Configuration de SSO pour SD-WAN à l'aide de Microsoft Entra ID

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Avantages de l'authentification unique

Configurer

- Étape 1. Obtention des métadonnées SAML du gestionnaire Cisco SD-WAN
- Étape 2. Configuration d'une application d'entreprise pour SSO dans Microsoft Entra ID
- Étape 3. Ajouter un compte d'utilisateur ou de groupe à l'application d'entreprise
- Étape 4. Configuration de la mise en service de groupe SAML pour Microsoft Entra ID
- Étape 5. Importation du fichier de métadonnées SAML Microsoft Entra ID dans Cisco SD-WAN Manager

Vérifier

Informations connexes

Introduction

Ce document décrit comment configurer l'authentification unique (SSO) pour les réseaux étendus définis par logiciel (SD-WAN) Cisco Catalyst avec Microsoft Entra ID.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance générale des sujets suivants :

- Authentification unique
- Solution SD-WAN Cisco Catalyst

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco Catalyst SD-WAN Manager version 20.15.3.1
- ID d'entrée Microsoft

Remarque : La solution anciennement appelée Azure Active Directory (Azure AD) s'appelle désormais Microsoft Entra ID.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'authentification unique est une méthode d'authentification qui permet aux utilisateurs d'accéder en toute sécurité à plusieurs applications ou sites Web indépendants à l'aide d'un seul jeu d'informations d'identification. Grâce à SSO, les utilisateurs n'ont plus besoin de se connecter séparément à chaque application. Une fois authentifiés, ils peuvent accéder en toute transparence à toutes les ressources autorisées.

L'une des méthodes courantes d'implémentation de l'authentification unique est la fédération, qui établit la confiance entre un fournisseur d'identité (IdP) et un fournisseur de services (SP) à l'aide de protocoles tels que SAML 2.0, WS-Federation ou OpenID Connect. La fédération améliore la sécurité, la fiabilité et l'expérience utilisateur en centralisant l'authentification.

Microsoft Entra ID est un fournisseur d'identité cloud largement utilisé qui prend en charge ces protocoles de fédération. Dans une configuration SSO avec Cisco Catalyst SD-WAN, Microsoft Entra ID agit en tant que fournisseur d'ID et Cisco SD-WAN Manager agit en tant que fournisseur de services.

L'intégration fonctionne comme suit :

1. Un administrateur réseau tente de se connecter à Cisco SD-WAN Manager.
2. Cisco SD-WAN Manager envoie une demande d'authentification à Microsoft Entra ID.
3. Microsoft Entra ID invite l'administrateur à s'authentifier avec son compte Entra ID (Microsoft).
4. Une fois les informations d'identification validées, Microsoft Entra ID renvoie une réponse sécurisée au Cisco SD-WAN Manager pour confirmer l'authentification.
5. Cisco SD-WAN Manager octroie l'accès sans exiger d'informations d'identification distinctes.

Dans ce modèle :

- Fournisseur d'identité (IdP) : stocke les données utilisateur, valide les informations d'identification (par exemple, Microsoft Entra ID, Okta, PingID, ADFS).
- Fournisseur de services : héberge l'application à laquelle accéder (par exemple, Cisco SD-WAN Manager).
- Utilisateurs : disposent d'un compte dans l'annuaire IdP et sont autorisés à accéder au fournisseur de services.

Cisco Catalyst SD-WAN est compatible avec tout fournisseur d'identité SAML 2.0 lorsqu'il est configuré conformément aux normes industrielles.

