Microsoft Entra IDを使用したSD-WANのSSOの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

- [シングルサインオンを使用する利点](#)

[設定](#)

- [手順1:Cisco SD-WAN ManagerのSAMLメタデータの取得](#)
- [ステップ 2：Microsoft Entra IDでSSO用のエンタープライズアプリケーションを設定する](#)
- [ステップ3：エンタープライズアプリケーションへのユーザアカウントまたはグループアカウントの追加](#)
- [手順4:Microsoft Entra IDのSAMLグループプロビジョニングを設定する](#)
- [手順5:Microsoft Entra ID SAMLメタデータファイルをCisco SD-WAN Managerにインポートする](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Microsoft Entra IDを使用して、Cisco Catalystソフトウェア定義のワイドエリアネットワーク(SD-WAN)のシングルサインオン(SSO)を設定する方法について説明します。

前提条件

要件

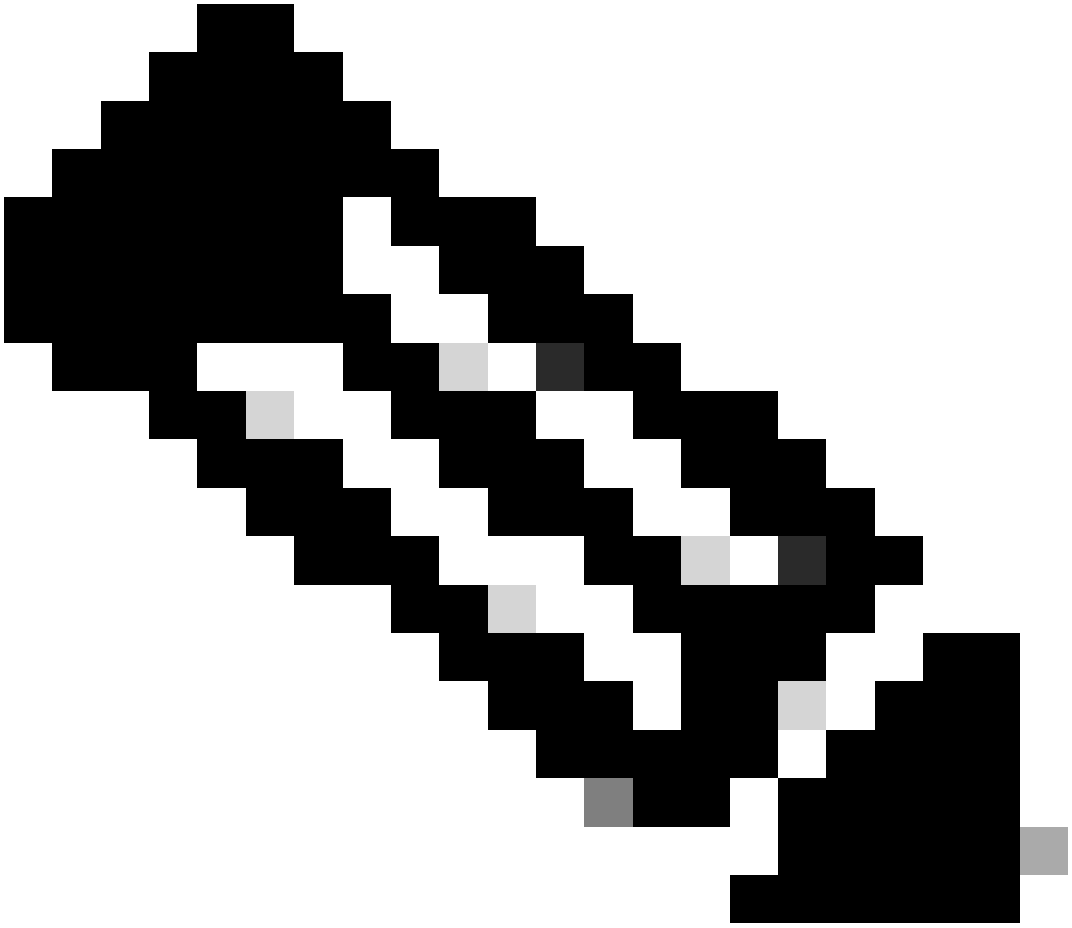
次の項目に関する一般的な知識があることが推奨されます。

- シングル サインオン
- Cisco Catalyst SD-WANソリューション

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Catalyst SD-WAN Managerリリース20.15.3.1
- Microsoftエントリ ID



注：以前はAzure Active Directory (Azure AD)と呼ばれていたソリューションは、現在はMicrosoft Entra IDと呼ばれています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

シングルサインオンは、ユーザが単一のクレデンシャルのセットを使用して、複数の独立したアプリケーションまたはWebサイトに安全にアクセスできるようにする認証方式です。SSOを使用すると、ユーザは各アプリケーションに個別にサインインする必要がなくなります。一度認証されると、許可されたすべてのリソースにシームレスにアクセスできるようになります。

SSOを実装する一般的な方法の1つは、SAML 2.0、WS-Federation、OpenID Connectなどのプロトコルを使用してアイデンティティプロバイダー(IdP)とサービスプロバイダー(SP)間の信頼を確

立するフェデレーションを使用することです。フェデレーションにより、認証が一元化され、セキュリティ、信頼性、ユーザエクスペリエンスが向上します。

Microsoft Entra IDは、これらのフェデレーションプロトコルをサポートする、広く使用されているクラウドベースのアイデンティティプロバイダーです。Cisco Catalyst SD-WANを使用したSSO設定では、Microsoft Entra IDがIdPとして機能し、Cisco SD-WAN Managerがサービスプロバイダーとして機能します。

統合は次のように機能します。

1. ネットワーク管理者がCisco SD-WAN Managerへのログインを試みます。
2. Cisco SD-WAN ManagerがMicrosoft Entra IDに認証要求を送信します。
3. Microsoft Entra IDを使用すると、管理者はEntra ID(Microsoft)アカウントを使用して認証を行うように求められます。
4. クレデンシャルが検証されると、Microsoft Entra IDは、認証を確認するセキュアな応答をCisco SD-WAN Managerに送信します。
5. Cisco SD-WAN Managerは、個別のクレデンシャルを必要とせずにアクセスを許可します。

このモデルでは、次のようになります。

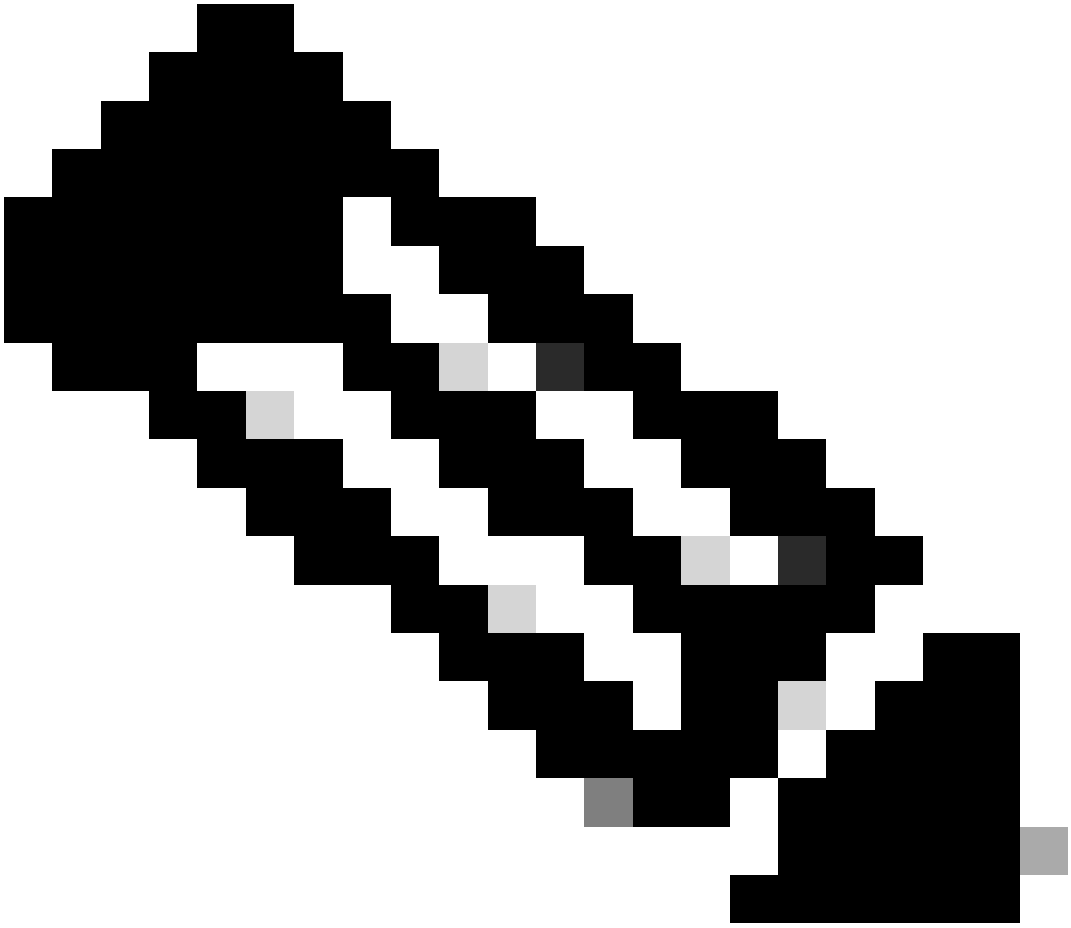
- アイデンティティプロバイダー(IdP)：ユーザデータを保存し、クレデンシャル（Microsoft Entra ID、Okta、PingID、ADFSなど）を検証します。
- サービスプロバイダー：アクセスされるアプリケーション（Cisco SD-WAN Managerなど）をホストします。
- ユーザ：IdPディレクトリにアカウントを持ち、サービスプロバイダーへのアクセスを許可されています。

Cisco Catalyst SD-WANは、業界標準に従って設定されている場合、SAML 2.0準拠の任意のIdPと互換性があります。

シングルサインオンを使用する利点

- IDプロバイダーを通じて資格情報の管理を一元化します。
- 複数の脆弱なパスワードを排除することで、認証のセキュリティを強化
- 管理者の安全なアクセスを合理化します。
- Cisco Catalyst SD-WAN Managerおよびその他の承認済みアプリケーションにワンクリックでアクセスできます。

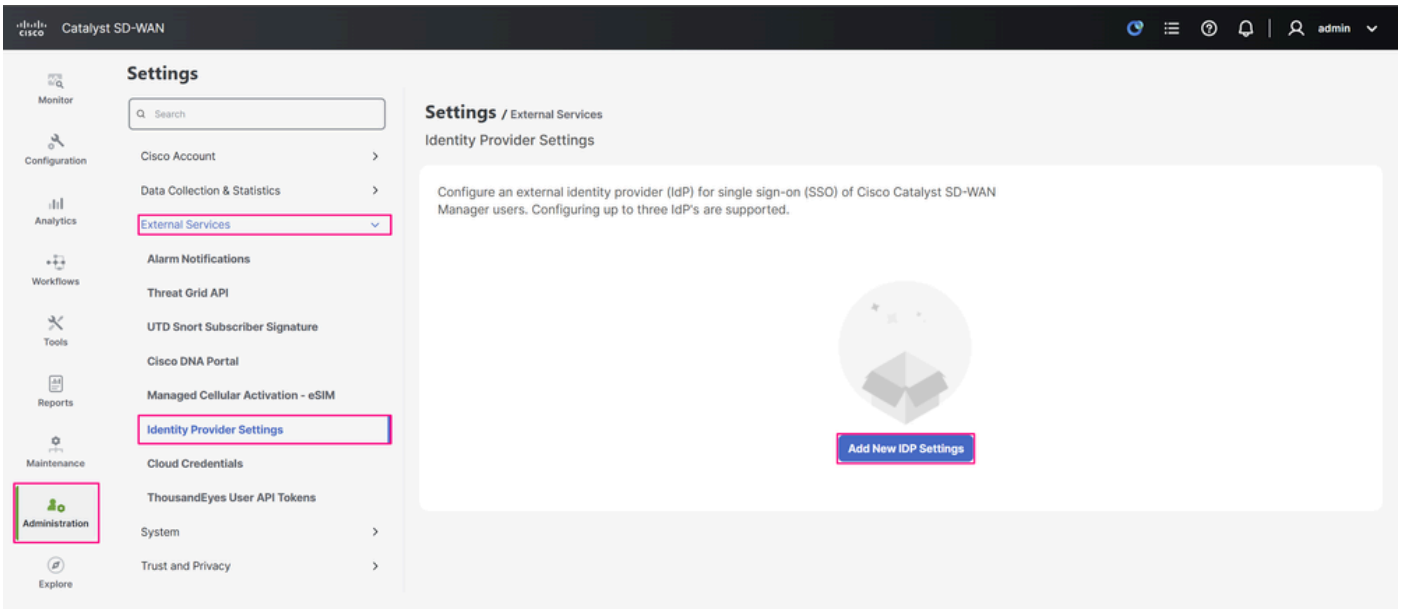
設定



注：サポートされる最小リリース：Cisco Catalyst SD-WAN Managerリリース20.8.1。

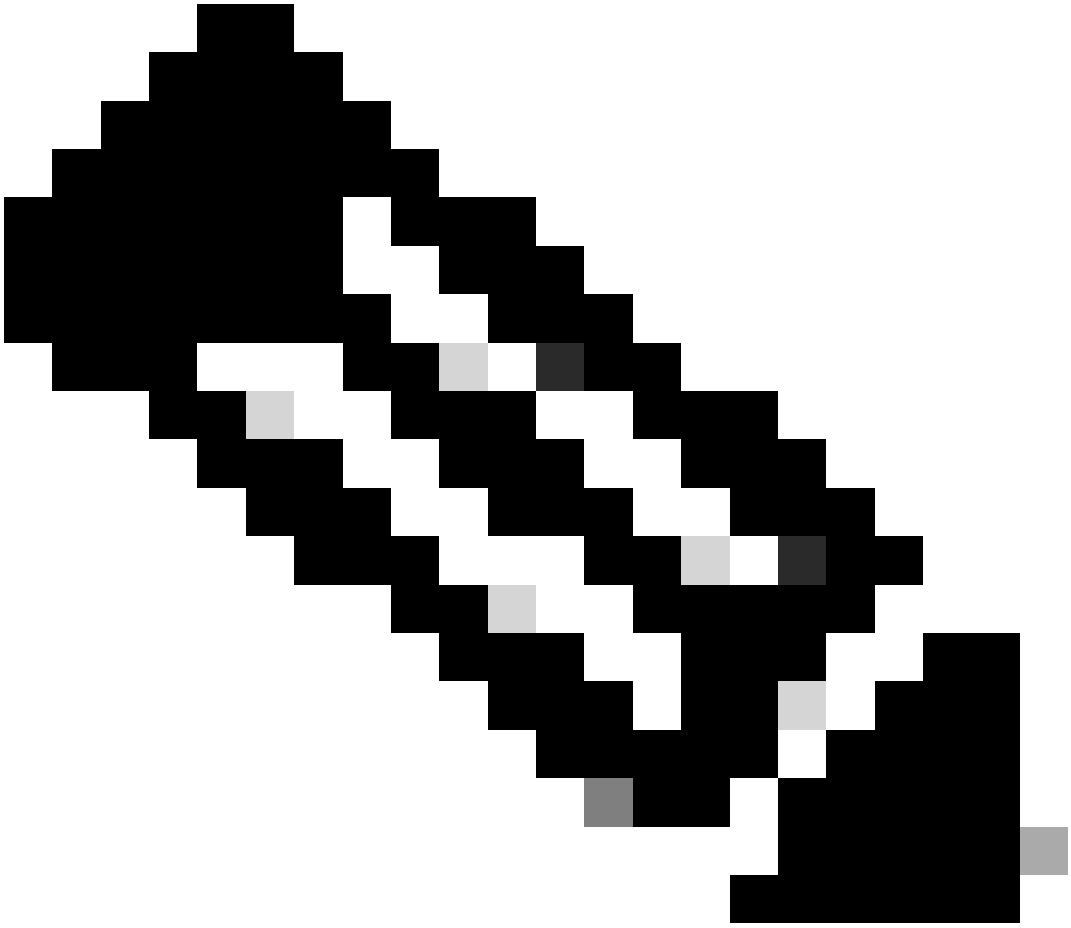
ステップ 1： Cisco SD-WAN ManagerのSAMLメタデータの取得

- Cisco SD-WAN Managerで、Administration > Settings > External Services > Identity Provider Settingsの順に移動し、Add New IDP Settingsをクリックします。



Cisco SD-WAN ManagerのUI

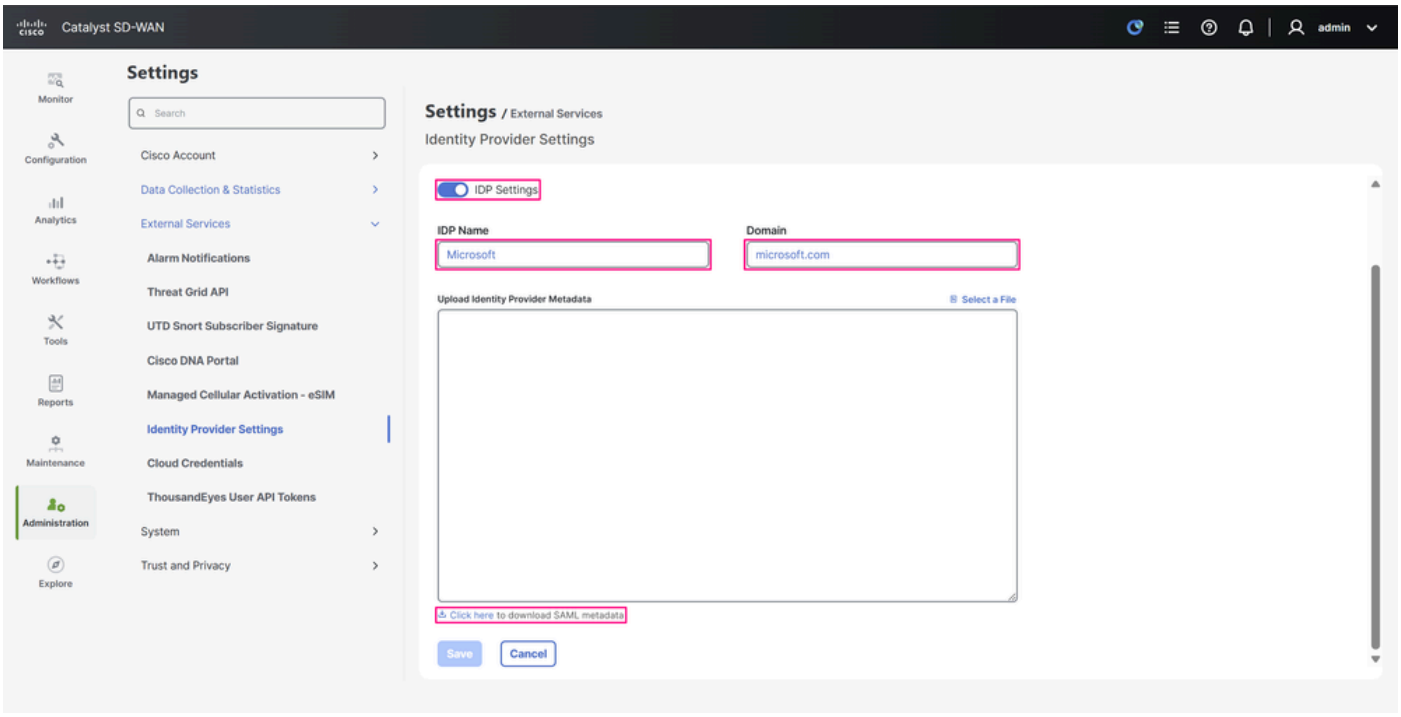
- IDプロバイダーの設定を有効にするには、IDP Settingsを切り替えます。IDP Nameフィールドに、使用しているIdPを参照する名前を入力し、Domainフィールドに、組織のエンタープライズアプリケーションでユーザが使用するドメイン名と一致するドメインを入力します。SAMLメタデータをダウンロードしてメタデータXMLファイルをコンピュータに保存するには、ここをクリックしてください。このファイルは、次の手順でMicrosoft Entra IDでSSOを設定するために使用されます。



注：この例では、メタデータXMLファイルはCisco SD-WAN ManagerのIPアドレスを直接指していますが、多くの実稼働環境では、このファイルは完全修飾ドメイン名(FQDN)を指しています。 スタンドアロンCisco SD-WAN Managerの場合、メタデータに含まれるエンティティIDは、ダウンロード時にCisco SD-WAN Managerへの口グインに使用するURLと一致します。これは、シングルノード設定であるため、IPアドレスまたはFQDNのいずれかで機能することを意味します。

Cisco SD-WAN Managerクラスタの場合、FQDNがクラスタノードの1つを指し、メタデータにこのドメインがエンティティIDとして含まれていても、同じ原則が適用されます。異なる点は、クラスタのFQDNでメタデータを使用する場合でも、そのIPアドレスを使用する特定のノードからの場合でも、Microsoft Entra IDとのSSO統合が正常に完了すると、他のノードがIdPサインインプロンプトにリダイレクトされることです。

