドメインの説明を入力します。
   c. **[**作成（**Create**）**]** をクリックしてドメインを保存します。

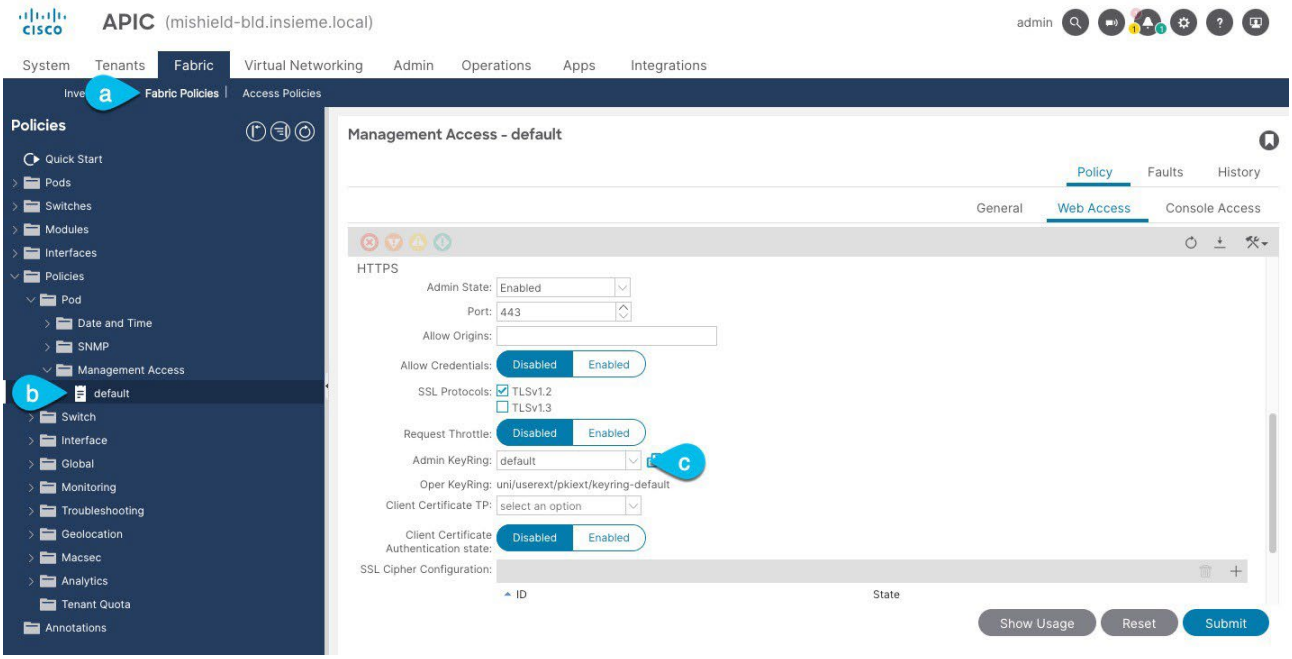
ピア証明書の検証

サイト コントローラの認証局（CA）ルート証明書チェーンを Nexus Dashboard にインポートできます。これにより、Nexus ダッシュボードが接続するホスト（サイト コントローラなど）の証明書が有効であり、

サイトを追加するときに信頼できる認証局（CA）によって署名されていることを確認できます。

Cisco APIC からの証明書チェーンのエクスポート

1. Cisco APIC にログインします。
2. 管理アクセスに使用されているキー リングを確認します。



a. 上部のナビゲーション バーで、**[ファブリック] > [ファブリック ポリシー]** を選択します。

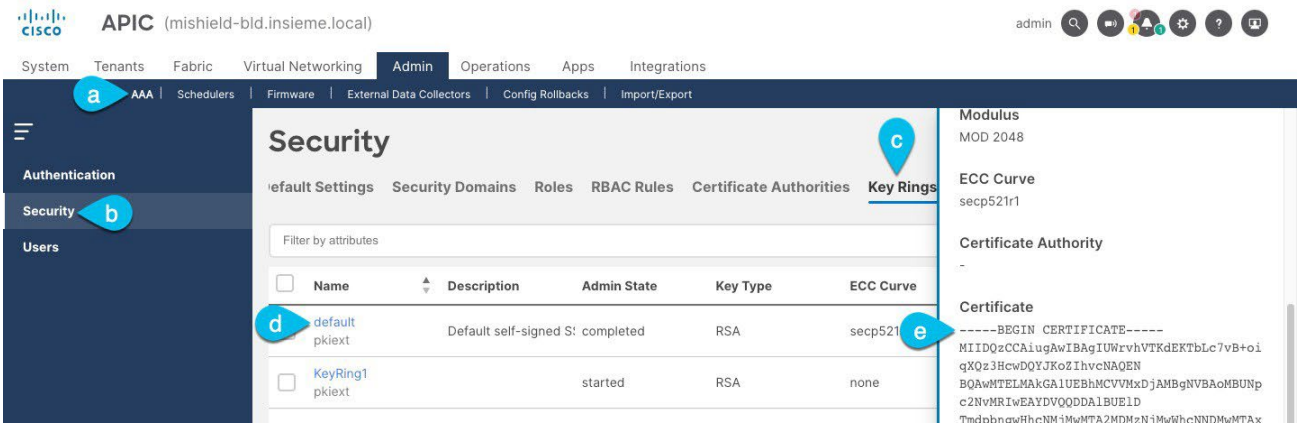
b. 左側のナビゲーション メニューで、**[ポリシー] > [ポッド] > [管理アクセス]** を選択します。

c. メイン ペインで、**Admin KeyRing** フィールドの名前を書き留めます。

上記の例では、default キー リングが使用されています。ただし、カスタム証明書チェーンを使用してカスタム キー リングを作成した場合は、そのキー リングの名前が **Admin KeyRing** フィールドにリストされます。