Avantages de l'authentification unique

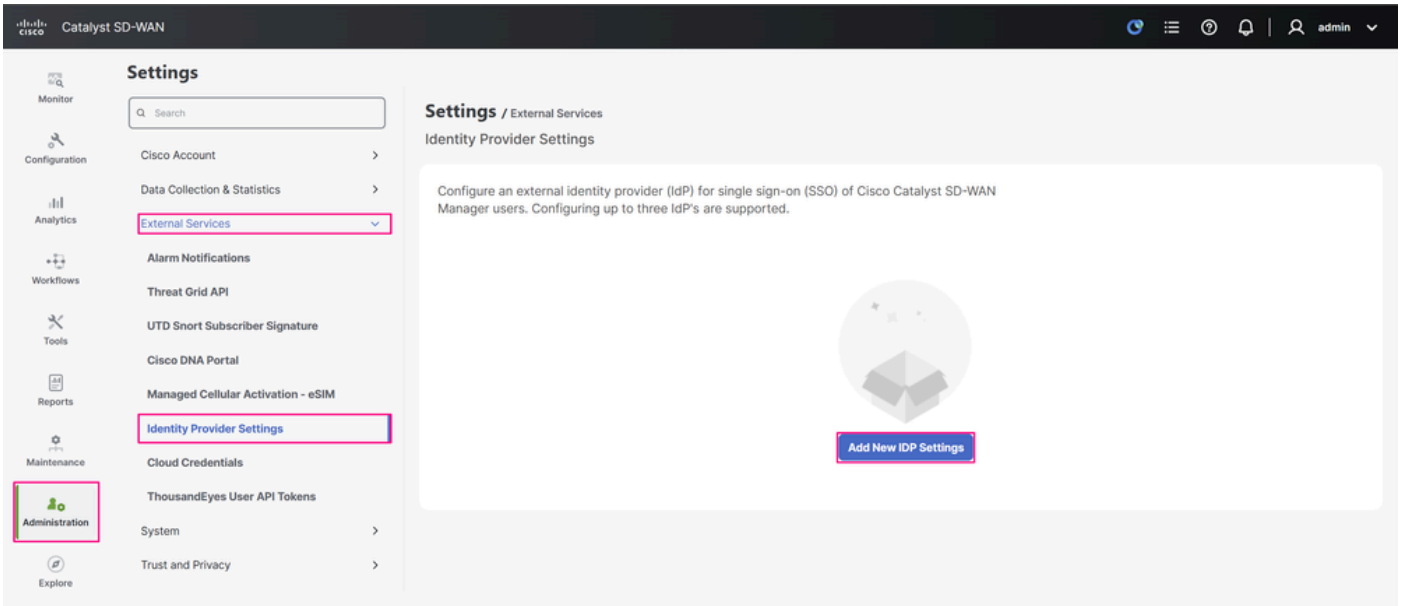
- Centralise la gestion des identifiants via le fournisseur d'identités.
- Renforce la sécurité de l'authentification en éliminant plusieurs mots de passe faibles.
- Rationalise l'accès sécurisé pour les administrateurs.
- Permet d'accéder en un clic à Cisco Catalyst SD-WAN Manager et à d'autres applications autorisées.

Configurer

Remarque : Version minimale prise en charge : Cisco Catalyst SD-WAN Manager version 20.8.1.

Étape 1. Obtention des métadonnées SAML du gestionnaire Cisco SD-WAN

- Dans Cisco SD-WAN Manager, accédez à Administration > Settings > External Services > Identity Provider Settings et cliquez sur Add New IDP Settings.



Interface utilisateur de Cisco SD-WAN Manager

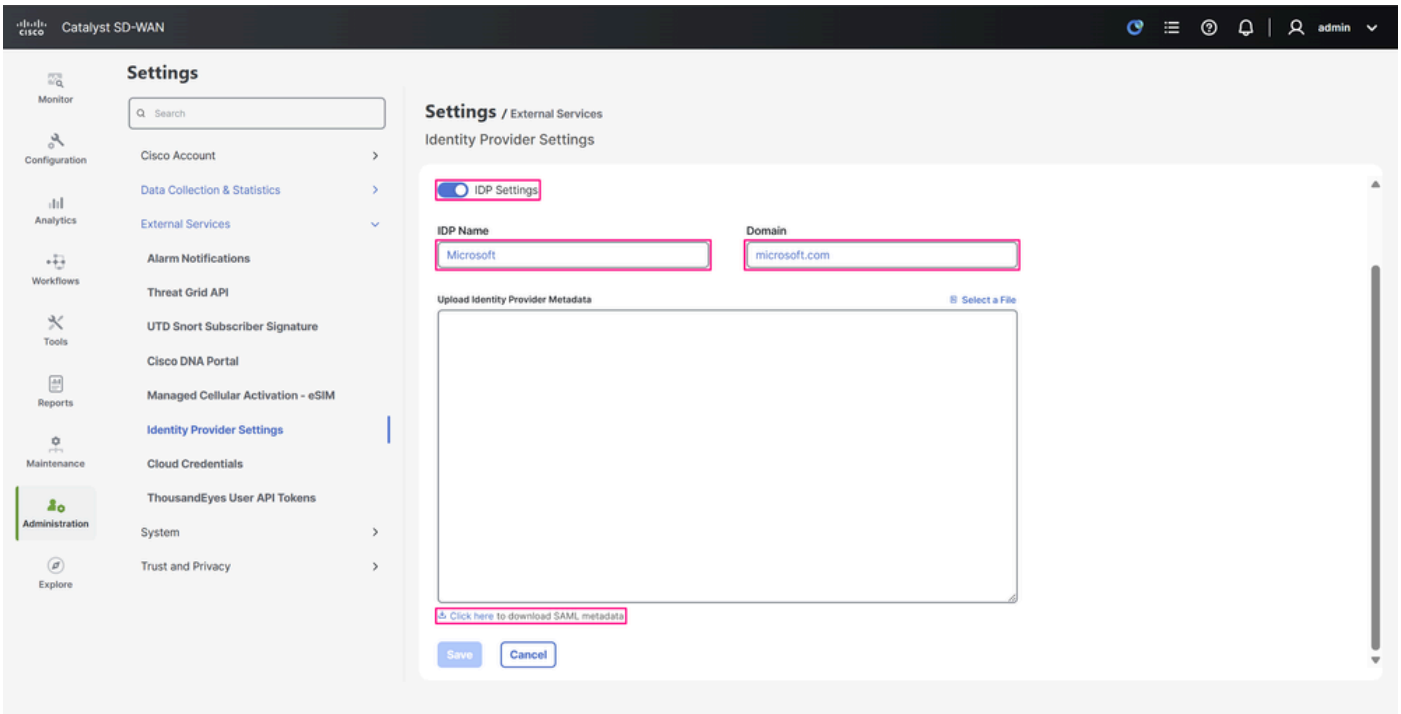
- Activez IDP Settings pour activer les paramètres du fournisseur d'identité. Dans le champ IDP Name, entrez un nom qui fait référence au fournisseur d'identité que vous utilisez et dans le champ Domain, entrez un domaine qui correspond aux noms de domaine utilisés par les utilisateurs dans l'application d'entreprise de votre organisation. Cliquez sur Cliquez ici pour télécharger les métadonnées SAML et enregistrer le fichier XML de métadonnées sur votre ordinateur. Ce fichier est utilisé pour configurer l'authentification unique dans