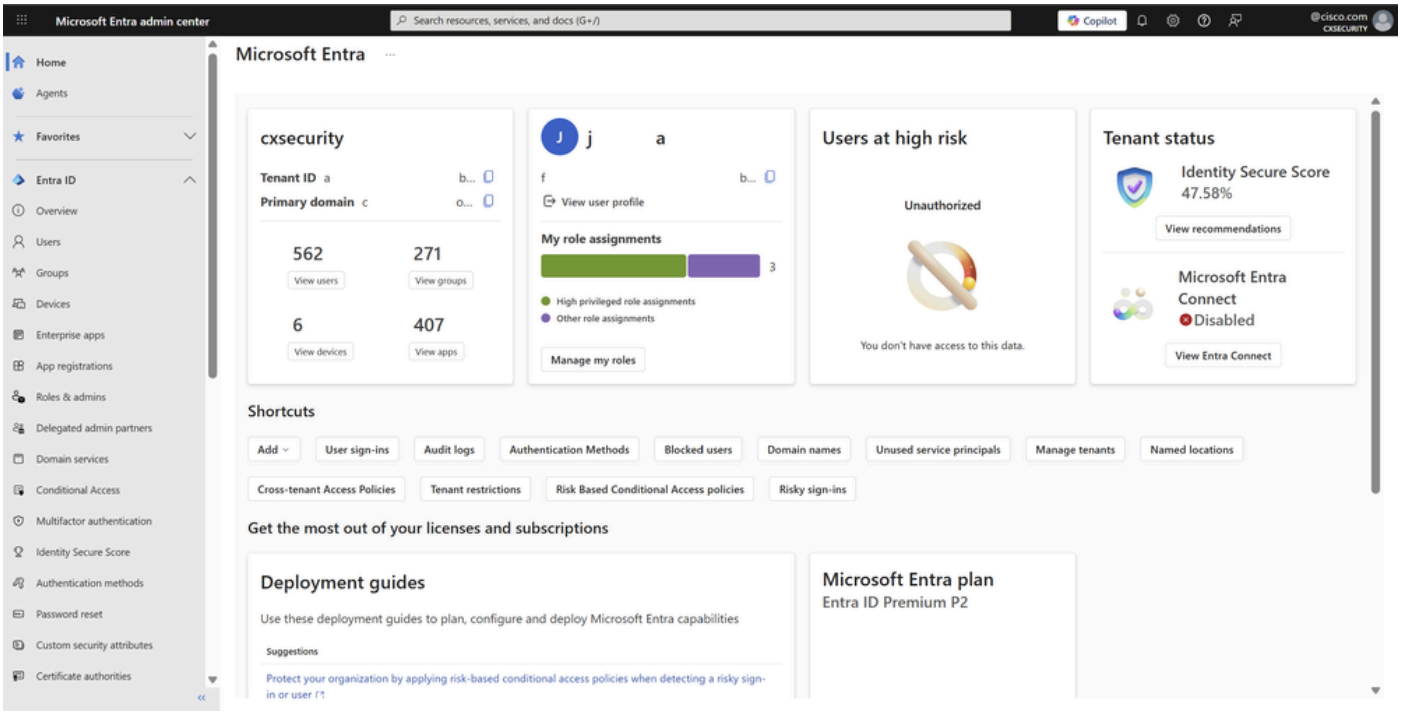
両方のシナリオの主な要件は、Cisco SD-WAN Managerで使用するエンティティID（IPアドレスまたはFQDN）が、IdP側で設定されたIDと一致することです。



IdP Settings Configurationページ

ステップ 2：Microsoft Entra IDでSSO用のエンタープライズアプリケーションを設定する

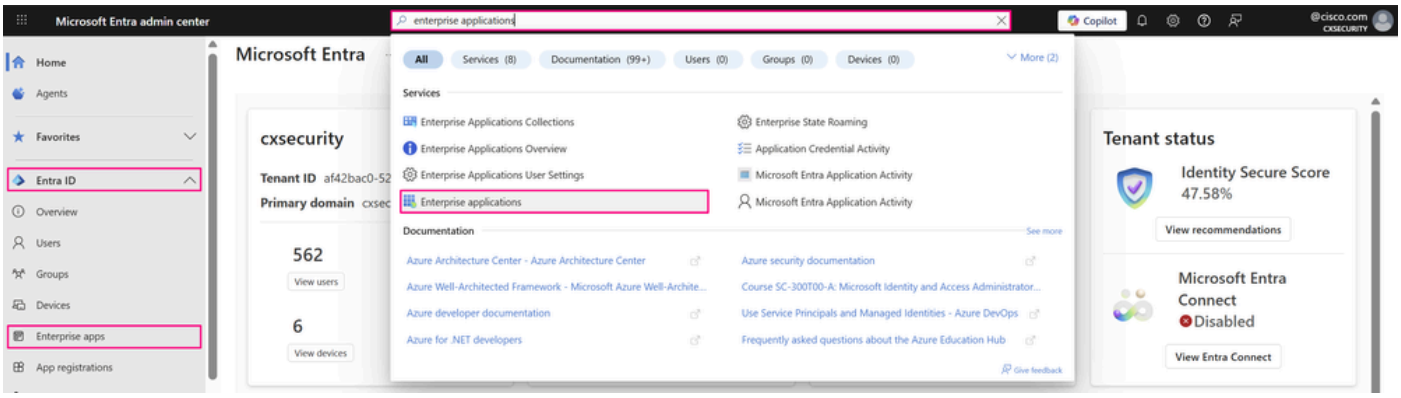
- Cloud Application Administrator、Application Administrator、またはサービスプリンシパルの所有者のいずれかのロールを使用して、Microsoft Entra管理センターポータルにログインします。



Microsoft Entra管理センターポータル

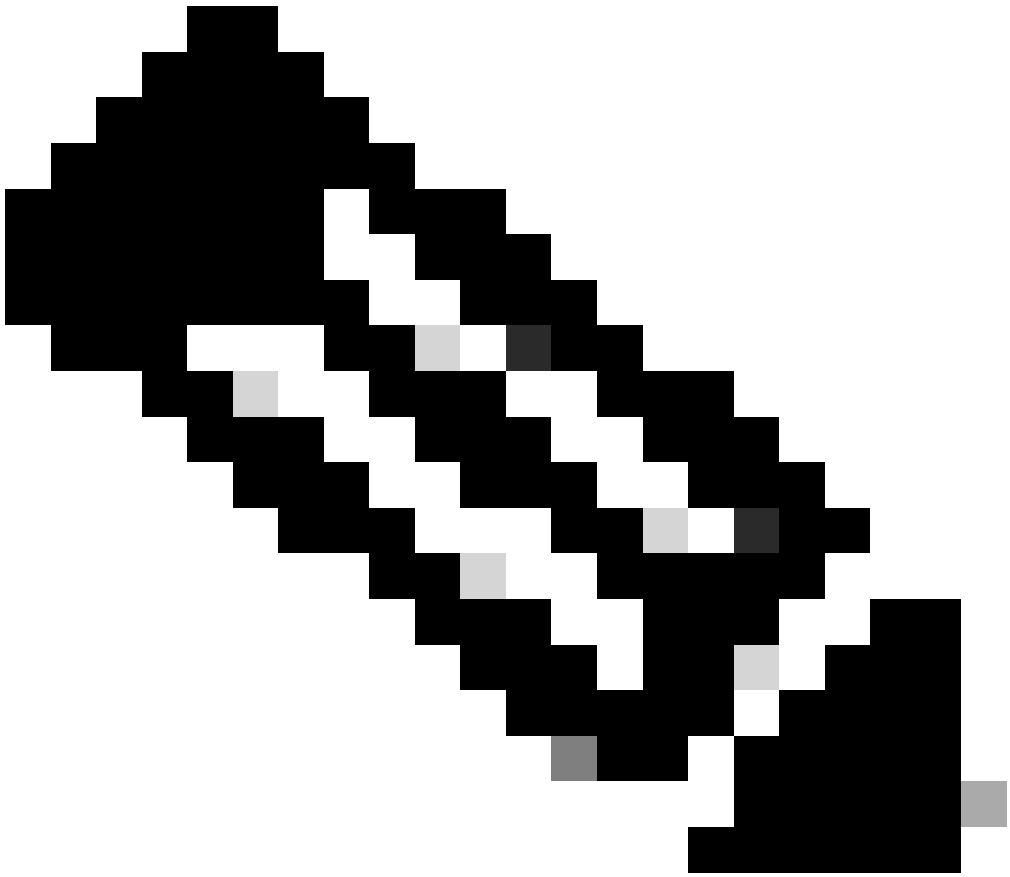
- Enter ID > Enterprise appsの順に移動するか、ポータル上部の検索バーにenterprise

applicationsと入力してEnterprise Applicationsを選択する方法でも、このサービスにアクセスできます。



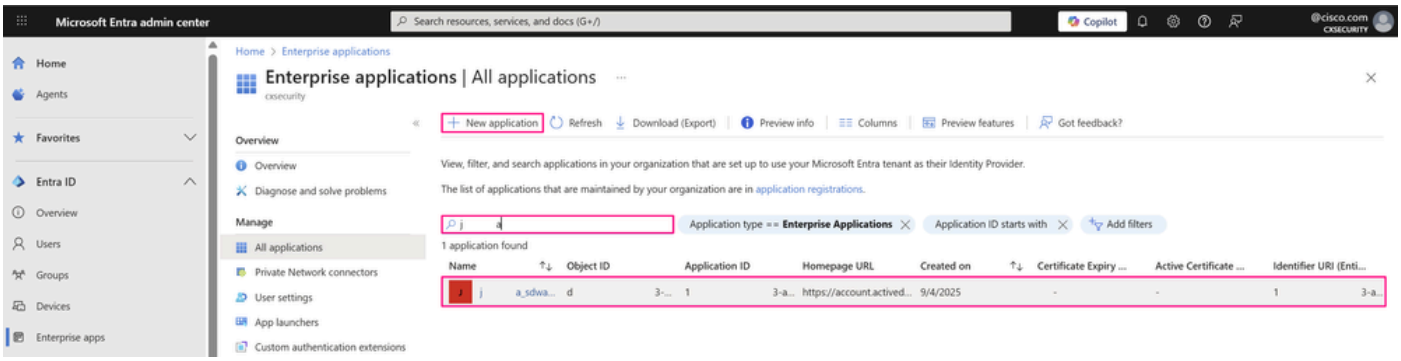
Microsoft Entra管理センターポータル

- All applicationsページが開きます。検索ボックスに既存のアプリケーションの名前を入力し、検索結果からアプリケーションを選択します。



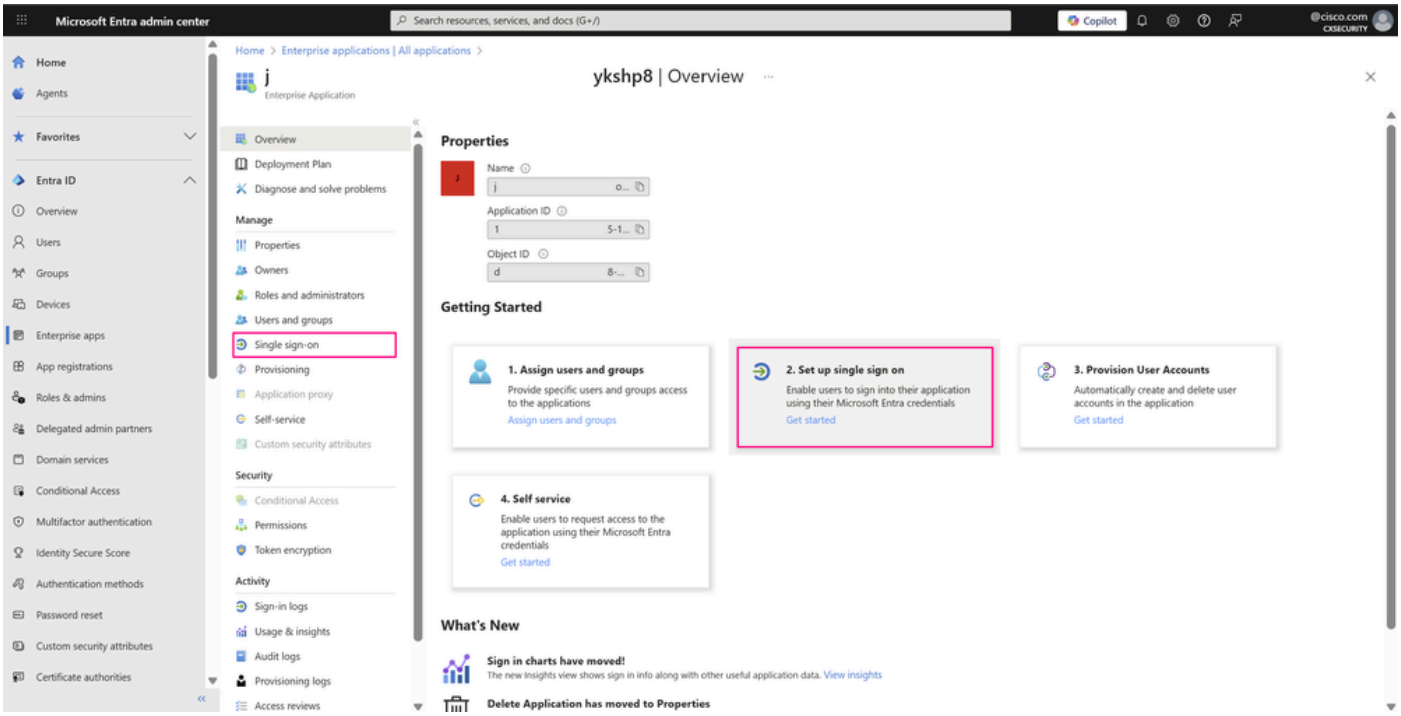
注：この同じページで、組織の要件に基づいてカスタムエンタープライズアプリケ

ーションを作成し、まだSSO認証がない場合は[新しいアプリケーション]をクリックすると、SSO認証で構成できます。



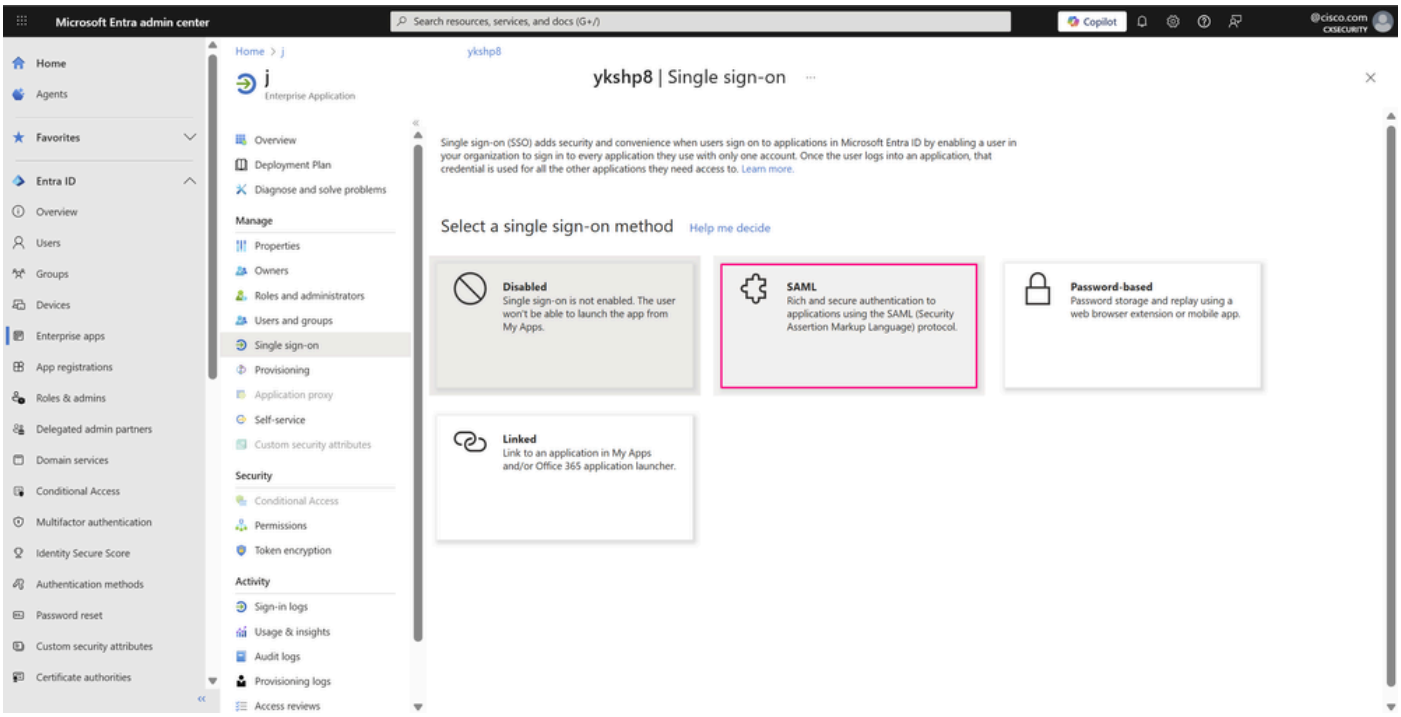
エンタープライズアプリケーションダッシュボード

- 左側のメニューのManageセクションでSingle sign-onをクリックするか、Overviewセクションの Getting Startedペインで2をクリックします。シングルサインオンを設定し、編集用にシングルサインオンペインを開きます。