Cisco APIC のカスタムセキュリティ設定については、ご使用のリリースの *『Cisco APIC Security Configuration Guide』* を参照してください。

3. キー リングで使用される証明書をエクスポートします。



a. 上部のナビゲーション バーで、**[Admin] > [AAA]** を選択します。

b. 左側のナビゲーション メニューで、**[セキュリティ]** を選択します。

c. メイン ペインで、**[キー リング]** タブを選択します。

d. 前の手順で見つけたキー リングの名前をクリックし、証明書 をコピーします。

上記の例は、前のステップの「デフォルト」キー リングを示しています。ただし、カスタム キー リングが構成されている場合は、キー リングの作成に使用された CA 証明書チェーンを選択します。

コピーするテキストには、-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- を含める必要があります。
次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIUWrvhVTKdEKTbLc7vB+oiqXQz3HcwDQYJKoZIhvcNAQEN
[...]
-----END CERTIFICATE-----
```

Cisco NDFC からの証明書チェーンのエクスポート

1. サービスをホストしている Nexus Dashboard にログインします。

   NDFC の場合、サービスとは別の証明書がないため、Nexus Dashboard ホストの証明書を使用します。

2. 証明書をエクスポートします。
   a. メイン ナビゲーション メニューから、**[管理] > [セキュリティ]** を選択します。
   b. メインペインで、**[セキュリティの設定]** タブを選択します
   c. **[セキュリティ構成]** ページで、**[編集]** アイコンをクリックします。
   d. ルート証明書 をコピーします。

コピーした文字列にスペースや改行文字 (\n) が含まれないようにするために、証明書チェーンを [セキュリティ構成] ページから直接コピーするのではなく、[編集] ページからコピーすることをお勧めします。

コピーするテキストには、-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- を含める必要があります。
次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAm2gAwIBAgIIOqlnNF7g9e8wDQYJKoZIhvcNAQELBQAwSzELMAkGA1UE
[...]
-----END CERTIFICATE-----
```

Cisco DCNM からの証明書チェーンのエクスポート

1. 「sysadmin」ユーザーとして Cisco DCNM に SSH で接続します。

   他のサイト コントローラとは異なり、DCNM 証明書は UI では使用できないため、CLI を使用する必要があります。

```
# ssh -l sysadmin <dcnm-ip-address>
```

2. /var/lib/dcnm/afw/apigateway/ ディレクトリへ変更します。

   証明書（dcnmweb.crt）ファイルはこのディレクトリにありま

```
dcnm# cd /var/lib/dcnm/afw/apigateway/ dcnm#
ls -ltr /* View the contents of the folder total 128
-rw ------ 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019 11-20T132939-08:00
-rw------- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019 11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019 11-20T132950-08:00
-rw ------ 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
```

3. ルート証明書をチェックします。

   証明書の署名に使用した認証局によっては、ルート証明書が「dcnmweb.crt」ファイルに含まれている場合と、別のファイルとして提供されている場合があります。

   ルート証明書が含まれているかどうかを確認するには：

   dcnm# openssl x509 -text -noout -in *dcnmweb.crt*

   ファイルにルート証明書が含まれている場合は、それをコピーします。それ以外の場合は、証明書に署名するときに取得する必要があるルート証明書ファイルを使用します。

Cisco クラウド ネットワーク コントローラからの証明書チェーンのエクスポート

1. Cisco クラウド ネットワーク コントローラにログインします。
2. 証明書をエクスポートします。
   a. メイン ナビゲーション メニューから、**[管理] > [セキュリティ]** を選択します。
   b. メイン ペインで、**[キー リング]** タブを選択します。
   c. Nexus Dashboard にインポートする証明書の名前をクリックし、
   認証局（CA） をコピーします。

      上記の例は、default キー リングを示しています。ただし、カスタム キー リングが構成されている場合は、キー リングの作成に使用された CA 証明書チェーンを選択します。

      コピーするテキストには、-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- を含める必要があります。
      次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIDvTCCAqWgAwIBAgIJAI6W9R8DXDgLMA0GCSqGSIb3DQEBDQUAMEAxCzAJBg
NV
```

```
[...]
-----END CERTIFICATE-----
```

Nexus Dashboard への証明書のインポート

1. サイトを導入準備する予定の Nexus ダッシュボードにログインします。
2. 証明書を Nexus ダッシュボードにインポートします。
   a. サイトを導入準備する Nexus ダッシュボードにログインします。
   b. 左側のナビゲーション メニューで、**[管理] > [セキュリティ]** を選択します。
   c. メインペインで、**CA** 証明書 タブを選択します。
   d. **CA** 証明書を追加 をクリックし、証明書の一意の名前を指定して、サイトのコントローラからコピーした証明書チェーンを貼り付けます。
3. 通常どおりサイトの追加を続行しますが、**[ピア証明書の検証]** オプションを有効にします。

   有効な証明書をインポートせずに **[ピア証明書を検証]** オプションを有効にするとサイトの導入準備は機能不全になることに注意してください。

   サイトの追加については [サイトの追加] で説明しています。

商標

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

初版：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883