Microsoft Entra ID à l'étape suivante.

Remarque : Dans cet exemple, le fichier XML de métadonnées pointe directement vers l'adresse IP de Cisco SD-WAN Manager, mais dans de nombreux environnements de production, il pointe vers son nom de domaine complet (FQDN). Pour un gestionnaire Cisco SD-WAN autonome, l'ID d'entité contenu dans les métadonnées correspond à l'URL que vous utilisez pour vous connecter au gestionnaire Cisco SD-WAN au moment où vous le téléchargez. Cela signifie qu'il fonctionne avec l'adresse IP ou le nom de domaine complet (FQDN), puisqu'il s'agit d'une configuration à noeud unique.

Pour un cluster Cisco SD-WAN Manager, le même principe s'applique dans la mesure où le nom de domaine complet pointe vers l'un des noeuds du cluster et où les métadonnées incluent ce domaine comme ID d'entité. La différence est que, que vous utilisiez des métadonnées avec le nom de domaine complet du cluster ou à partir d'un noeud spécifique utilisant son adresse IP, une fois l'intégration SSO avec Microsoft Entra ID terminée, les autres noeuds redirigent également vers l'invite de connexion IdP.

Dans les deux scénarios, la principale exigence est que l'ID d'entité que vous utilisez dans Cisco SD-WAN Manager (qu'il s'agisse d'une adresse IP ou d'un nom de domaine complet) corresponde à l'identificateur configuré côté fournisseur d'identité.