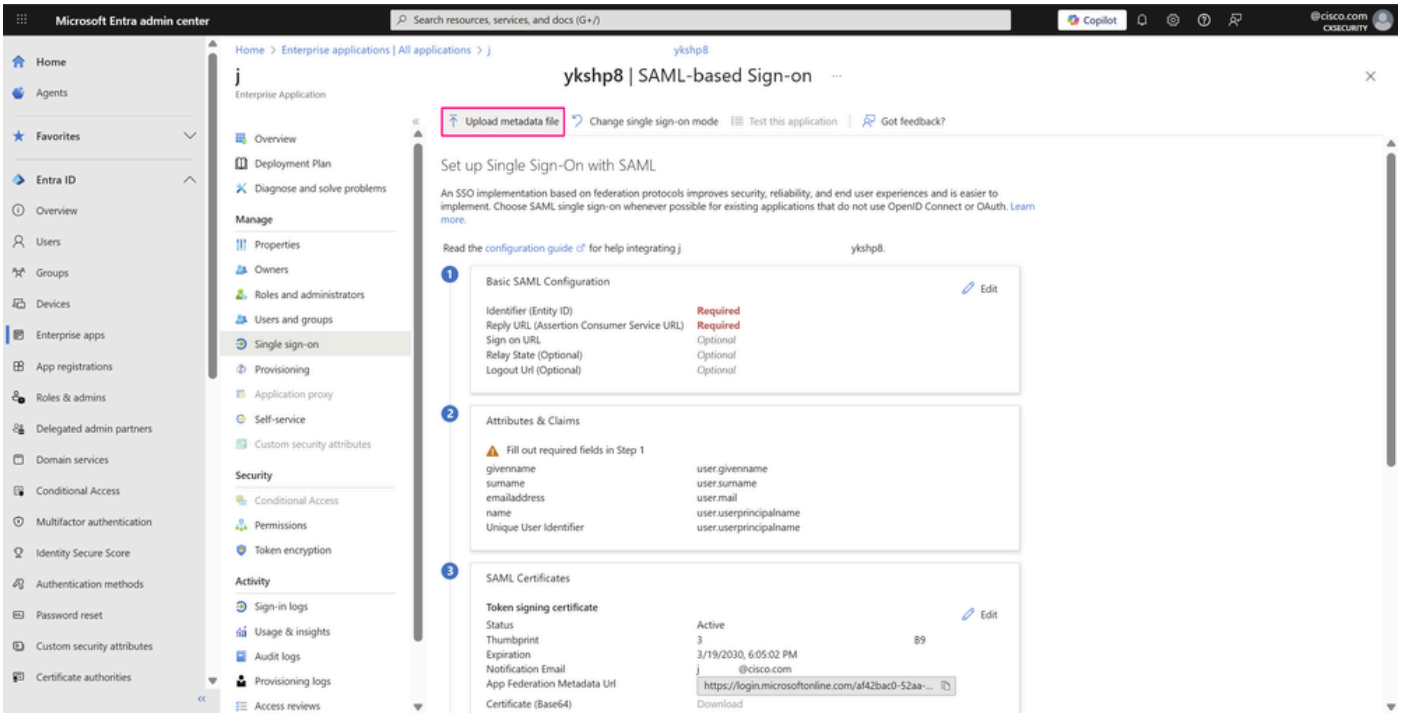
エンタープライズアプリケーションの概要

- SAMLを選択してSSO設定ページを開きます。



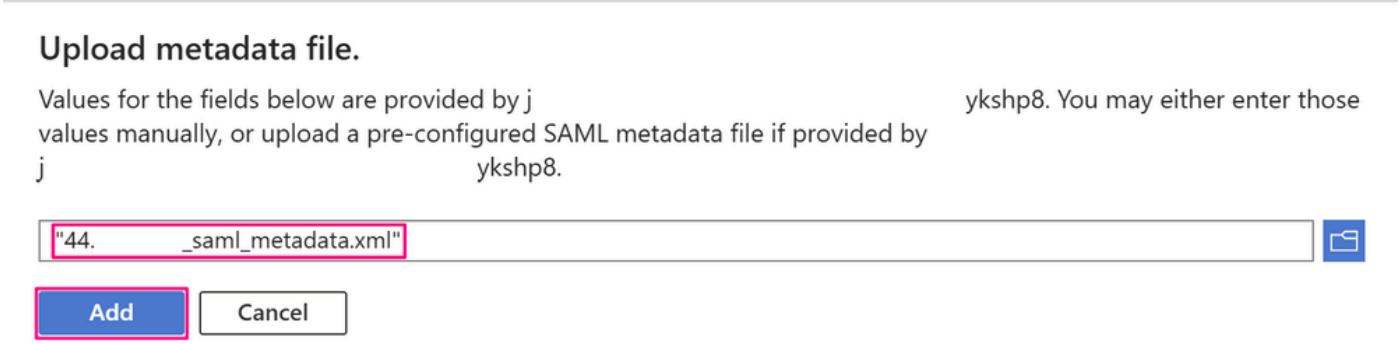
シングルサインオンウィンドウ

- Set up Single Sign-On with SAMLページで、Upload metadata fileをクリックします。



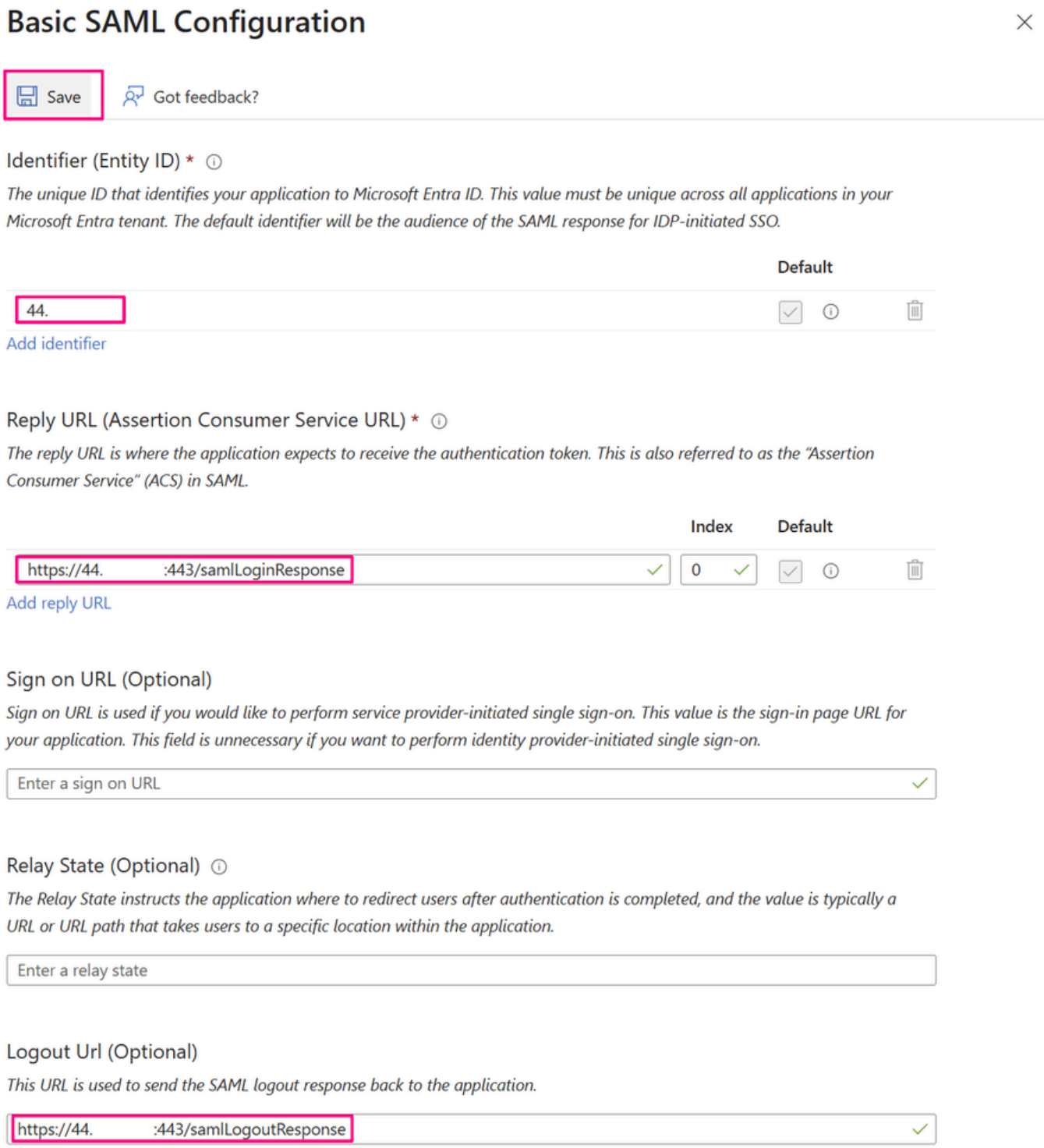
SAML設定を使用したSSOのページ

- Upload metadata fileウィンドウで、先ほどダウンロードしたmetadata XML fileを参照してクリックし、Addをクリックします。



Upload Metadata Fileウィンドウ

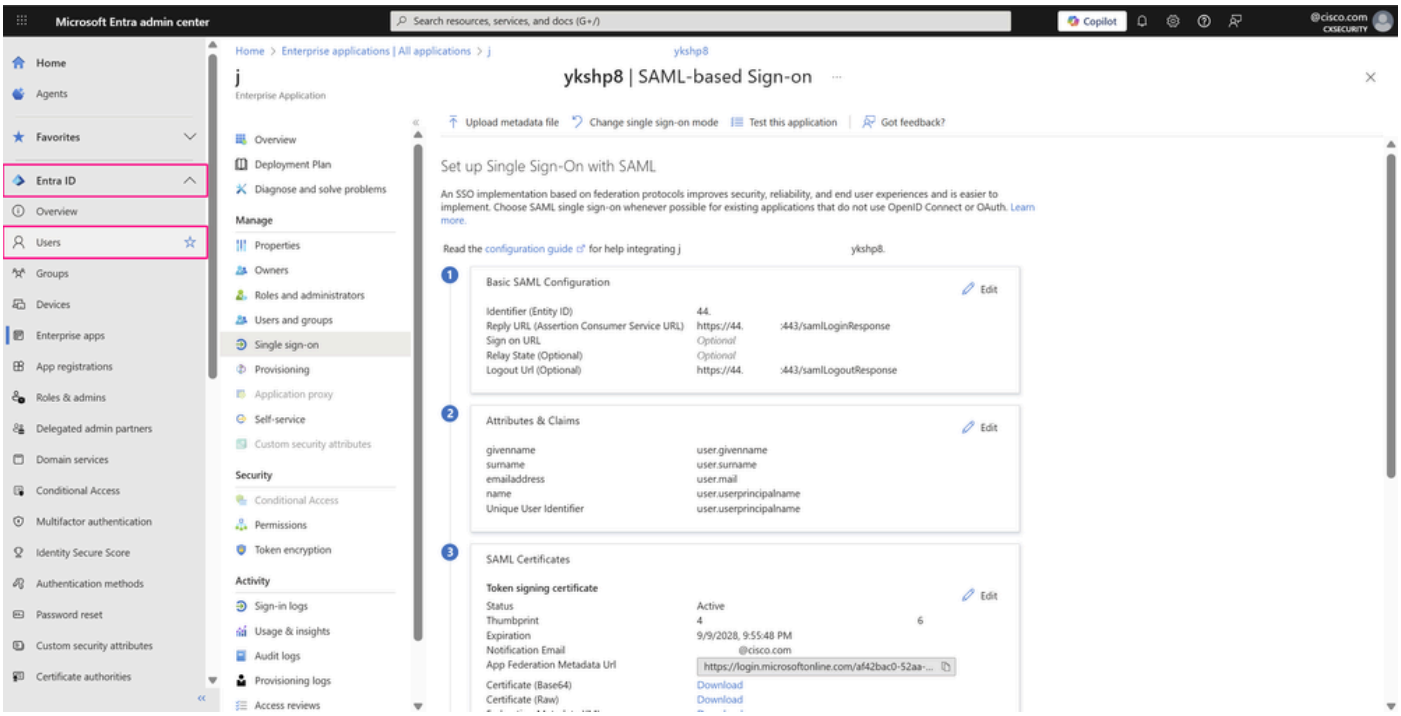
- Basic SAML Configurationウィンドウでは、通常、Identifier(Entity ID)は、統合するアプリケーション（この場合はCisco SD-WAN Manager）に固有のURLです（前述の手順を参照）。ファイルが正常にアップロードされると、返信URLとログアウトURLの値が自動的に入力されます。続行するにはSaveをクリックします。



基本的なSAML設定ウィンドウ

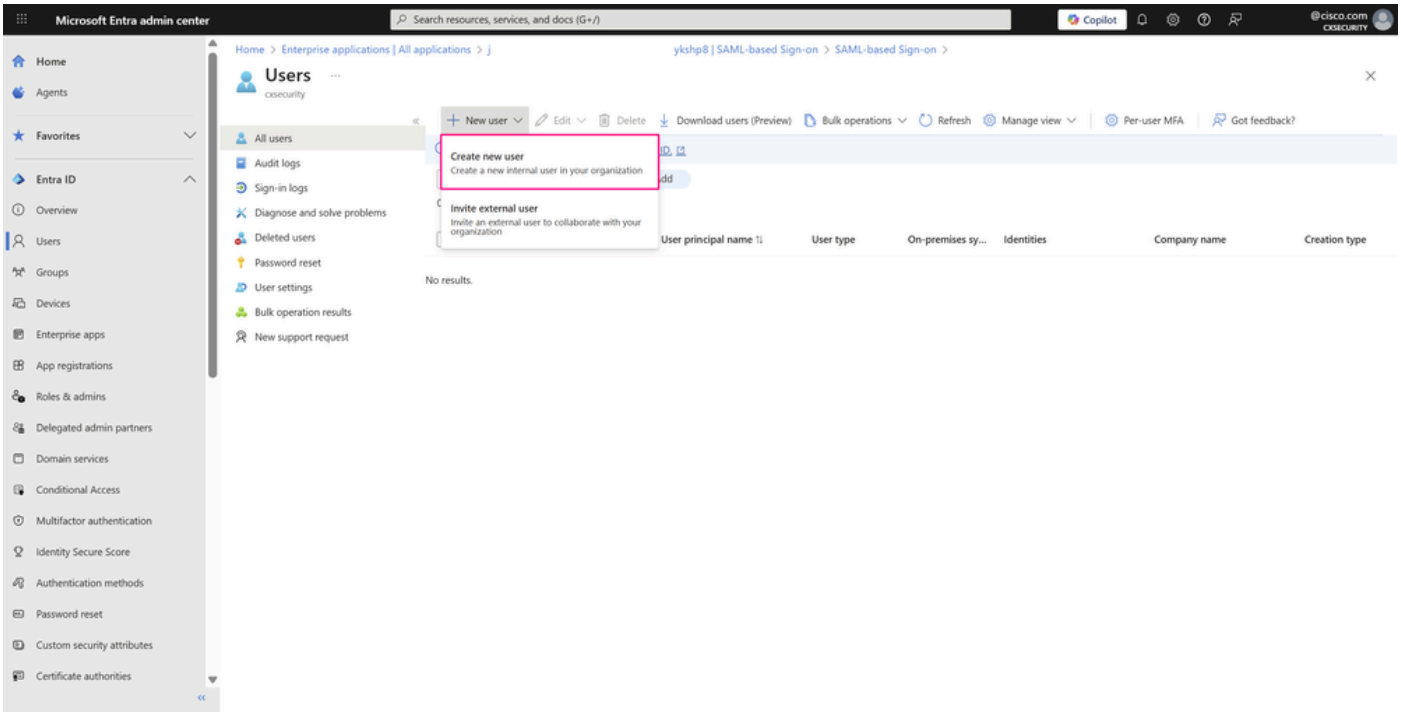
ステップ 3： エンタープライズアプリケーションへのユーザーまたはグループアカウントの追加

- アプリケーションのSAML設定パラメータを定義した状態で、アプリケーションにサインインするエンタープライズアプリケーションのユーザまたはグループを追加します。これを行うには、最初にEnter ID > Usersに移動します。または、前の手順で示したように、ポータル上部の検索バーでサービス名を検索するときにも、このサービスにアクセスできます。



SAML設定を使用したSSOのページ

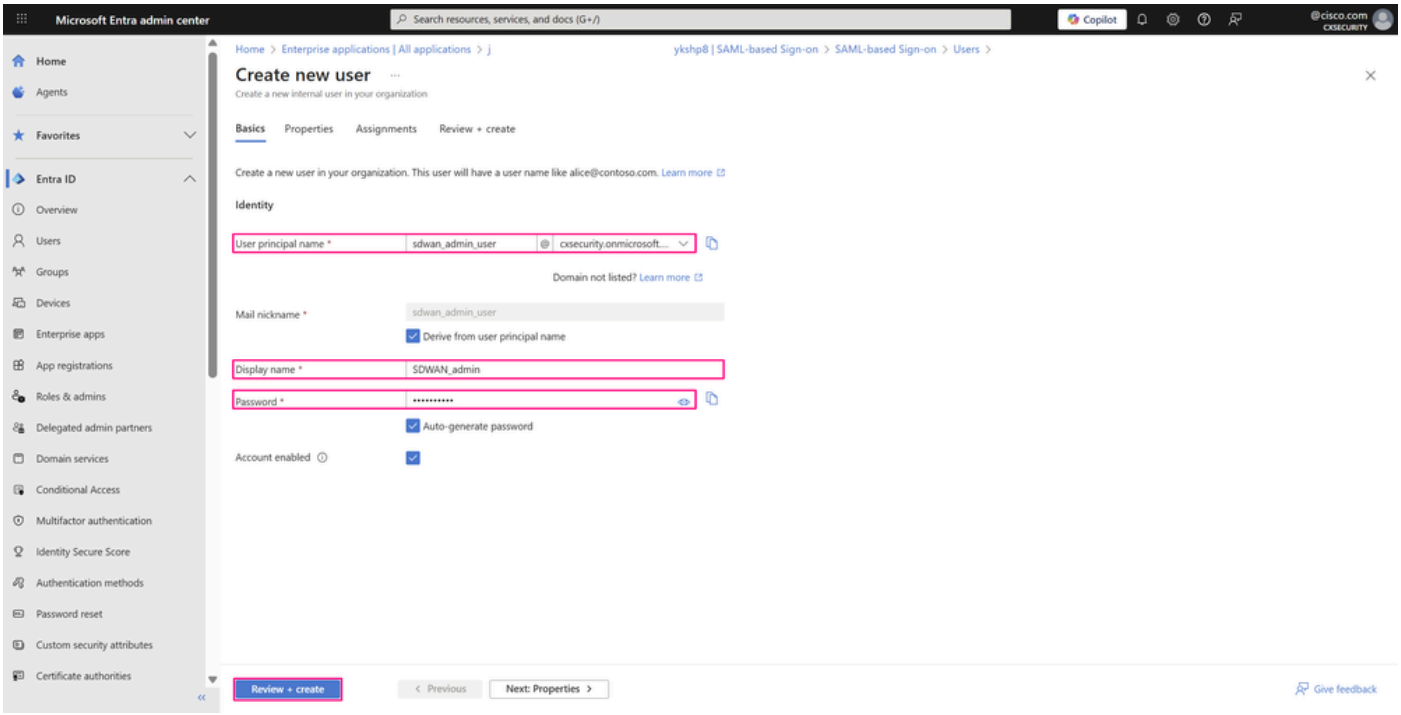
- Cisco SD-WAN Managerとそのユーザグループの1つであるnetadmin（実稼働環境で最も一般的）を使用したSSO認証を示すために、グループに関連付けるユーザを作成します。それには、IDの入力> Usersの順に移動します。 次に、New userをクリックして、Create new userを選択します。



ユーザダッシュボード

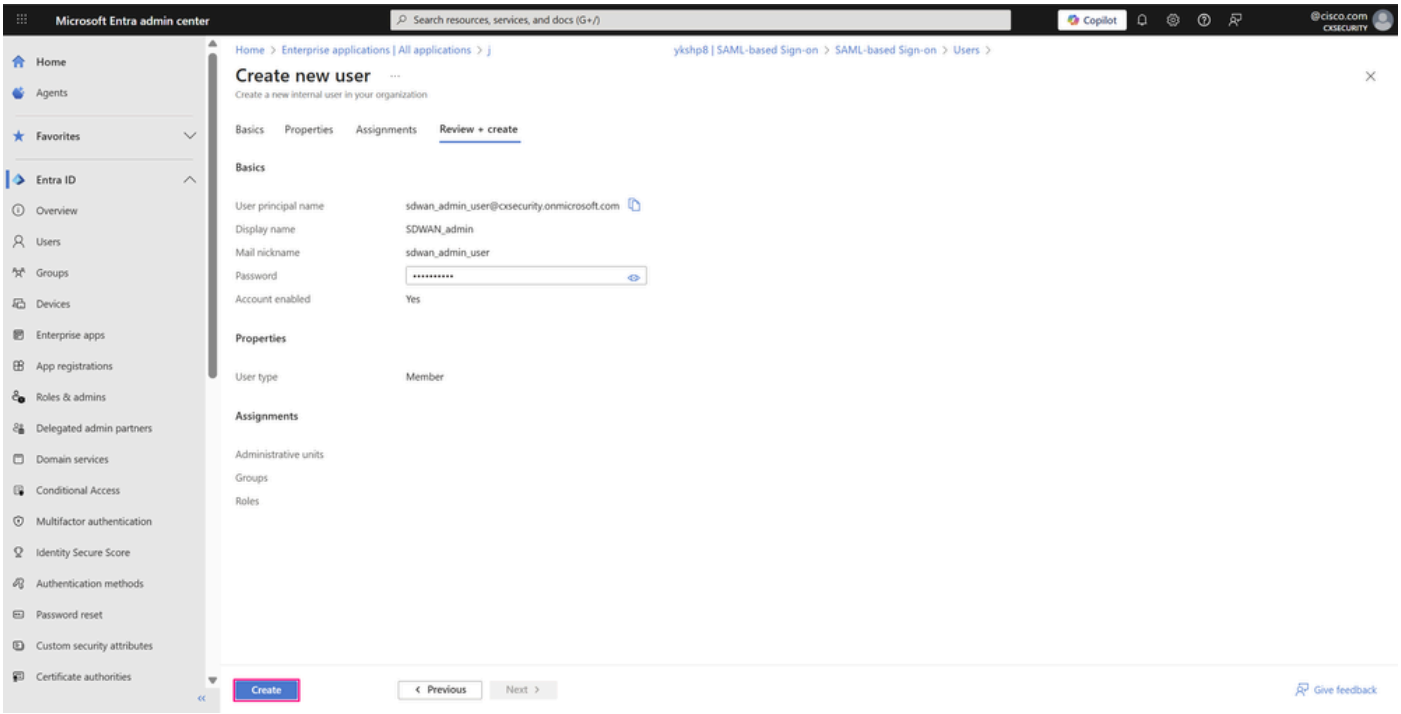
- Basicsタブには、新規ユーザの作成に必要なコアフィールドがあります。
  - ユーザプリンシパル名には、一意のユーザ名を入力し、組織内で使用可能なドメインのドロップダウンリストからドメインを選択します。
  - ユーザの表示名を入力します。

- カスタムパスワードを入力する場合はAuto-generate passwordのチェックマークを外し、パスワードを自動生成する場合はこのオプションのチェックマークを外します。
- 「割り当て」タブでユーザをグループに追加できますが、グループメンバーシップはまだ作成されていないため、「レビュー+作成」をクリックします。



ユーザー作成ページ

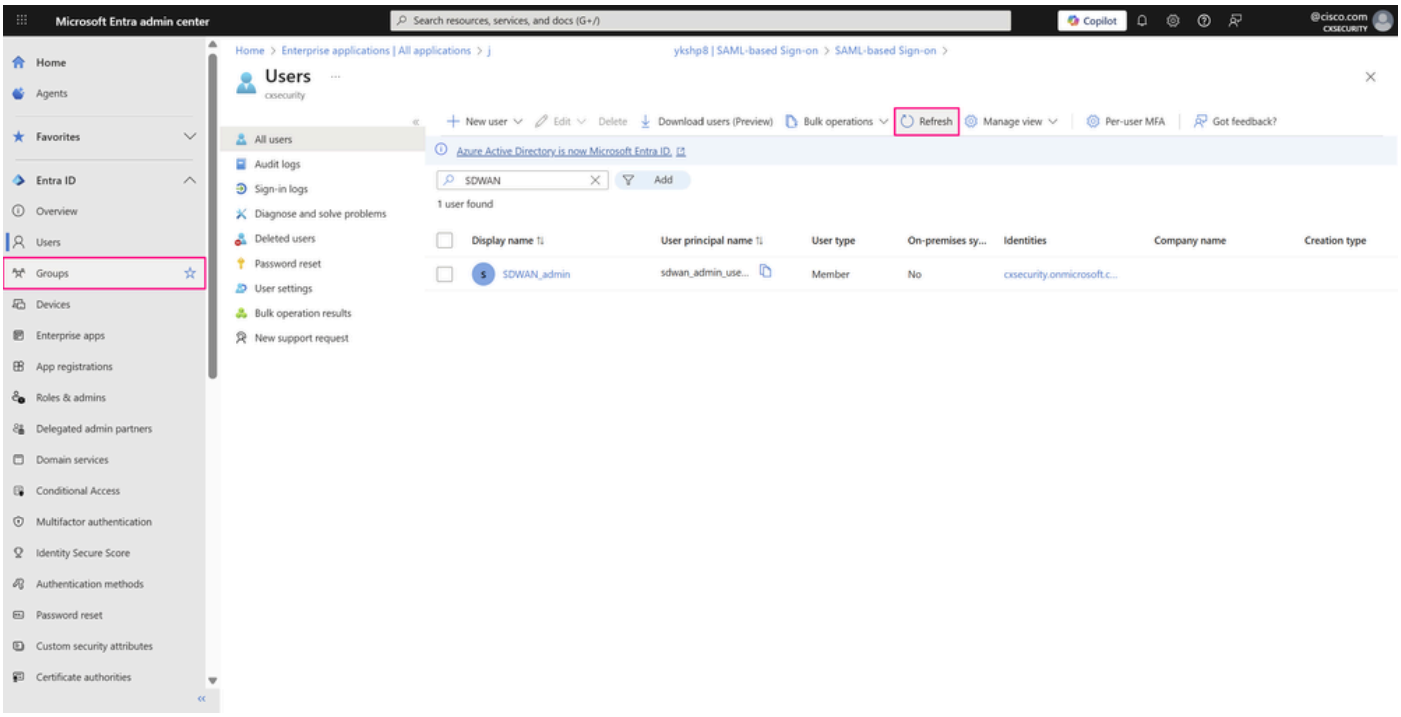
- 最後のタブには、ユーザ作成ワークフローのキーの詳細が表示されます。詳細を確認し、Createをクリックしてプロセスを完了します。



ユーザー作成ページ

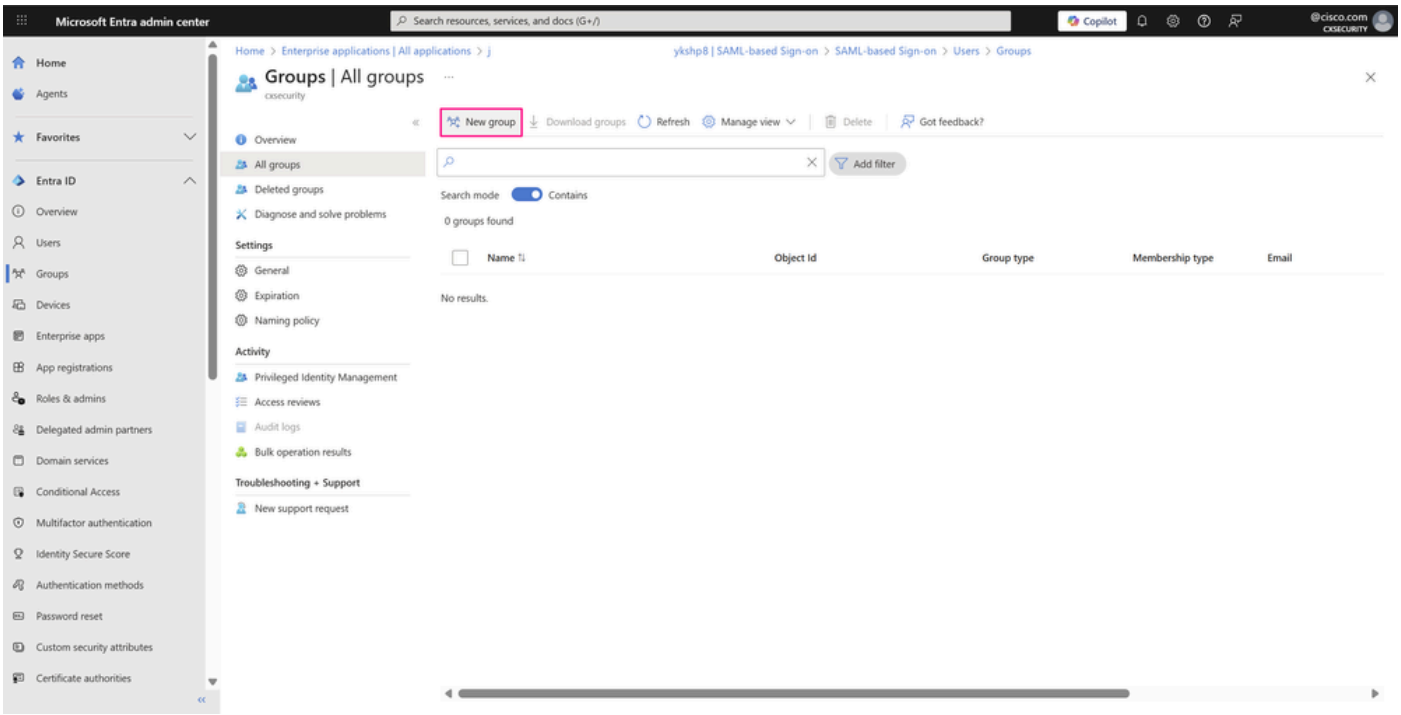
- 新しいユーザは、直後に表示されます。表示されていない場合は、Refreshをクリックし、

サービス内の検索バーを使用してユーザを検索します。次に、Entra ID > Groups > All groupsの順に移動して、新しいグループを作成します。



ユーザダッシュボード

- このページでは、組織内のさまざまなグループとその権限を管理します。 New groupをクリックして、ネットワーク管理者権限を持つグループを作成します。

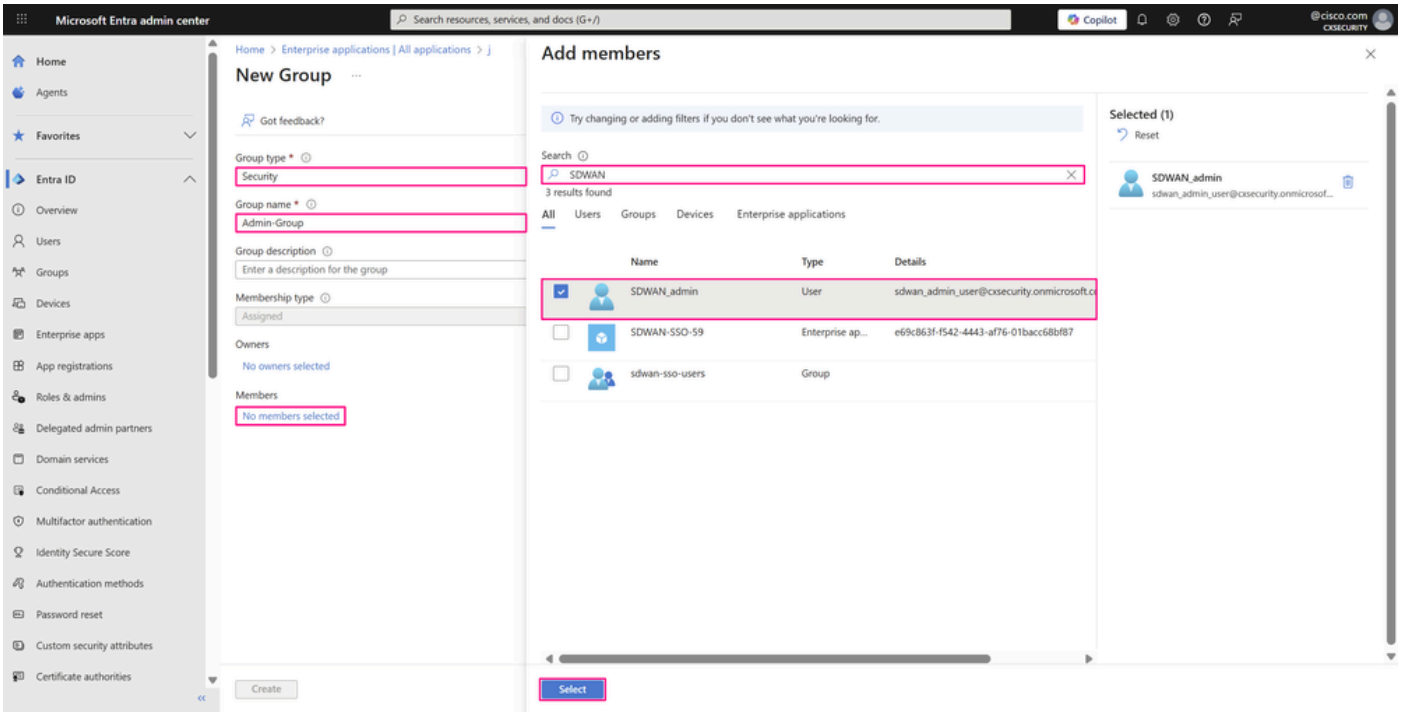


すべてのグループページ

- ドロップダウンリストからグループタイプを選択します。この場合、共有リソースへのアクセスのみが必要なので、セキュリティです。グループのロールまたは権限を参照する、任意のグループ名を入力します。この時点で、選択したメンバーを「メンバー」フィールドでク

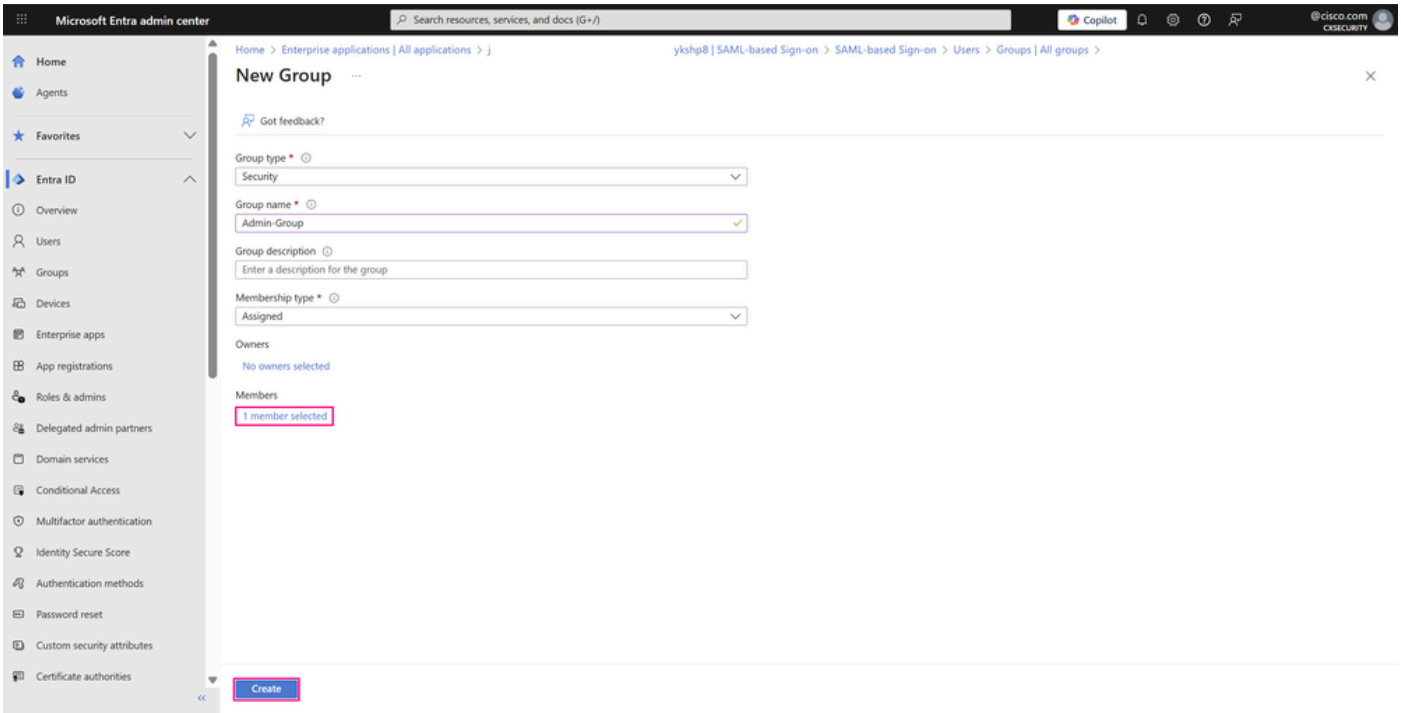
リックしたときに、ユーザーをグループに関連付けます。

- Add membersウィンドウで、追加するユーザ（この例では作成したばかりのユーザ）を参照して選択し、Selectをクリックします。



グループ作成ページ

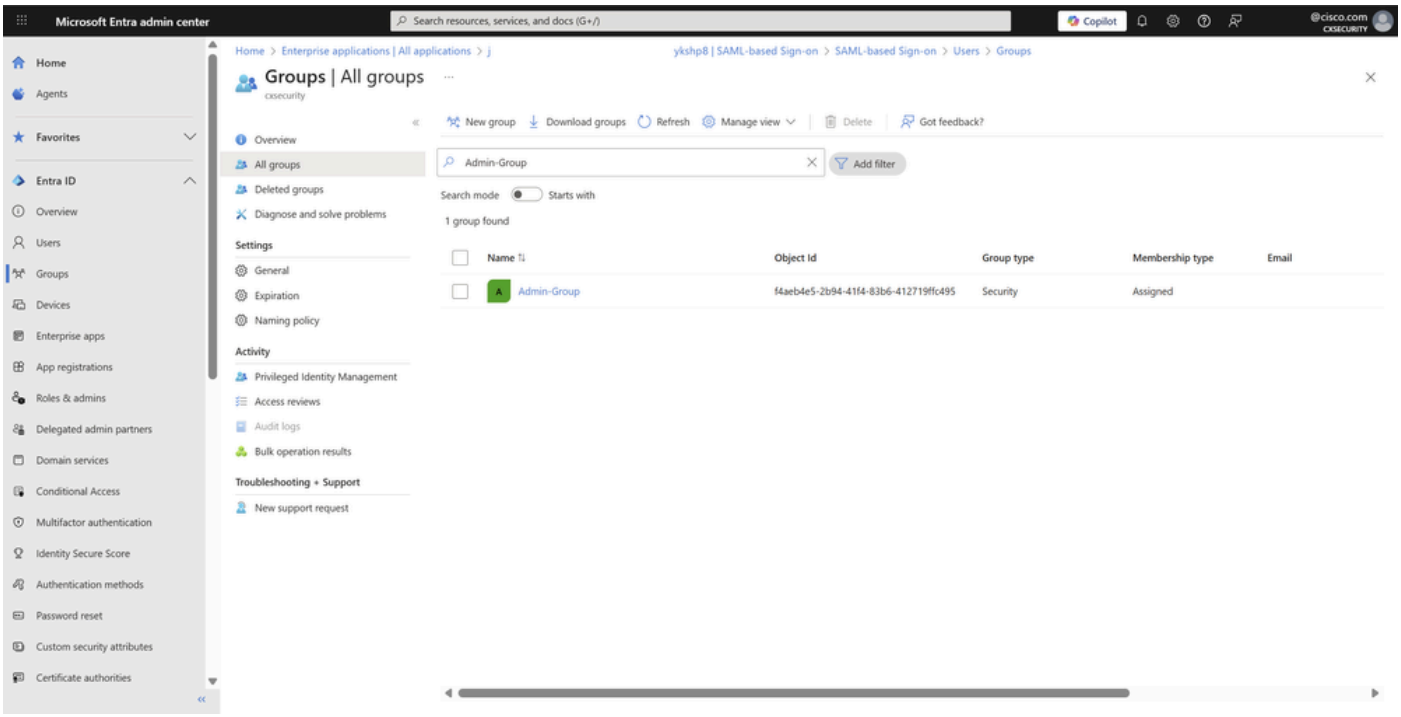
- Createをクリックして、グループを作成します。



グループ作成ページ

- 新しいグループは、直後に表示されます。表示されていない場合は、Refreshをクリックし、サービス内の検索バーでグループ名を検索します。 前の手順を繰り返して別のユーザを

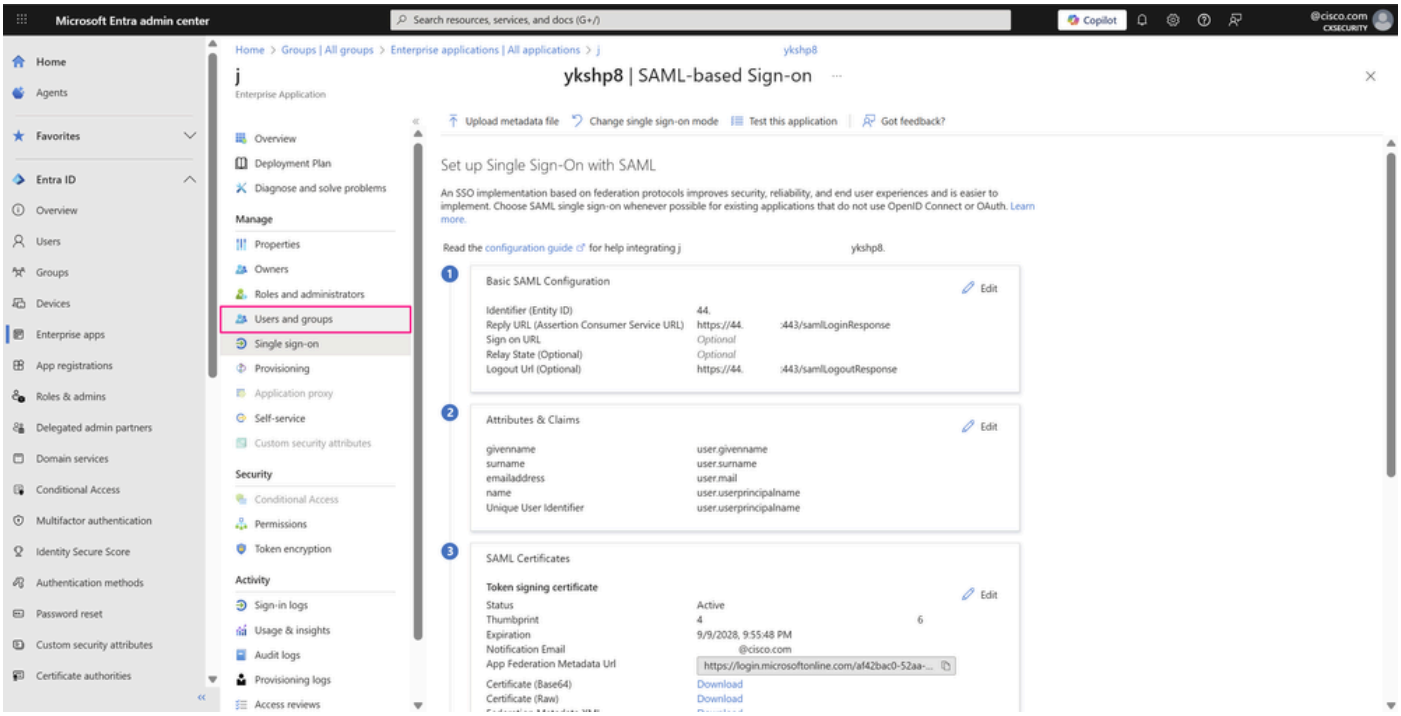
作成し、それを別のグループメンバーシップに追加して、アプリケーションおよびその他のユーザグループ（operatorなど）の1つでSSOサインインを検証します。



すべてのグループページ

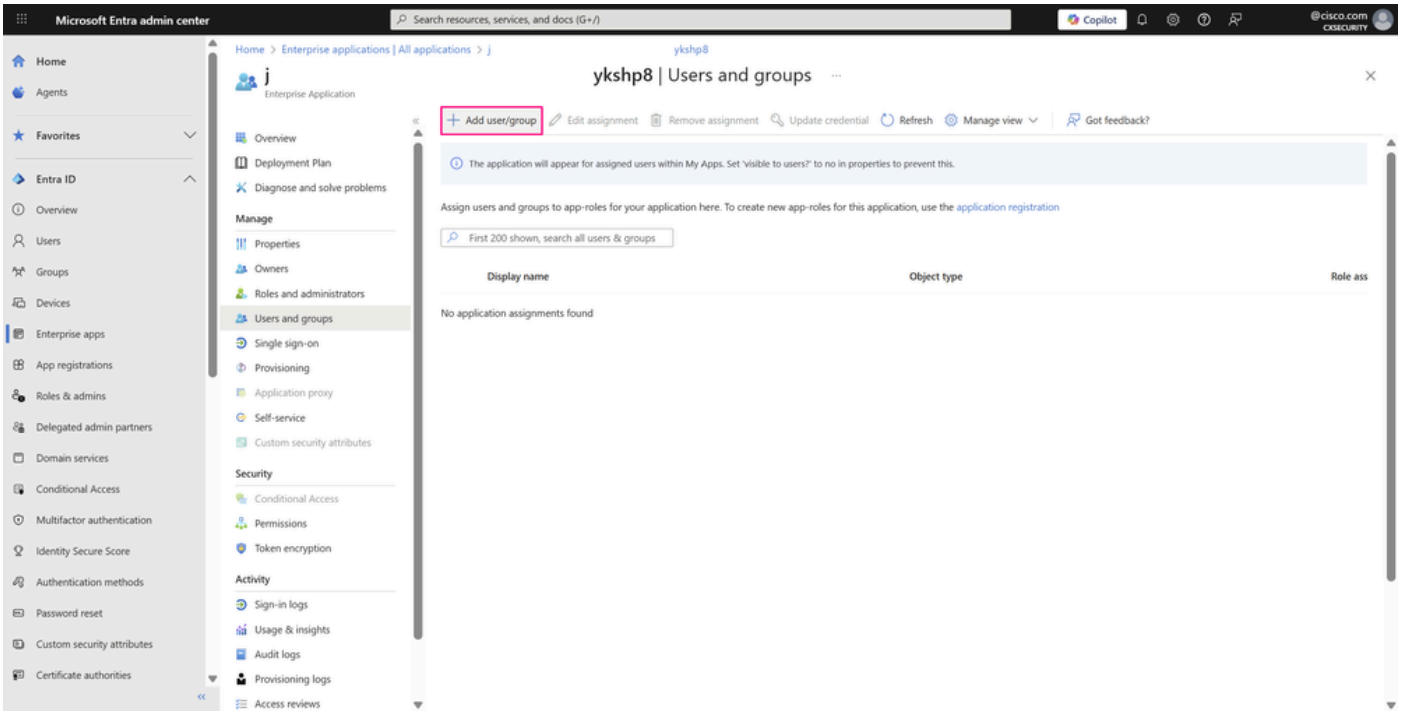
ステップ 4： Microsoft Entra IDのSAMLグループプロビジョニングの設定