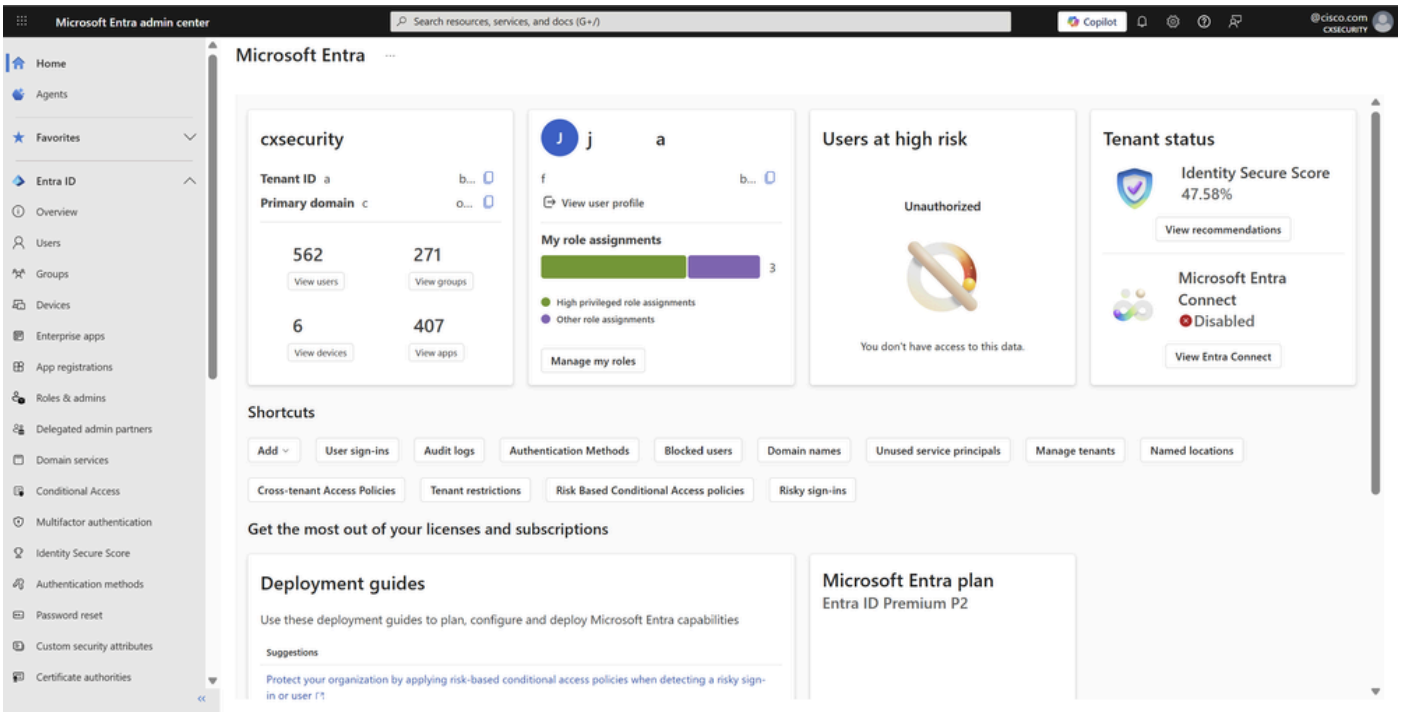


Page Configuration des paramètres IdP

Étape 2. Configuration d'une application d'entreprise pour SSO dans Microsoft Entra ID

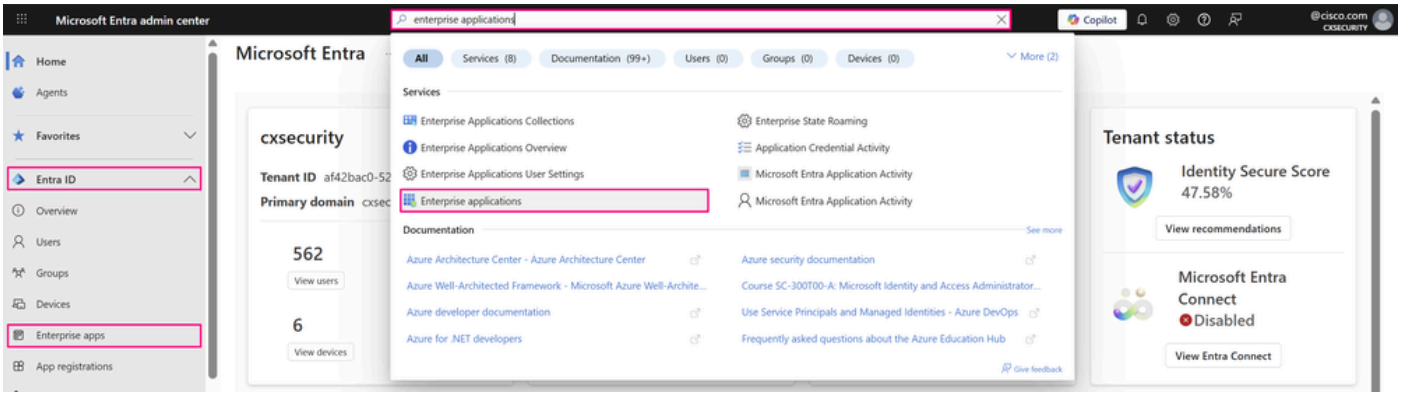
- Connectez-vous au portail du centre d'administration Microsoft Entra avec l'un des rôles

suivants : Administrateur d'applications cloud, Administrateur d'applications ou propriétaire du principal du service.



Portail Microsoft Entra Admin Center

- Accédez à ID d'entrée > Applications d'entreprise, ou vous pouvez également accéder à ce service lorsque vous entrez applications d'entreprise dans la barre de recherche en haut du portail, puis choisissez Applications d'entreprise.



Portail Microsoft Entra Admin Center

- La page Toutes les applications s'ouvre. Entrez le nom de votre application existante dans la zone de recherche, puis choisissez l'application dans les résultats de la recherche.

Remarque : Sur cette même page, vous pouvez créer une application d'entreprise personnalisée en fonction des besoins de votre organisation et la configurer avec l'authentification SSO si vous ne l'avez pas déjà fait, lorsque vous cliquez sur

---

Nouvelle application.

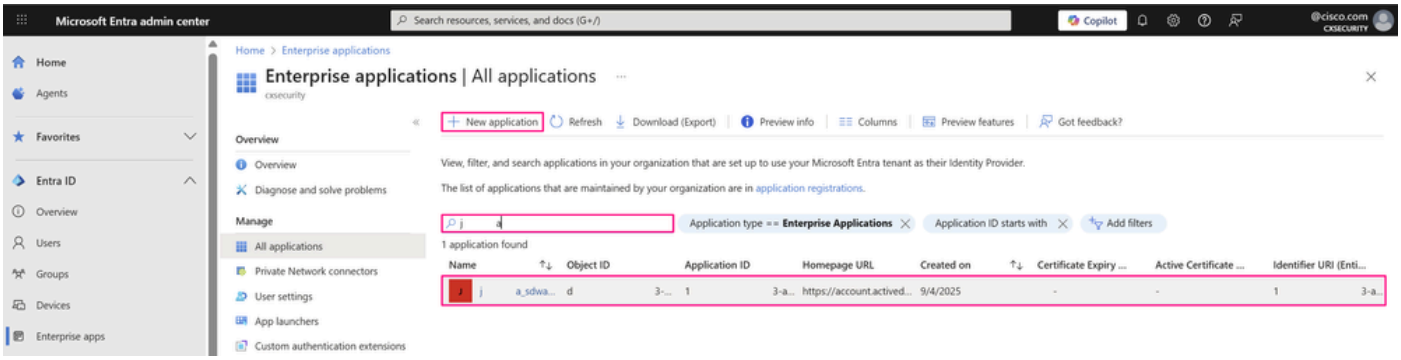
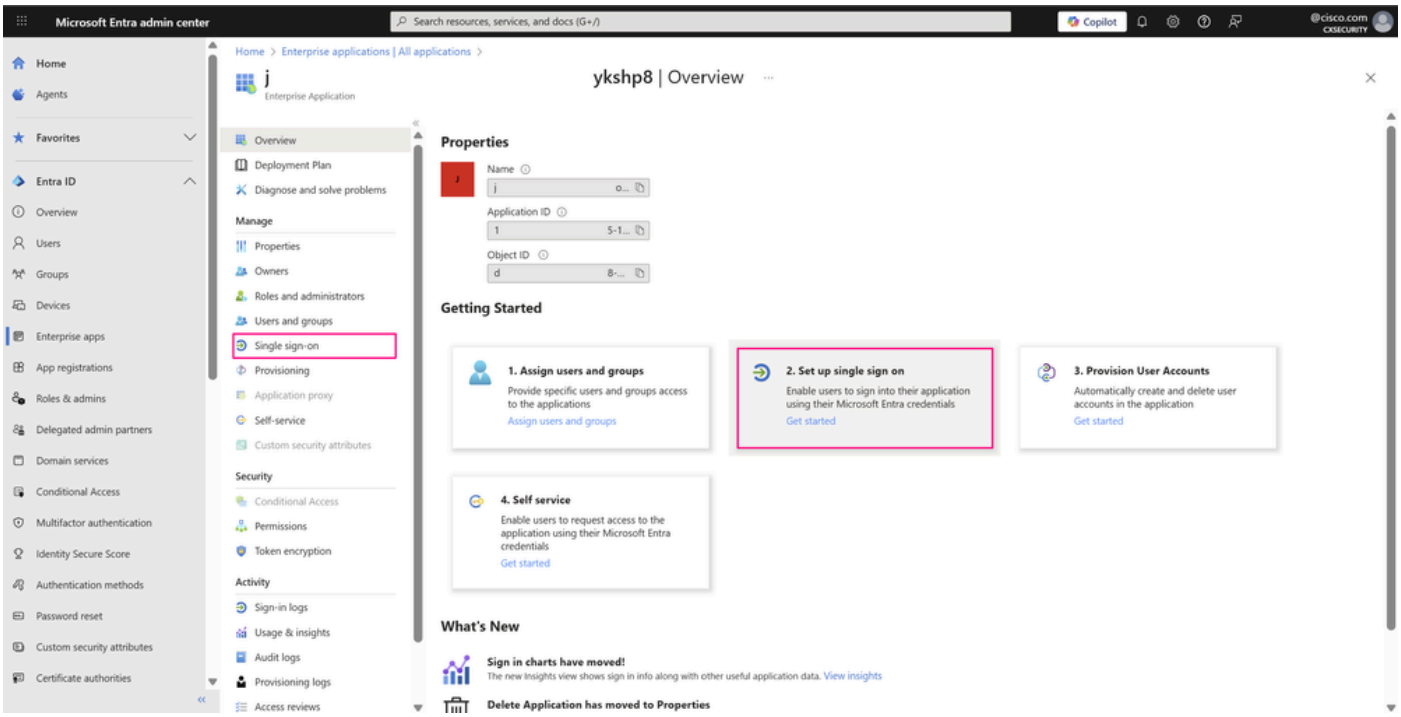