- SAML設定でグループまたはグループに関連付けられたユーザをプロビジョニングするには、それらをエンタープライズアプリケーションに割り当て、アプリケーション（たとえばCisco SD-WAN Manager）のログイン権限を付与する必要があります。Entra ID > Enterprise appsの順に戻り、エンタープライズアプリケーションを開きます。左側のメニューのManageセクションで、Users and groupsをクリックします。



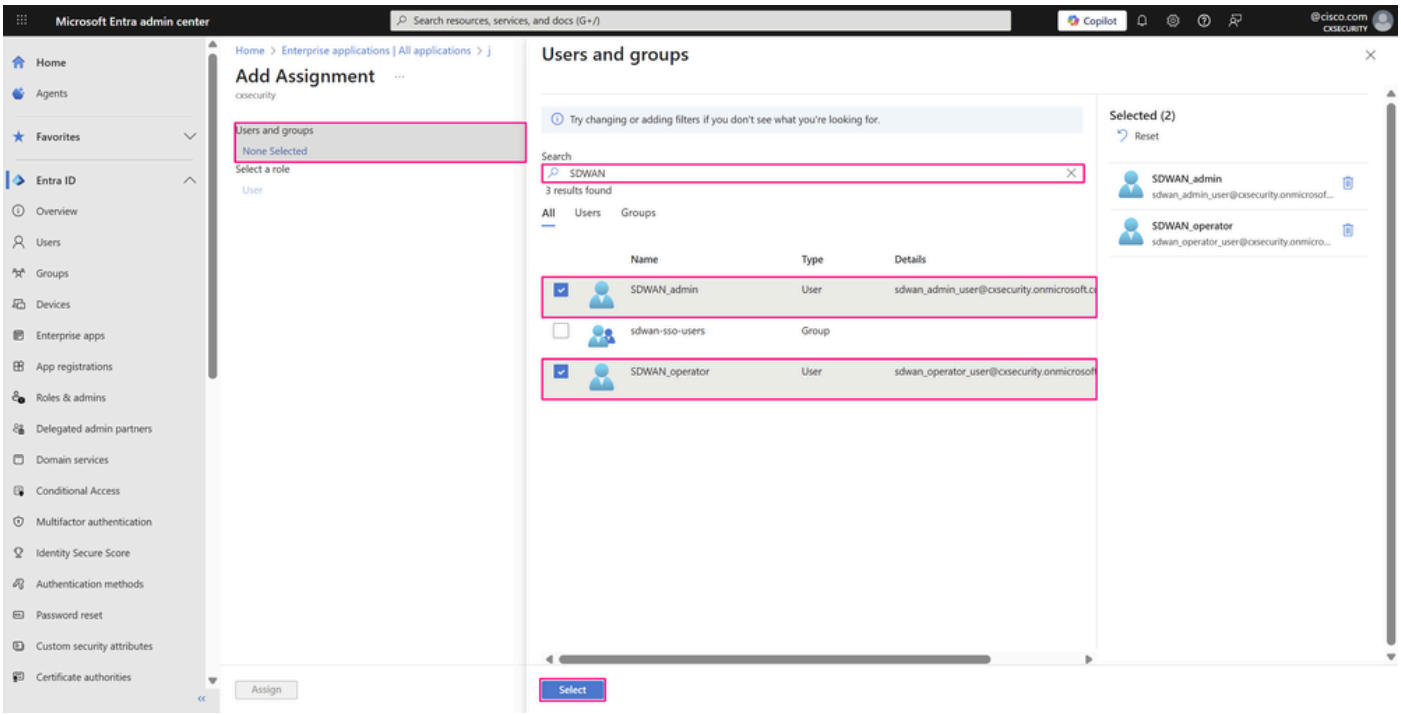
SAML設定を使用したSSOのページ

- 次に、Add user/groupをクリックします。



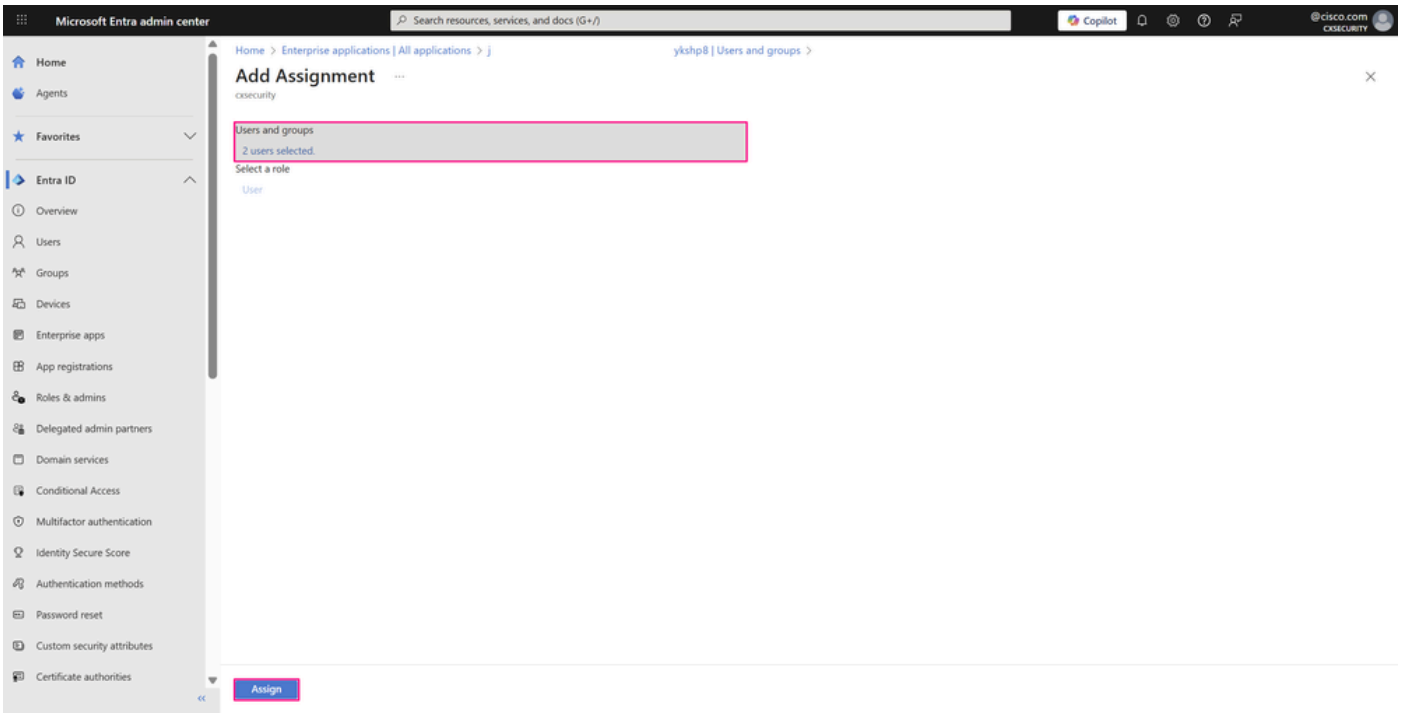
「ユーザーとグループ」ページ

- Add Assignmentペインで、Users and groupsフィールドの下にあるNone Selectedをクリックします。アプリケーションに割り当てるユーザまたはグループ（この例では、前のステップで作成した2人のユーザ）を検索して選択し、Selectをクリックします。



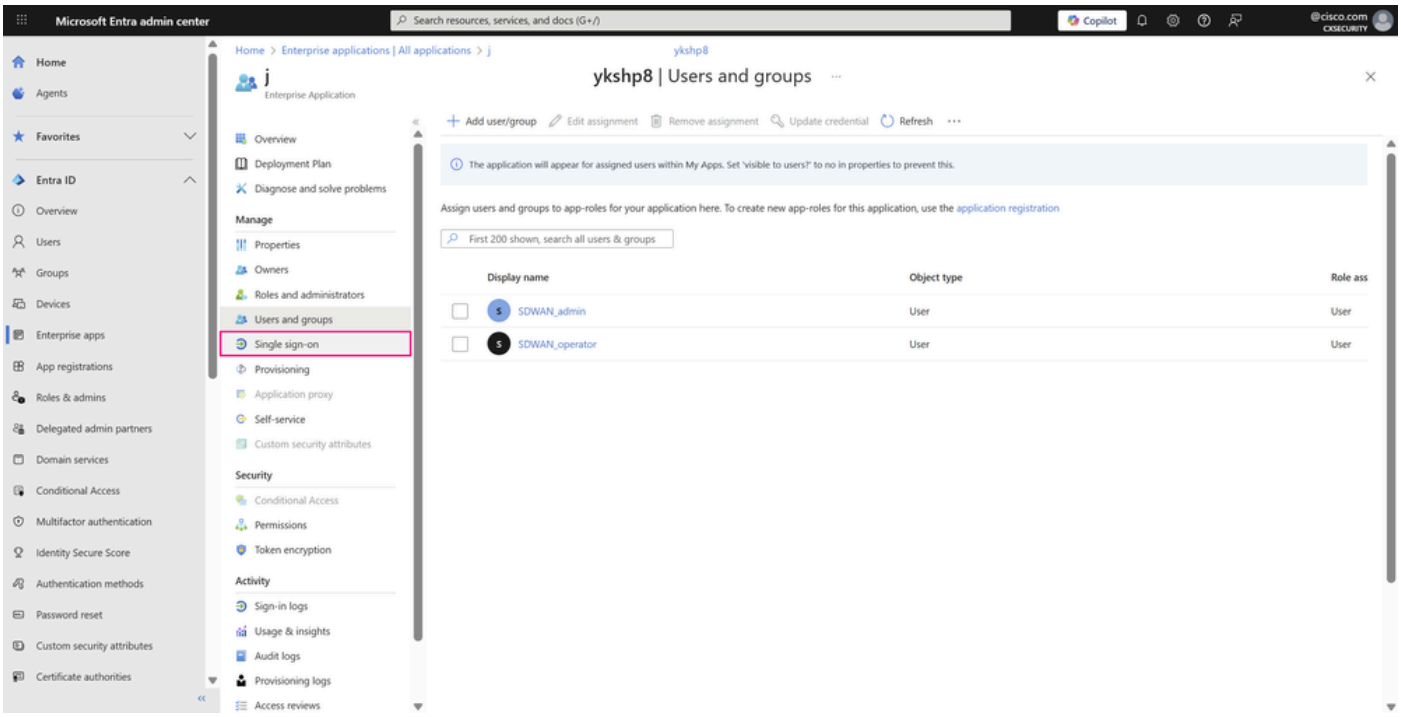
[ユーザー/グループの割り当て]ウィンドウ

- Assignをクリックして、ユーザまたはグループをアプリケーションに割り当てます。



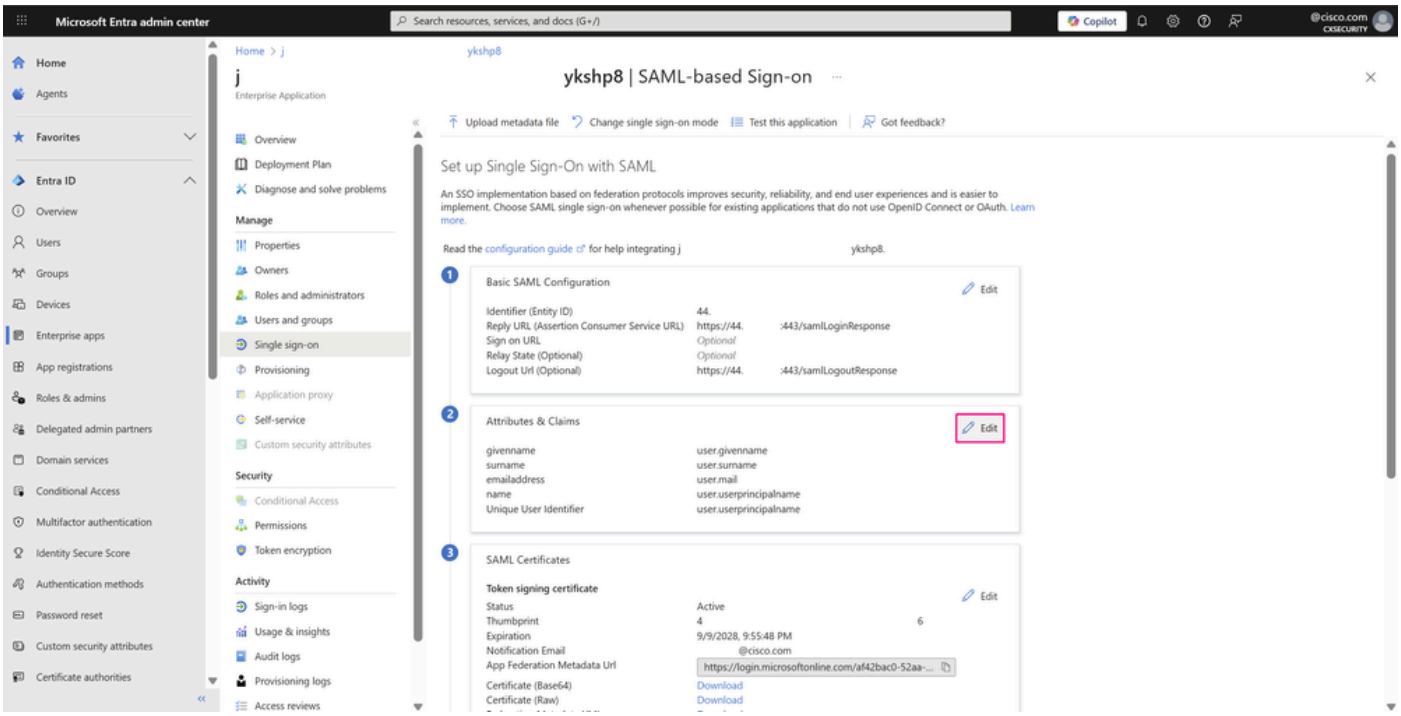
[ユーザー/グループの割り当て]ウィンドウ

- エンタープライズアプリケーションに割り当てられたユーザは、割り当ての直後に一覧表示されます。左側のメニューのManageセクションにあるSingle sign-onをクリックして、アプリケーションのSSO SAML設定にアクセスし、残りの必要な設定を完了します。



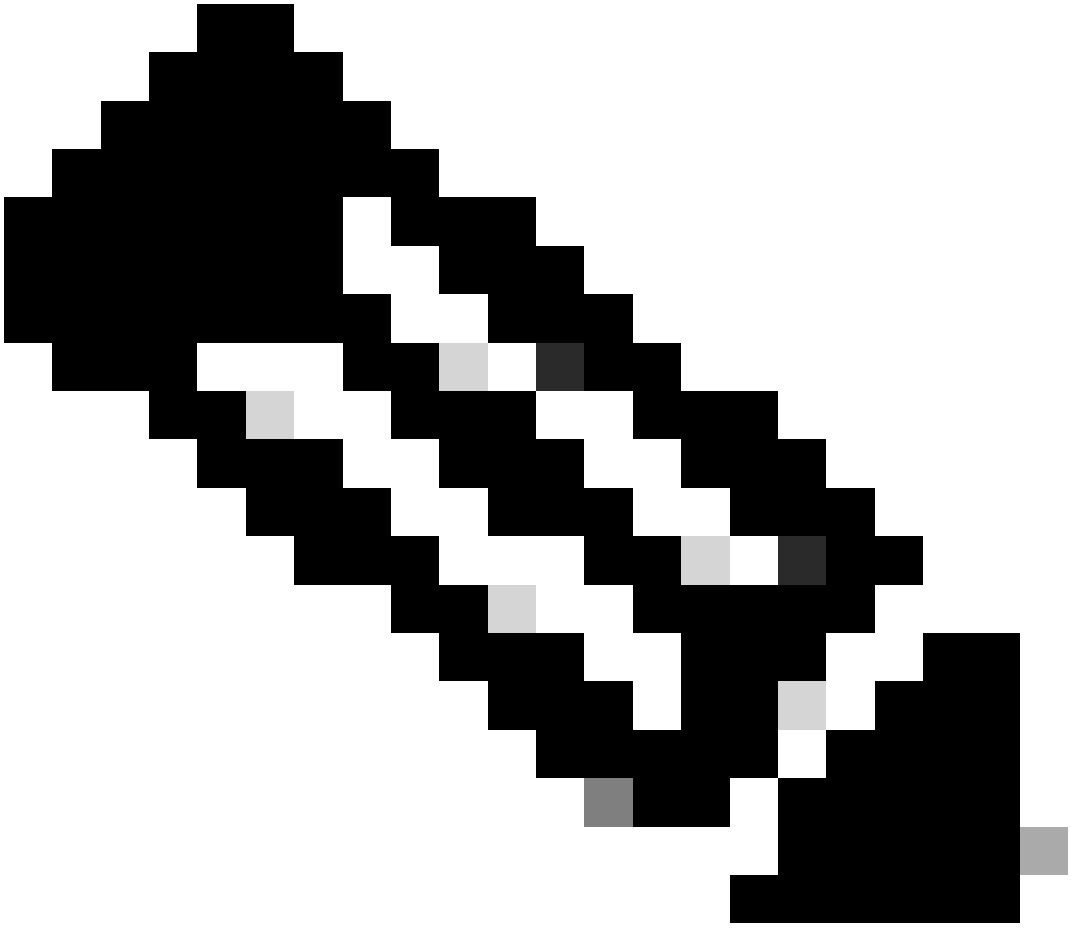
「ユーザーとグループ」ページ

- Set up Single Sign-On with SAMLページで、Attributes & Claimsの下にあるEditをクリックします。

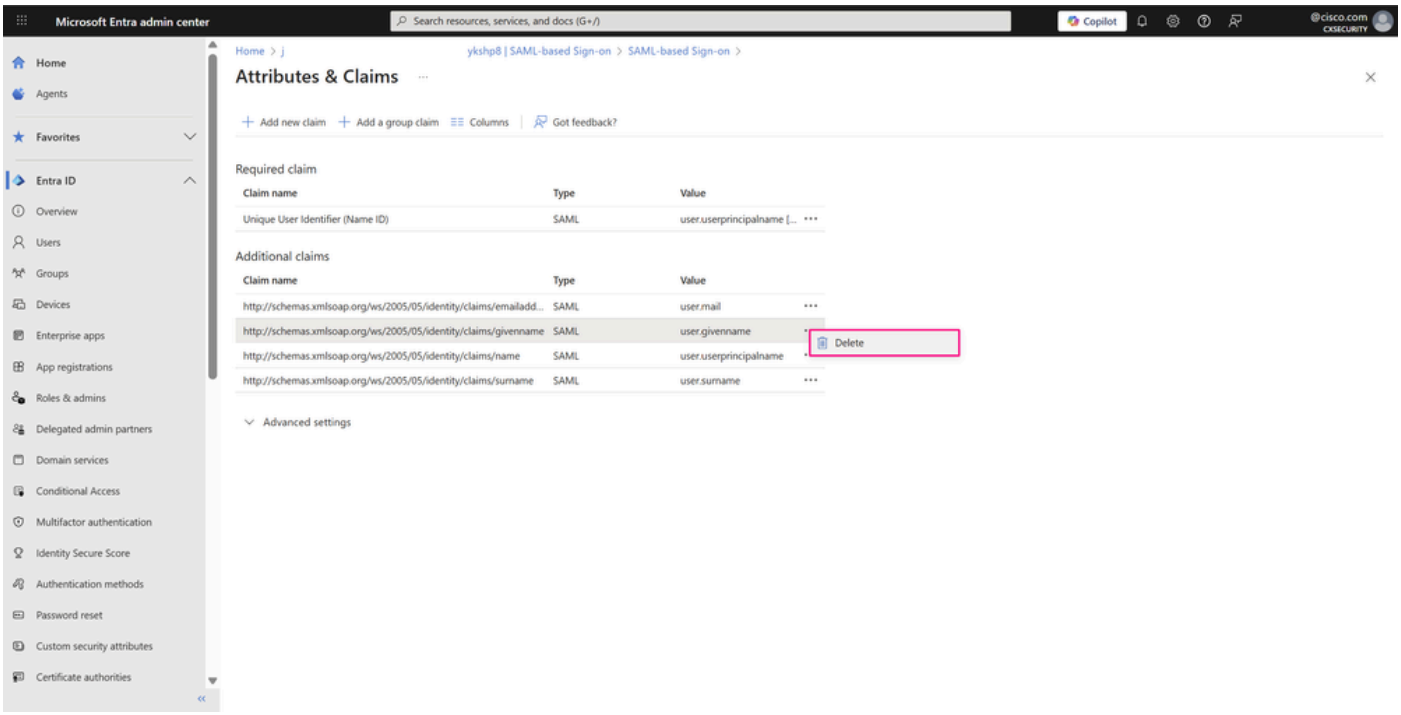


SAML設定を使用したSSOのページ

- [属性と要求]ページで、3つのドットのアイコンをクリックしてから[削除]をクリックし、値がuser.givennameの要求と値がuser.surnameの要求を、この例では必要ないので削除します。アプリケーションとの基本的なSSO認証には、次の要求のみが必要です。
    - ユーザ-user.mailの電子メールアドレス
    - ユーザ-user.userprincipalnameのユーザプリンシパル名(UPN)

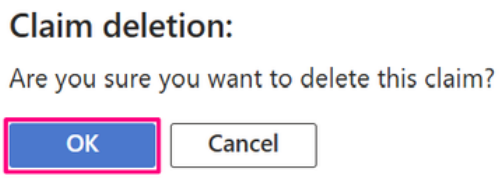


注：組織では、固有のニーズに応じて追加の請求が必要な場合があります。



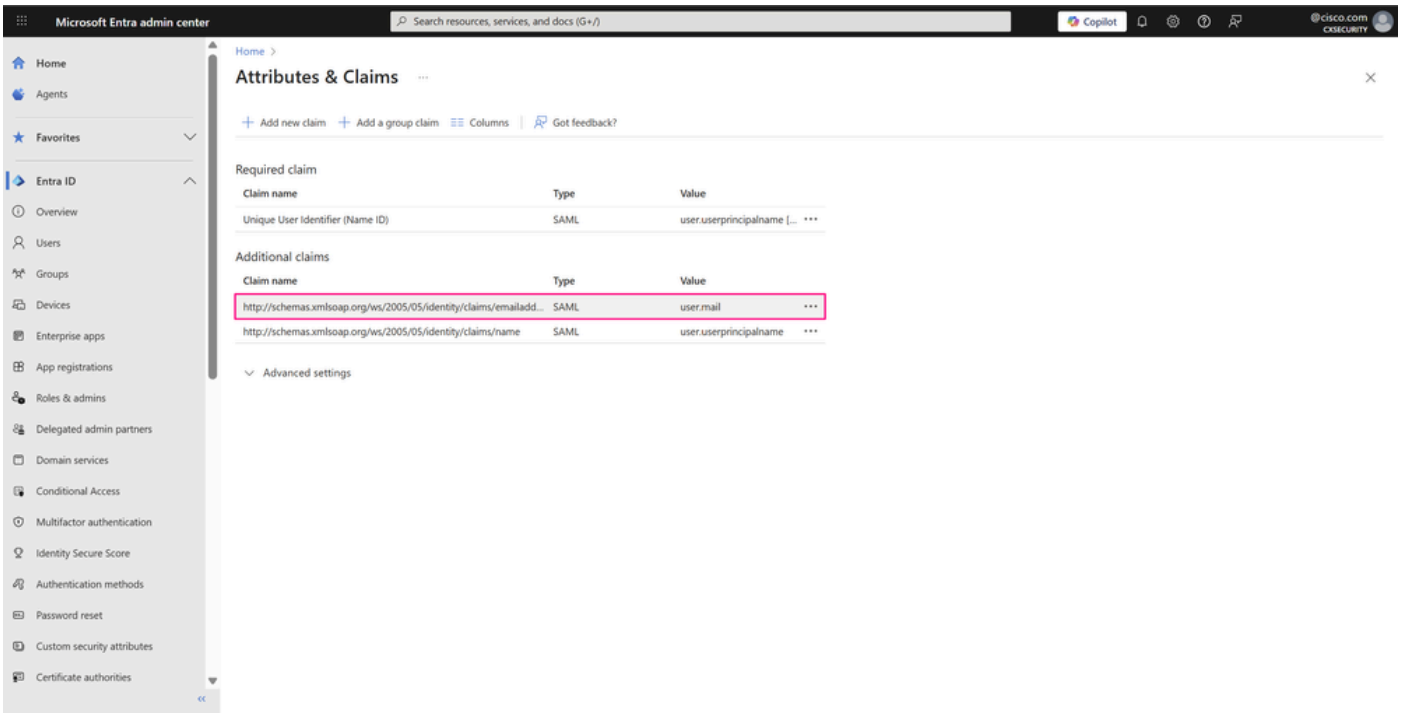
「属性および要求」ページ

- Claim deletionウィンドウで、OKをクリックしてクレームを削除します。



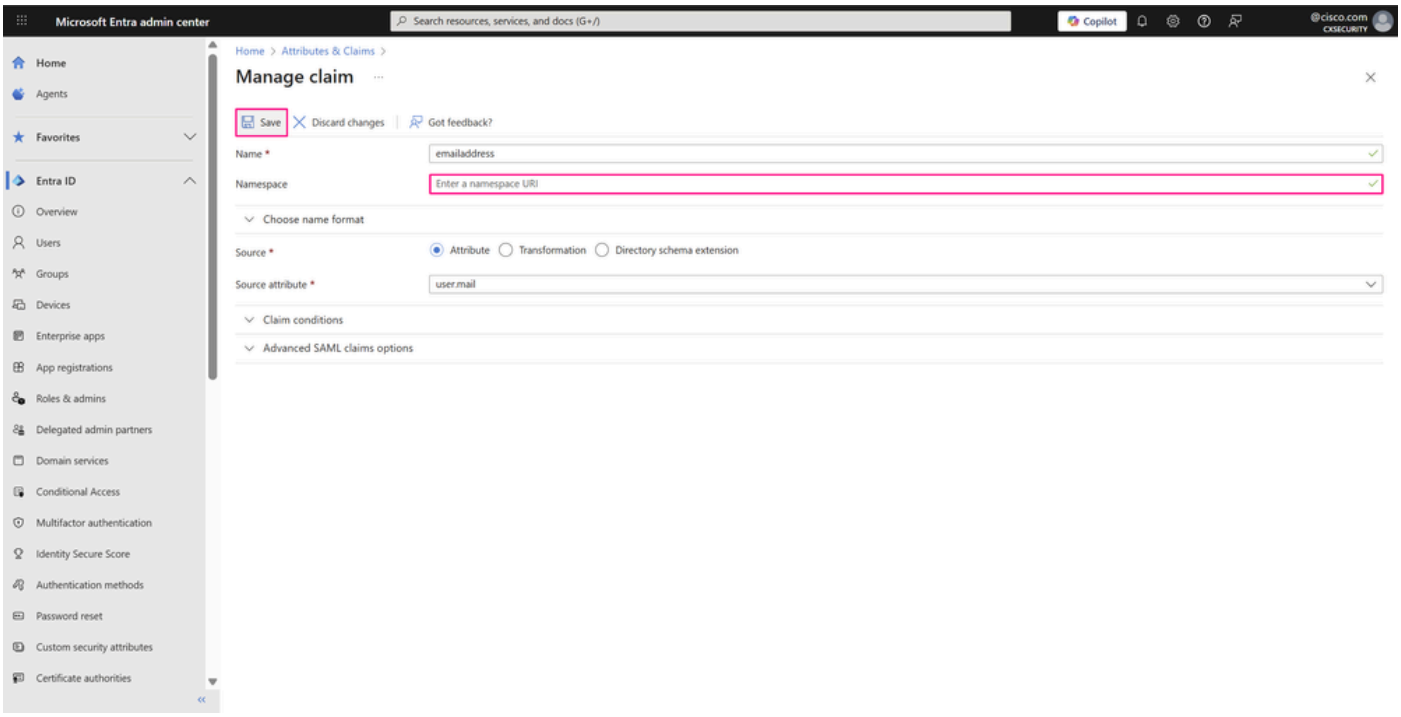
「要求の削除」ウィンドウ

- 次に、このフィールドはオプションであるため、残りの2つの要求の要求名から名前空間を削除します。この変更により、各の実際の名前がこのページに表示され、識別しやすくなります。各請求にカーソルを合わせてクリックすると、その設定にアクセスできます。



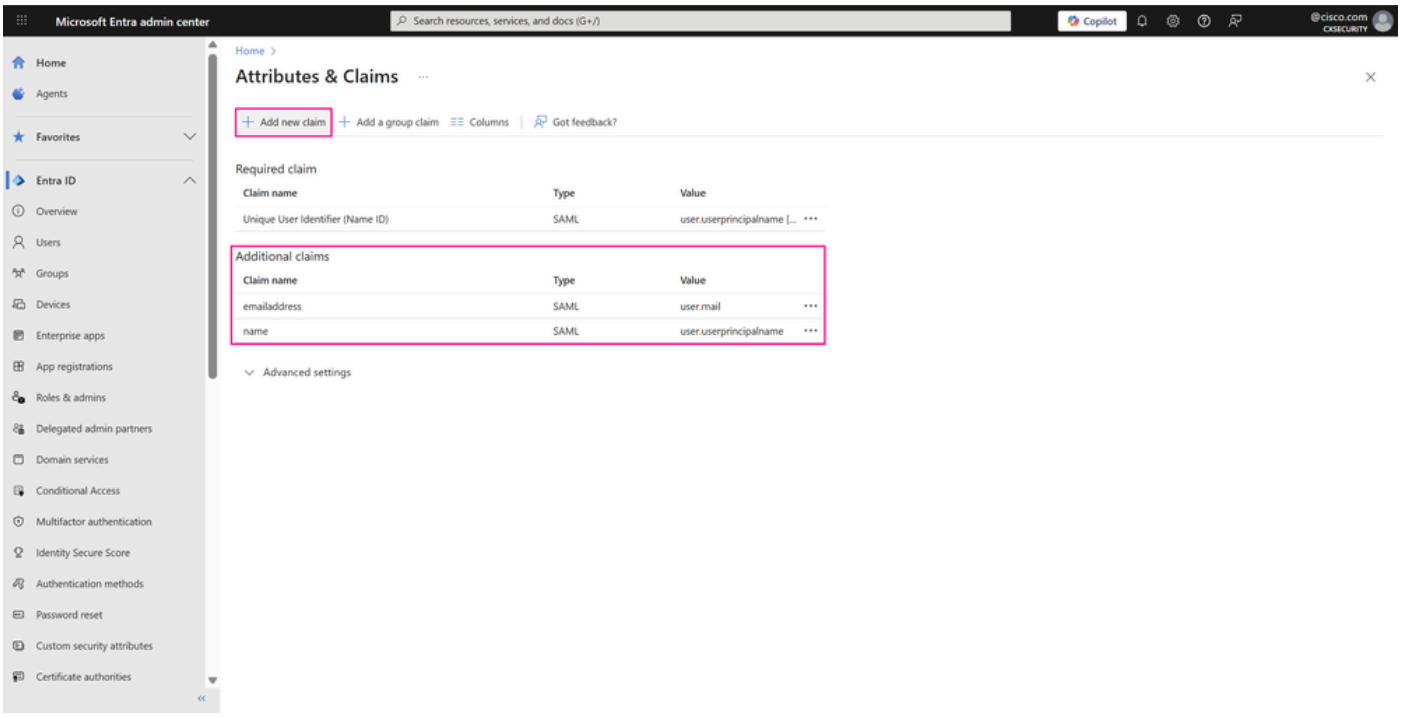
「属性および要求」ページ

- Manage claimページで、Namespaceフィールドを削除し、Saveをクリックして変更を適用します。



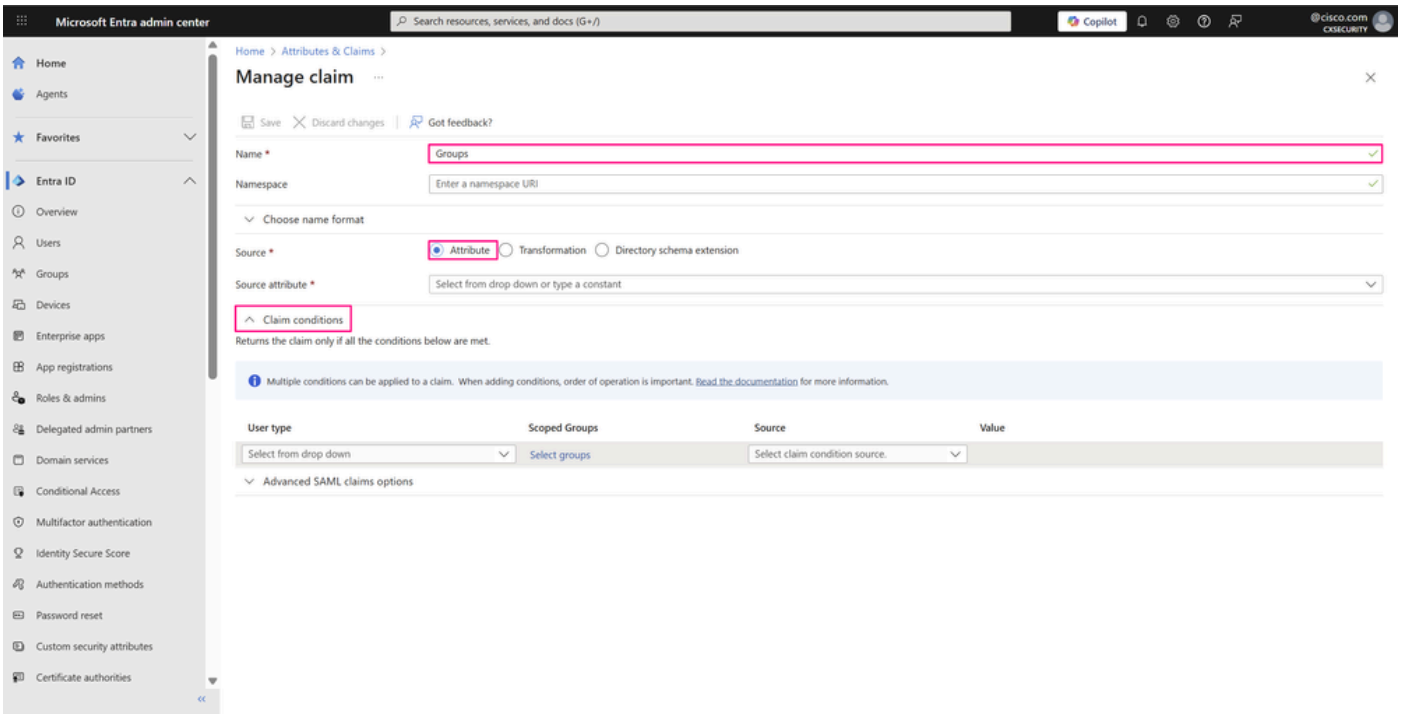
請求の管理ページ

- 必要な2つの要求の名前が表示されます。ただし、ユーザが属し、アプリケーションリソースにアクセスする権限を持つグループを定義するには、さらに1つの要求が必要です。これを行うには、[新しい要求の追加]をクリックします。



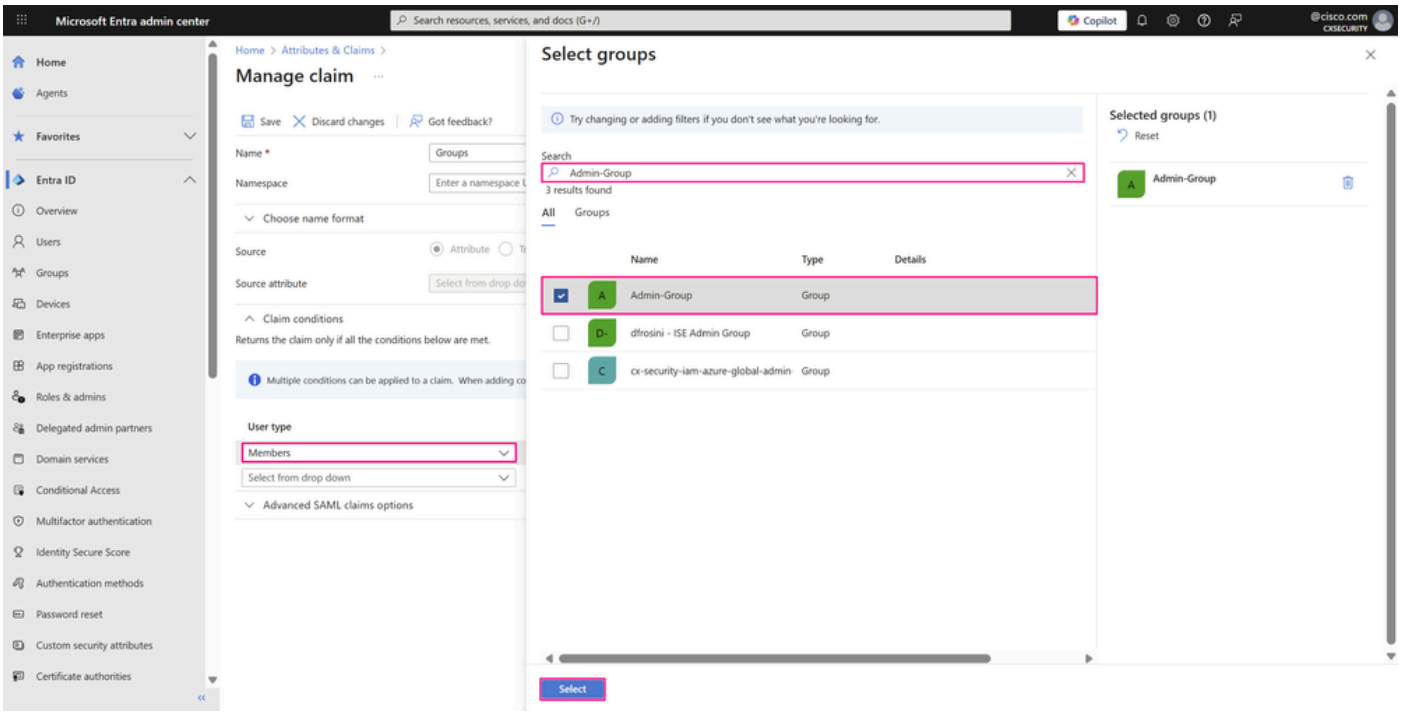
「属性および要求」ページ

- この請求を識別する名前を入力します。Sourceの横にあるAttributeを選択します。次に、クレーム条件をクリックしてオプションを展開し、複数の条件を設定します。



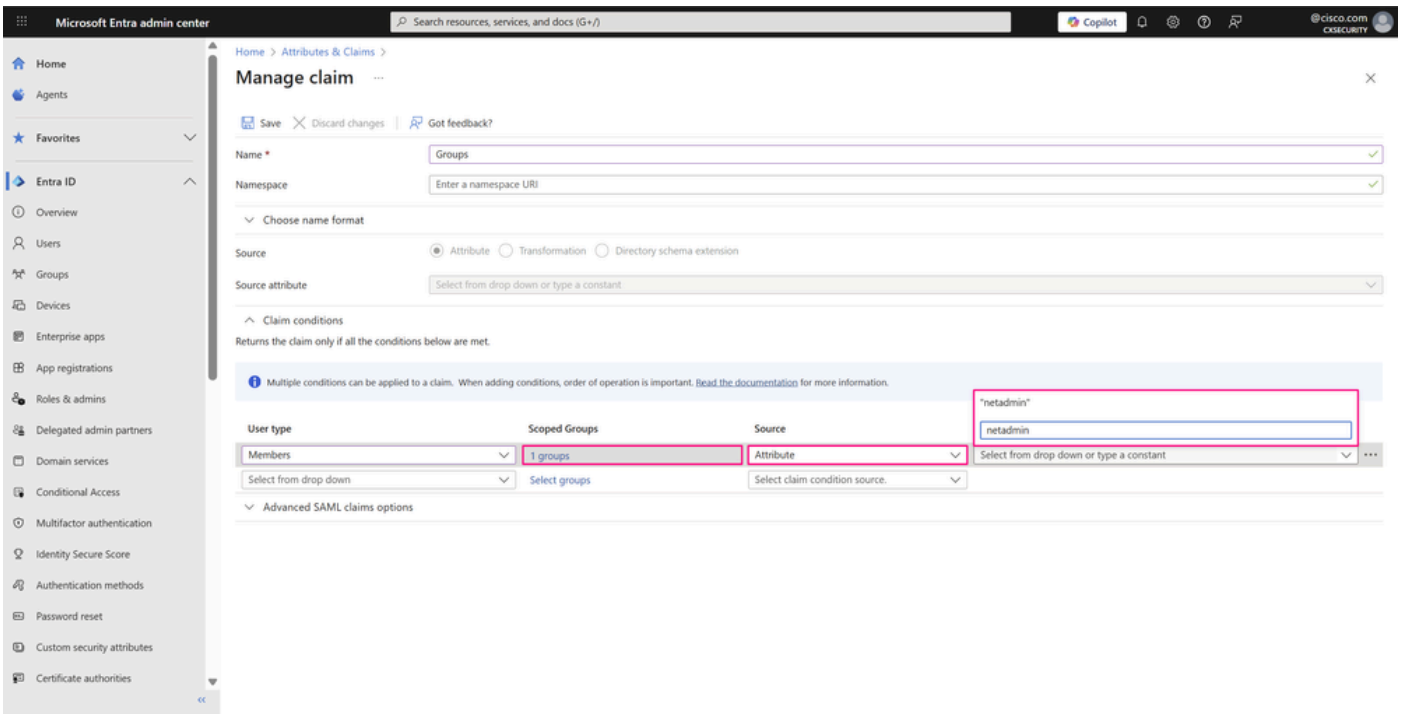
請求の管理ページ

- クレーム条件で、User typeドロップダウンリストからMembersを選択し、Select Groupsをクリックしてユーザが属する必要があるグループを選択し、Selectをクリックします。