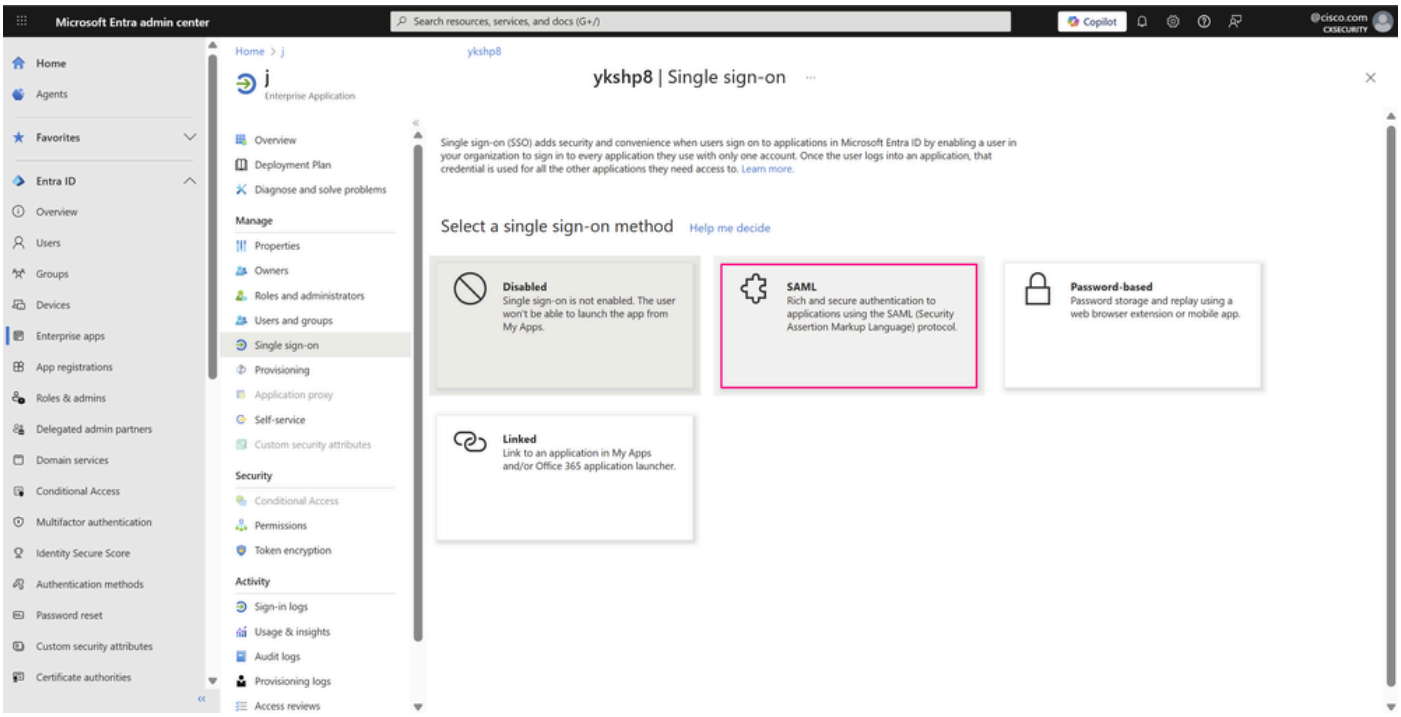
Tableau de bord Applications professionnelles

- Dans la section Gérer du menu de gauche, cliquez sur Authentification unique, ou dans le volet Mise en route de la section Présentation, cliquez sur 2. Configurez l'authentification unique pour ouvrir le volet d'authentification unique pour modification.