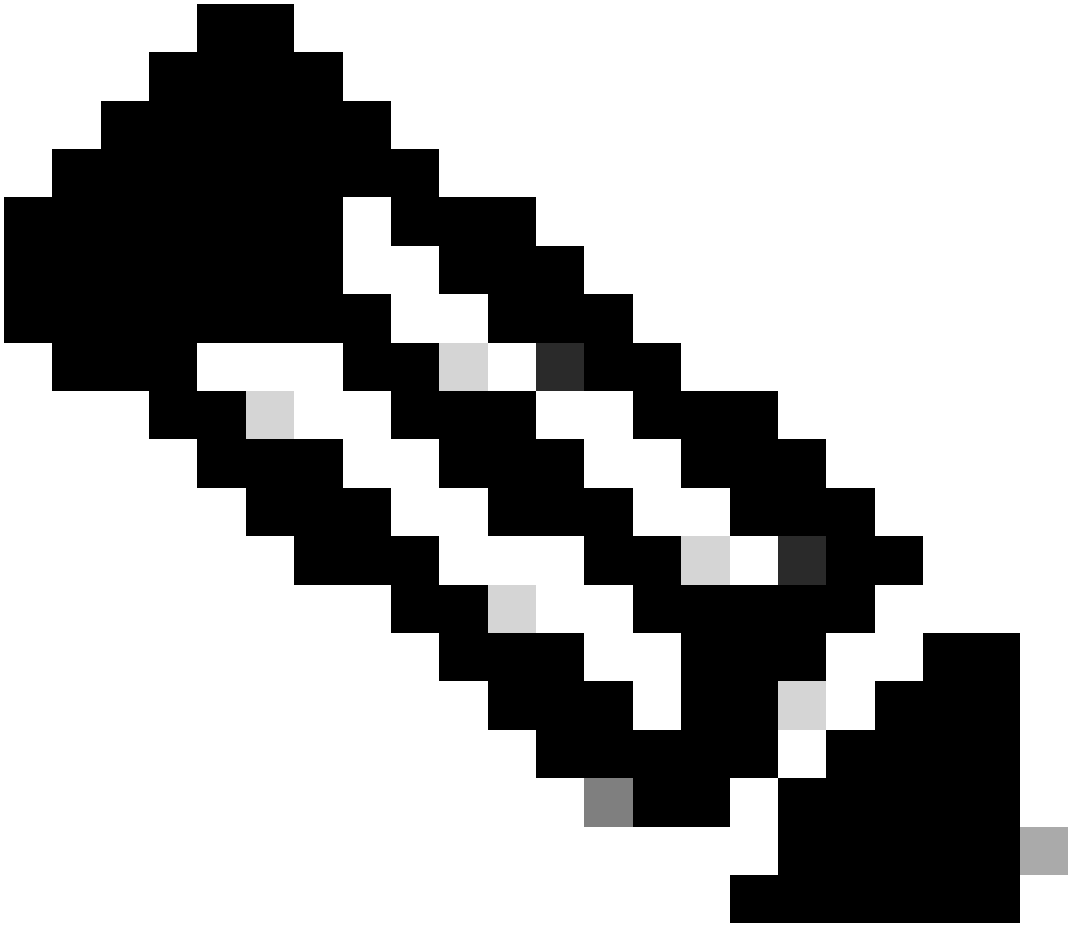
請求の管理ページ

- クレームが値を取得するSourceドロップダウンリストからAttributeを選択します。Valueフィールドに、アプリケーションで定義されたユーザグループを参照するユーザのcustom属性を入力します。この例では、netadminはCisco SD-WAN Managerの標準ユーザグループの1つです。 属性値を引用符なしで入力し、Enterキーを押します。

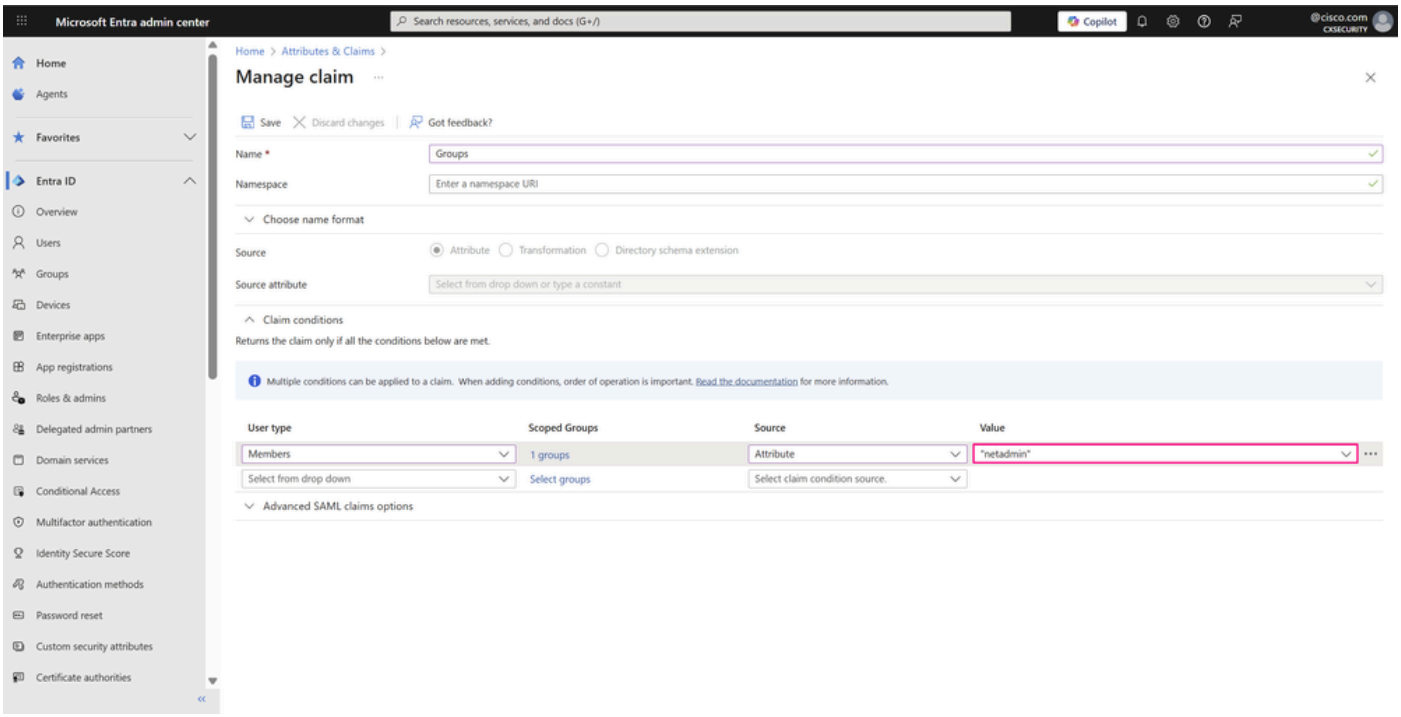


請求の管理ページ

- その直後に、属性値が引用符で囲まれて表示されます。これは、Microsoft Entra IDがこの値を文字列として処理するためです。

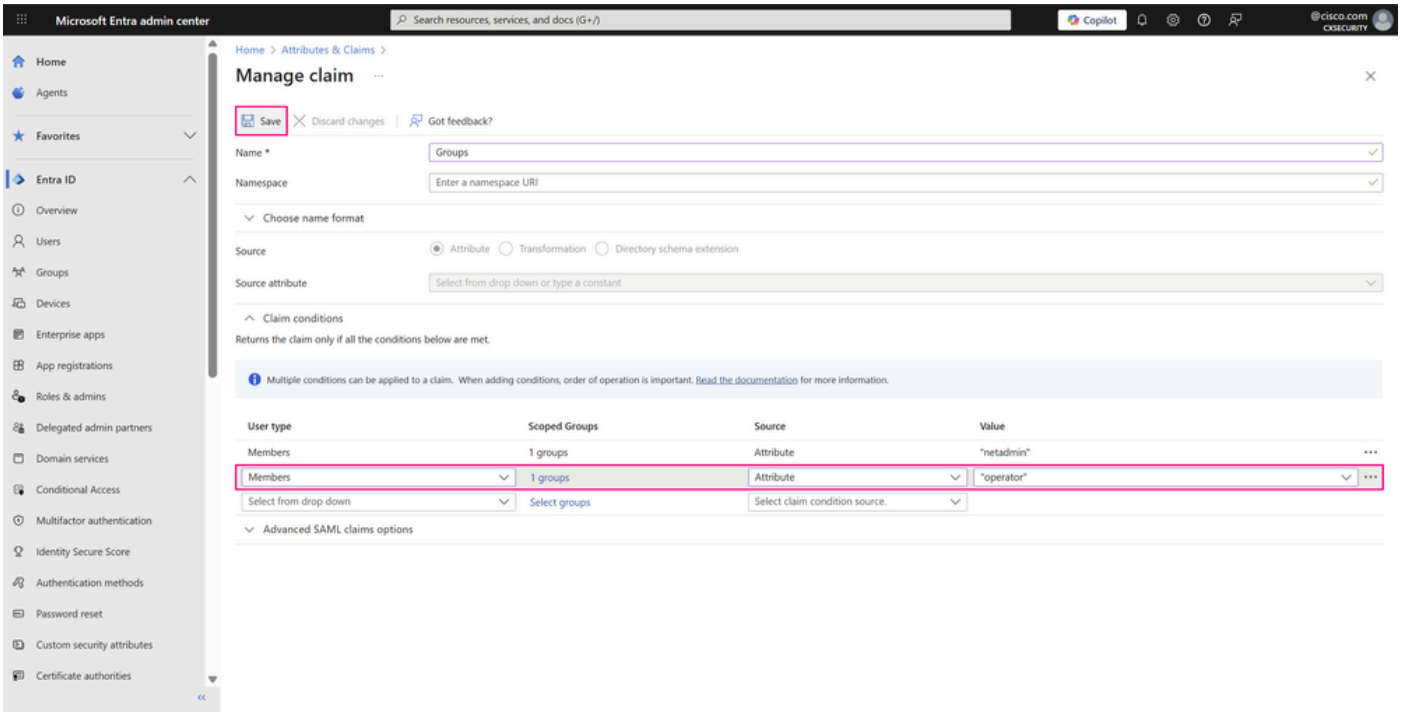


注：請求条件内のこれらのパラメータは、エンタープライズアプリケーションのSSO SAML設定において大きな関連性を持ちます。これらのカスタム属性は、常にCisco SD-WAN Managerで定義されたユーザグループと一致する必要があるためです。この照合により、ユーザがMicrosoft Entra IDに属するグループに基づいて、ユーザに付与される権限が決まります。



請求の管理ページ

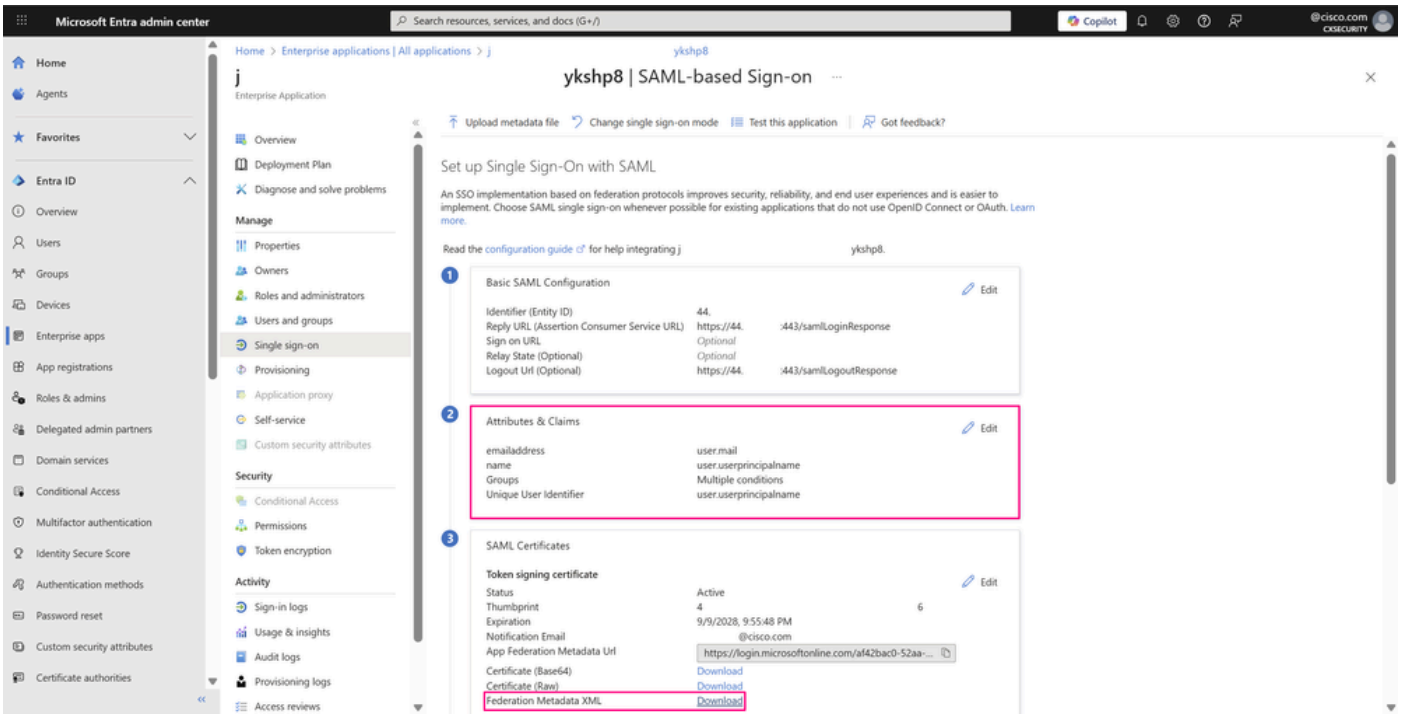
- Cisco SD-WAN Managerでoperatorユーザグループにマッピングされる2番目に作成されるグループの2番目の要求条件に対して、同じ手順を繰り返します。このプロセスは、アプリケーションにサインインする特定の権限を持つグループごとに必要です。1つの条件に複数のグループを追加することもできます。Saveをクリックして、変更を保存します。



請求の管理ページ

- Set up Single Sign-On with SAMLページで、Attributes & Claimsセクションに新しく加えられた変更が表示されます。Microsoft Entra IDで設定を完了するには、SAML Certificatesの下で、Federation Metadata XMLの横にあるDownloadをクリックし、アプリケーションにアイ

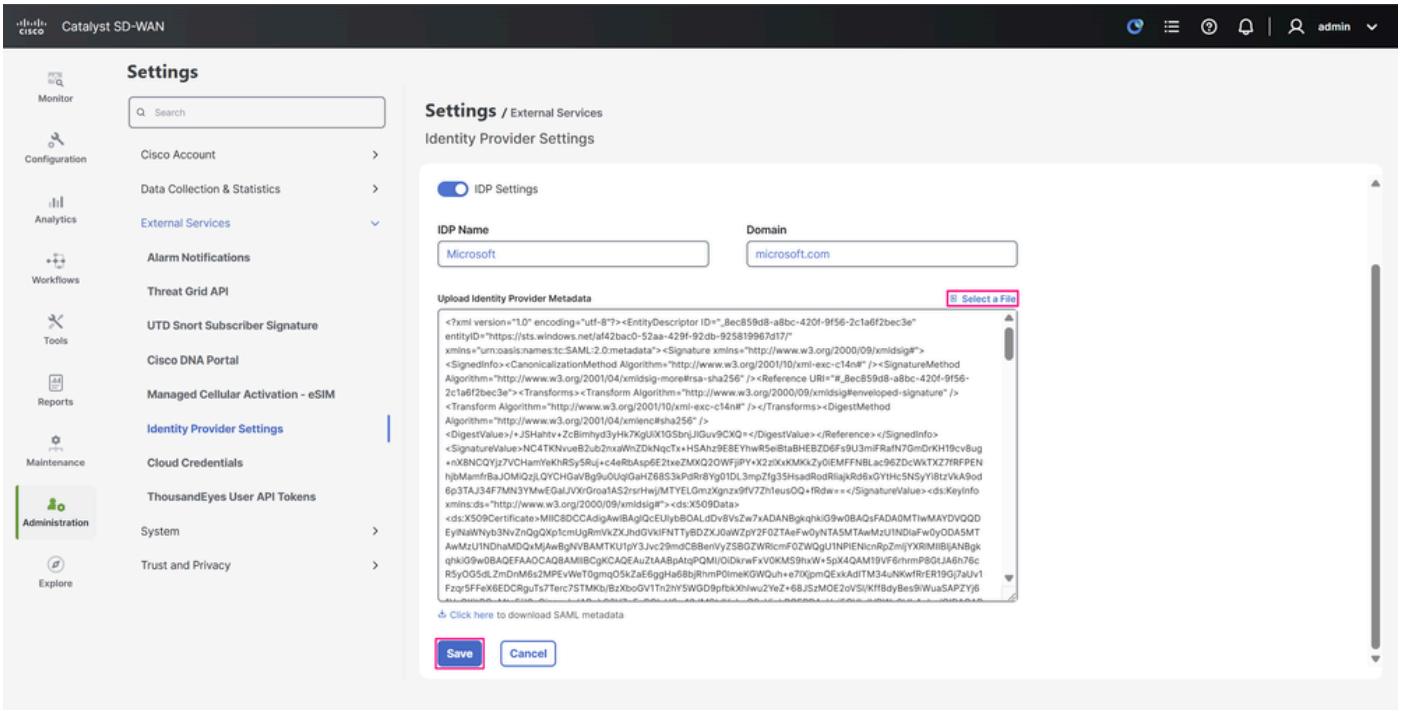
デンティティサービスを提供するXMLファイルをダウンロードします。



SAML設定を使用したSSOのページ

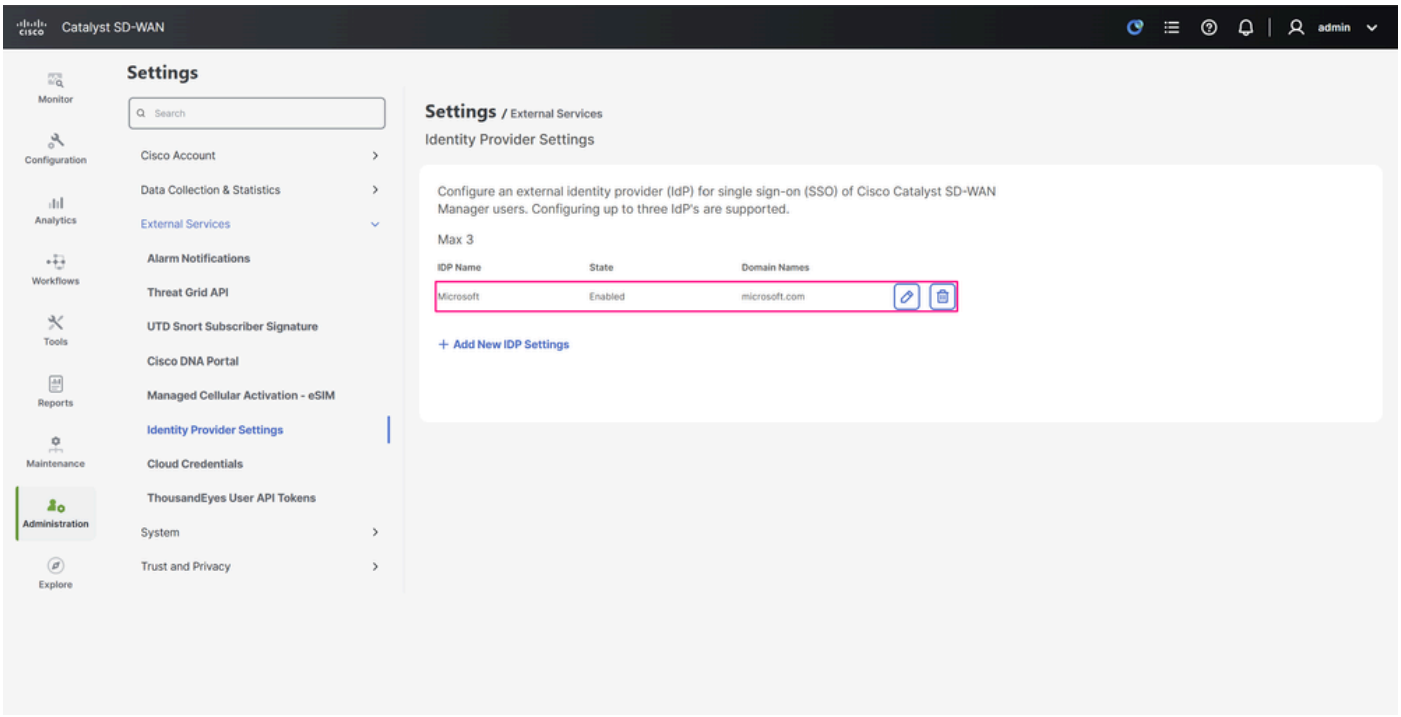
ステップ 5： Microsoft Entra ID SAMLメタデータファイルのCisco SD-WAN Managerへのインポート

- フェデレーションメタデータをCisco SD-WAN Managerにアップロードするには、Administration > Settings > External Services > Identity Provider Settingsの順に移動し、Select a fileをクリックします。Microsoft Entra IDからダウンロードしたファイルを選択し、Saveをクリックします。



IdP Settings Configurationページ

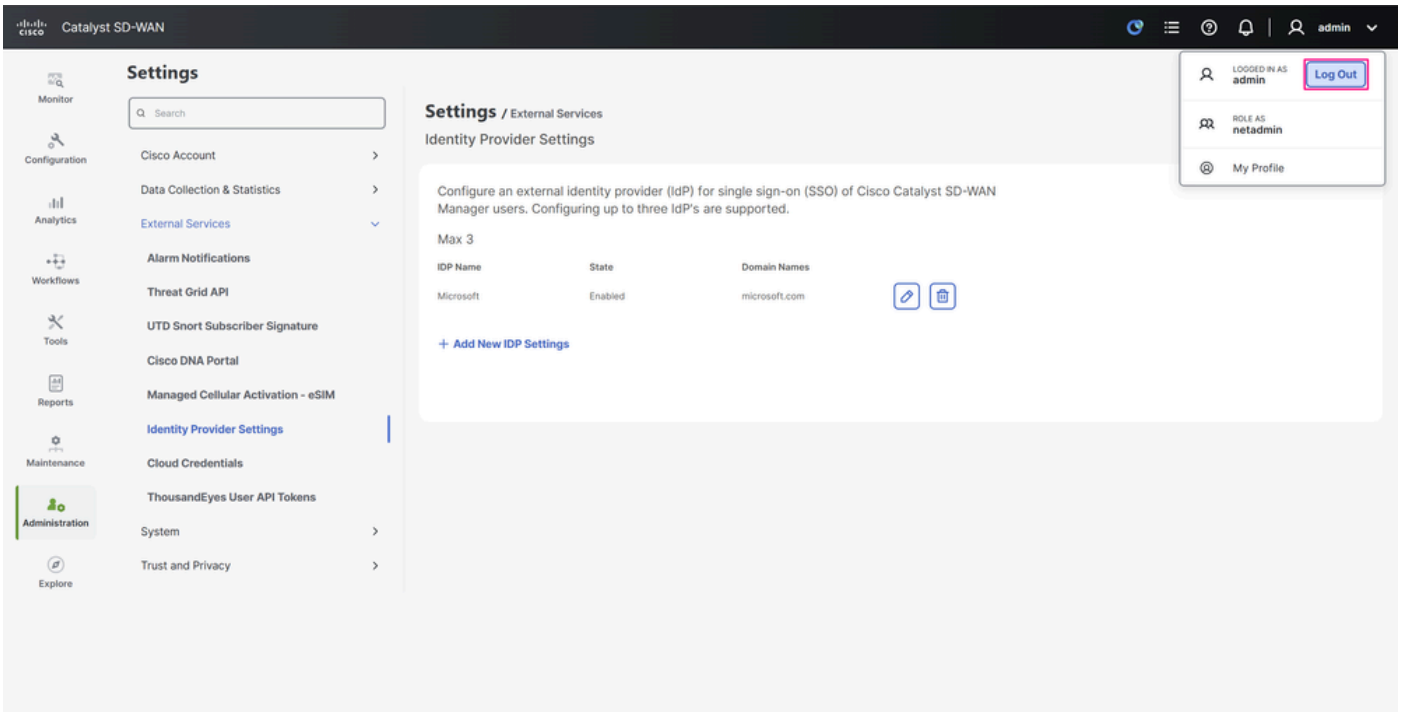
- IdP設定とメタデータが保存されました。



IdP Settings Configurationページ

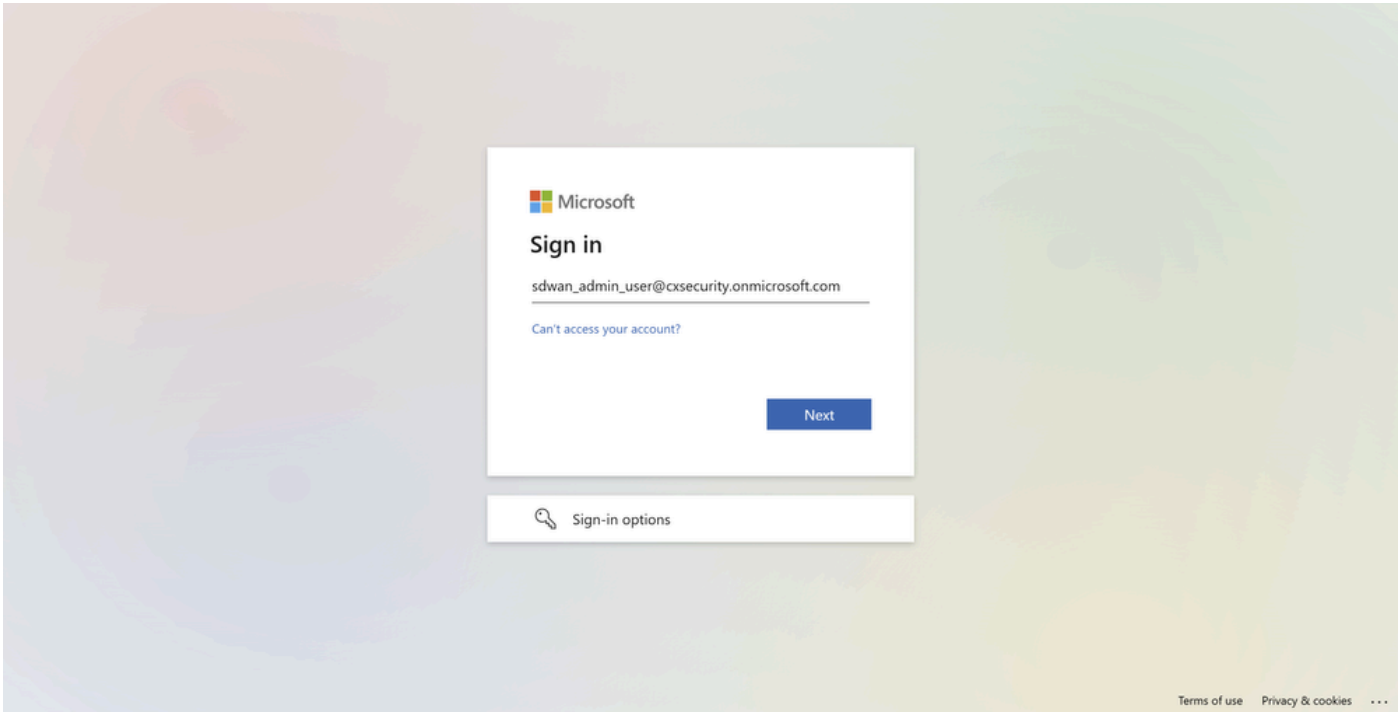
確認

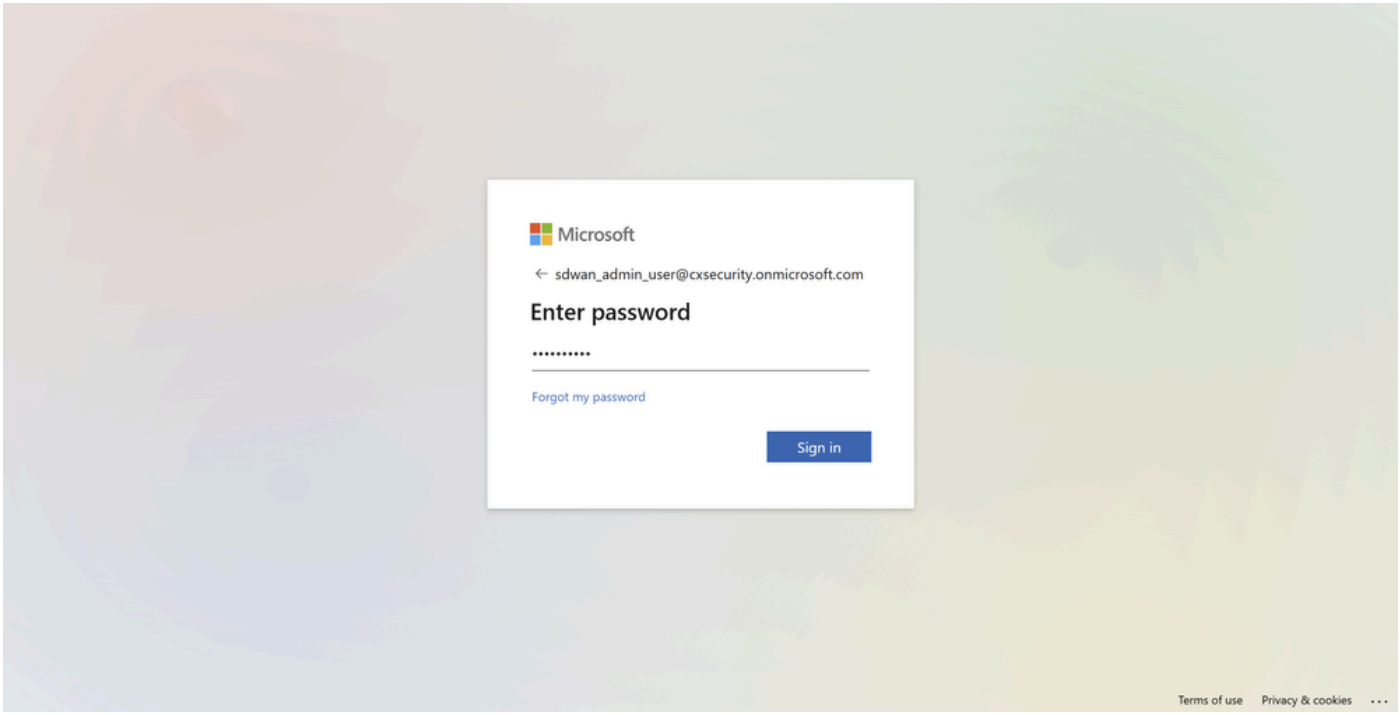
- UIの右上隅にあるプロファイル名をクリックしてオプションを展開し、そこからログアウトをクリックしてポータルをログアウトします。



プロファイルメニュー

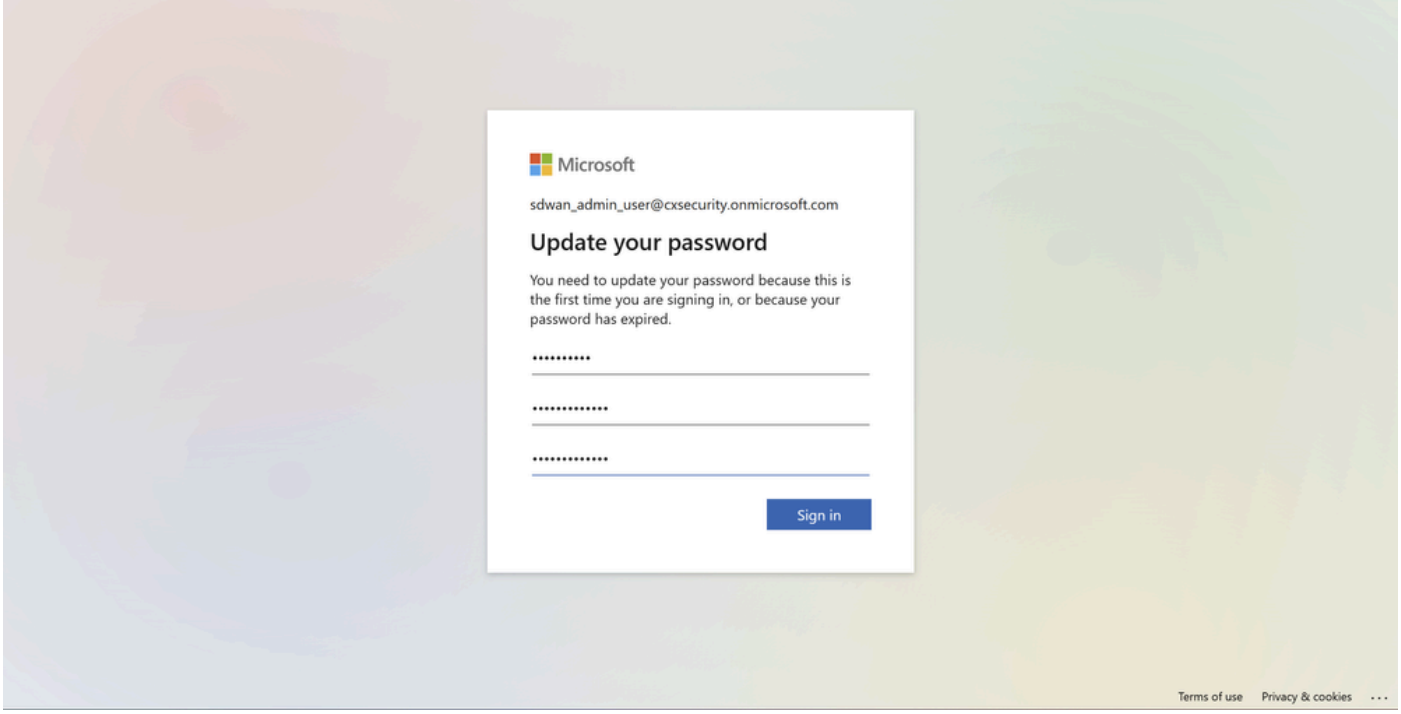
- すぐにMicrosoft認証画面にリダイレクトされます。この画面で、Microsoft Entra ID SSOユーザのクレデンシャルを使用してサインインします。





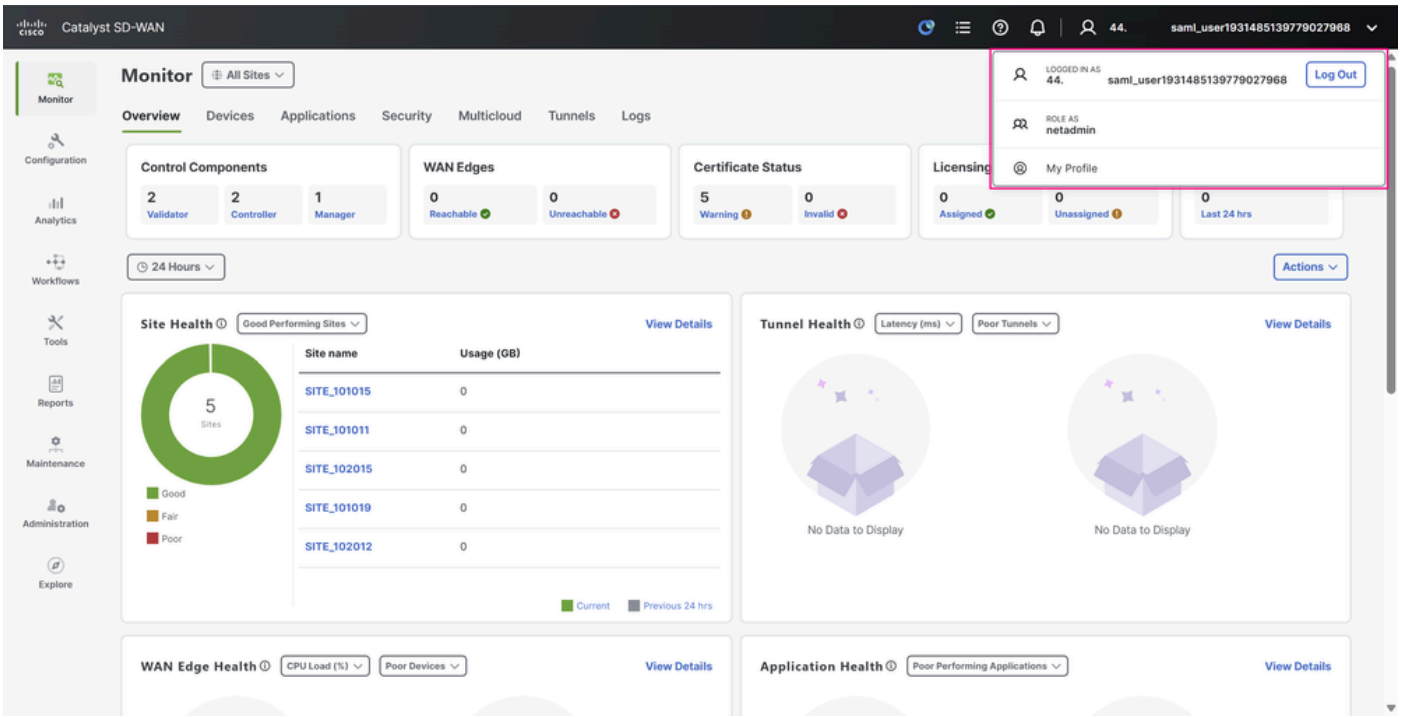
Microsoftログイン画面

- SSOユーザが初めてログインするときなので、プロンプトはパスワードの変更を要求します。



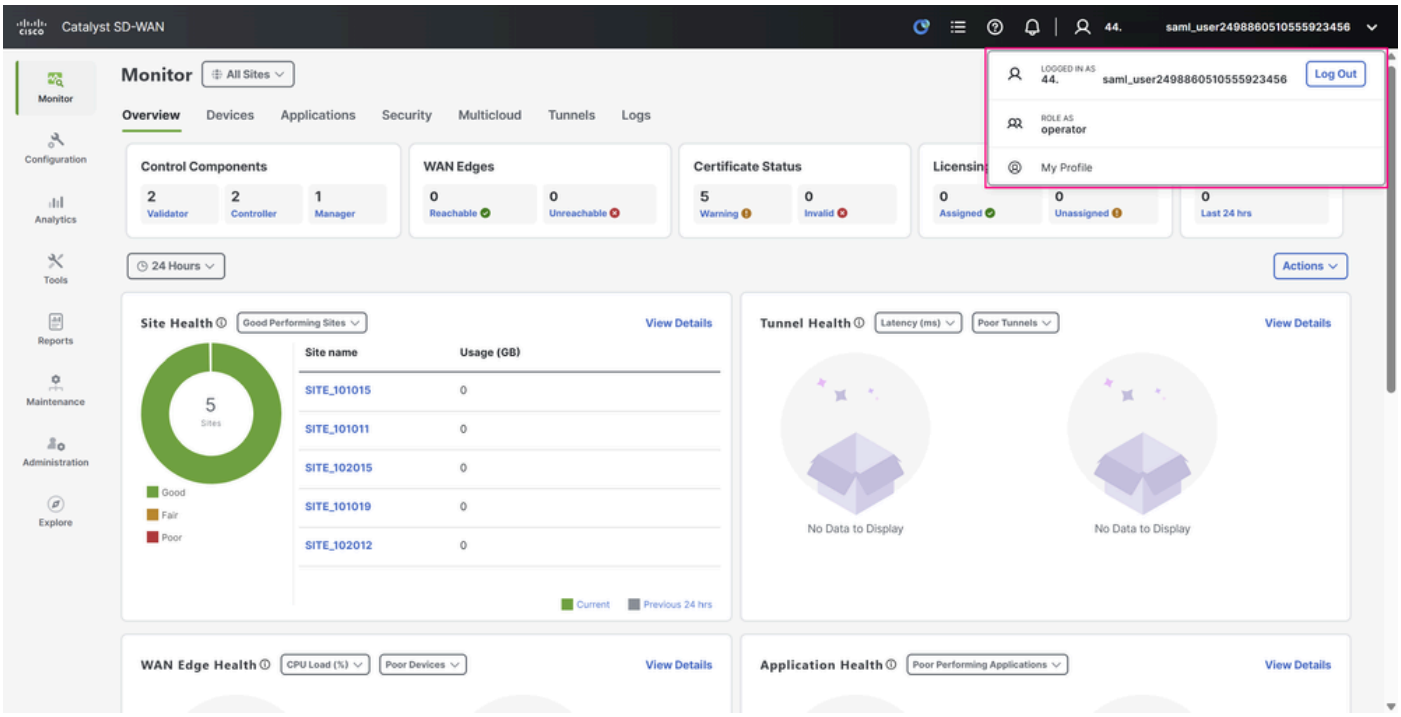
Microsoftログイン画面

- サインインに成功した後、ダッシュボードの右上隅にあるプロファイルの詳細をもう一度展開すると、Microsoft Entra IDで設定したとおりにnetadminロールによってユーザが検出されたことを確認できます。



Cisco SD-WAN ManagerのUI

- 最後に、他のユーザと同じサインインテストを実行します。同じ動作が表示されます。ユーザはoperatorロールで識別されます。



Cisco SD-WAN ManagerのUI

関連情報

- [Cisco IOS XE Catalyst SD-WANでのシングルサインオンの設定]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。