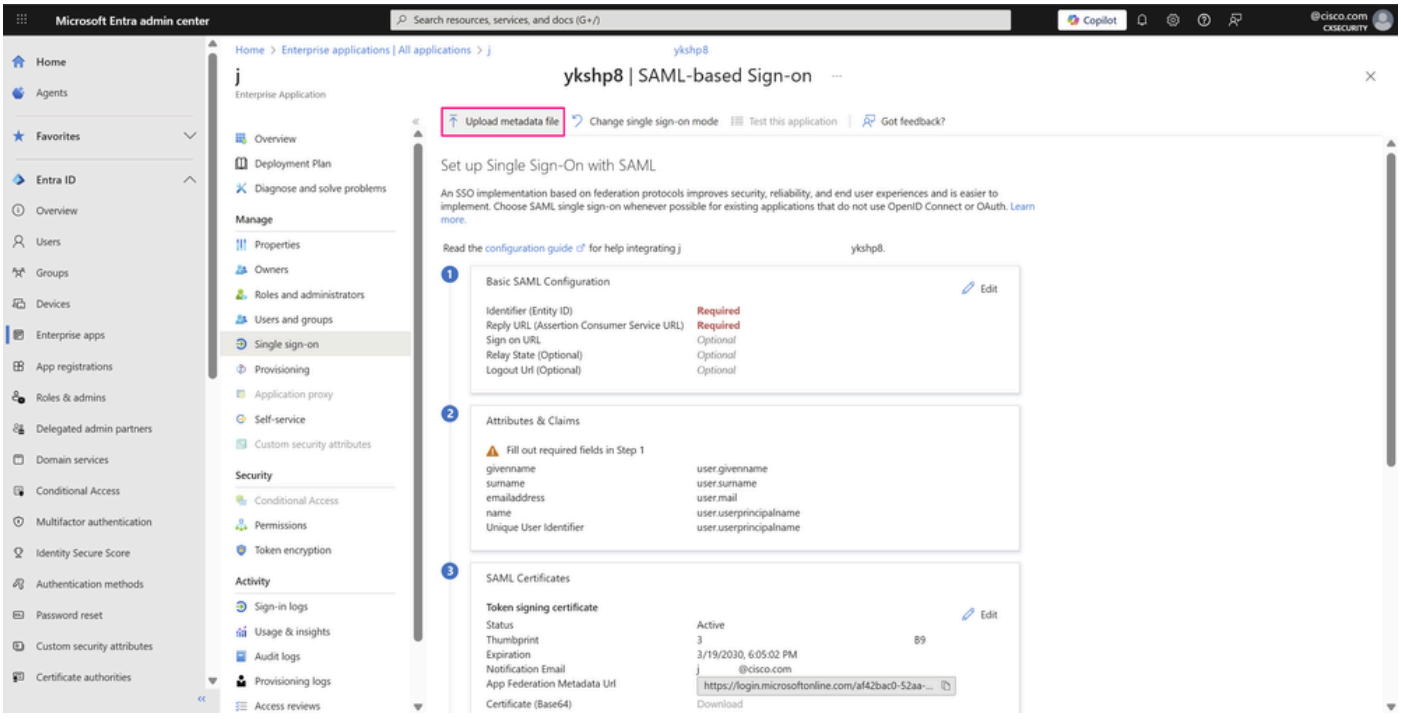
Présentation des applications d'entreprise

- Sélectionnez SAML pour ouvrir la page de configuration SSO.



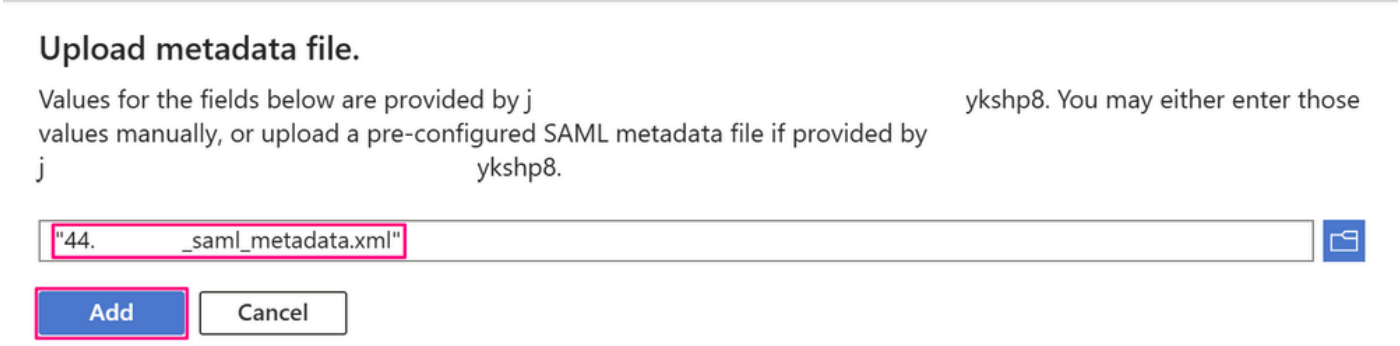
Volet d'authentification unique

- Sur la page Configurer l'authentification unique avec SAML, cliquez sur Télécharger le fichier de métadonnées.



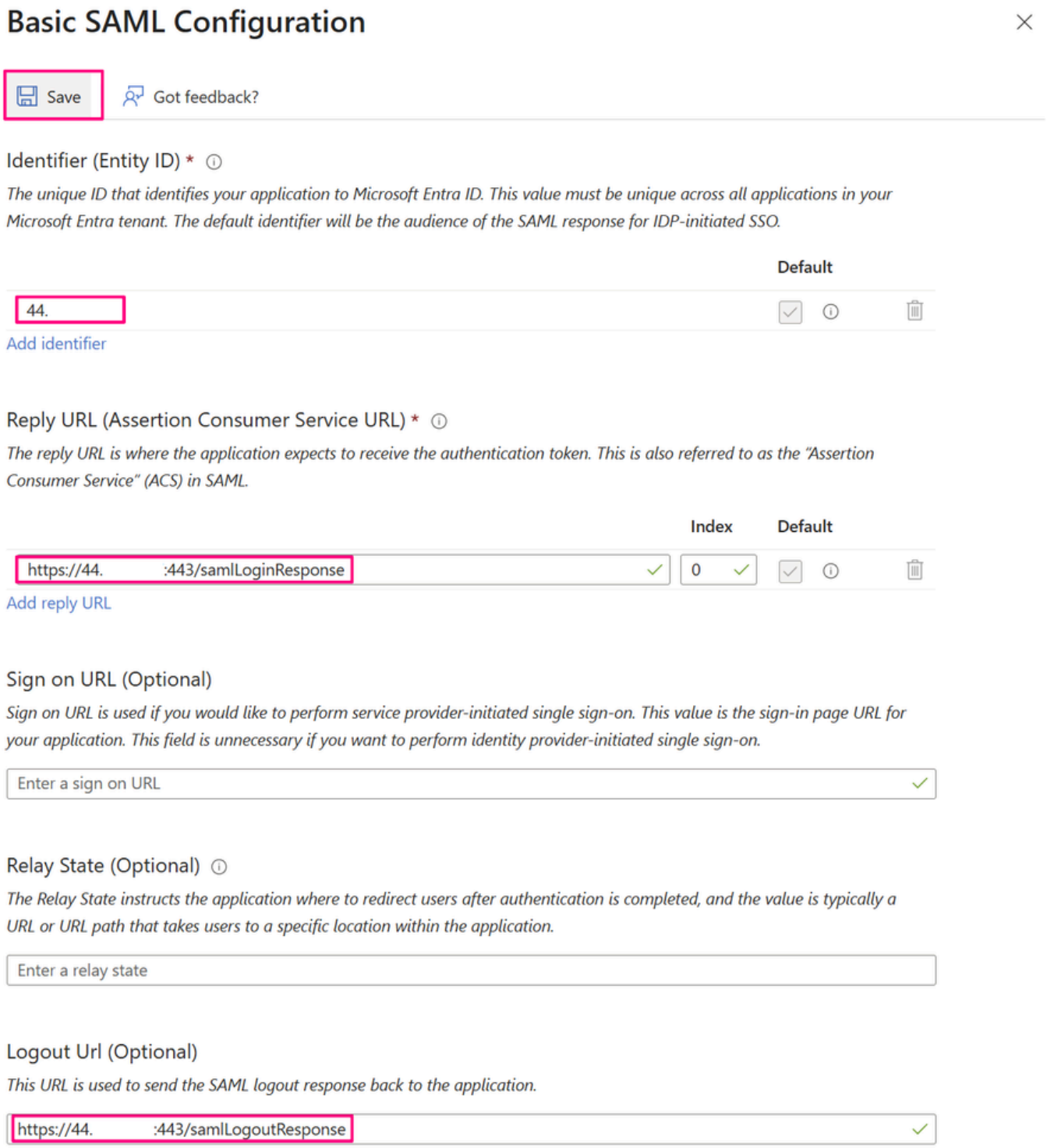
Page SSO with SAML Configuration

- Dans la fenêtre Télécharger le fichier de métadonnées, accédez au fichier XML de métadonnées que vous avez téléchargé, cliquez dessus, puis cliquez sur Ajouter.



Fenêtre Charger le fichier de métadonnées

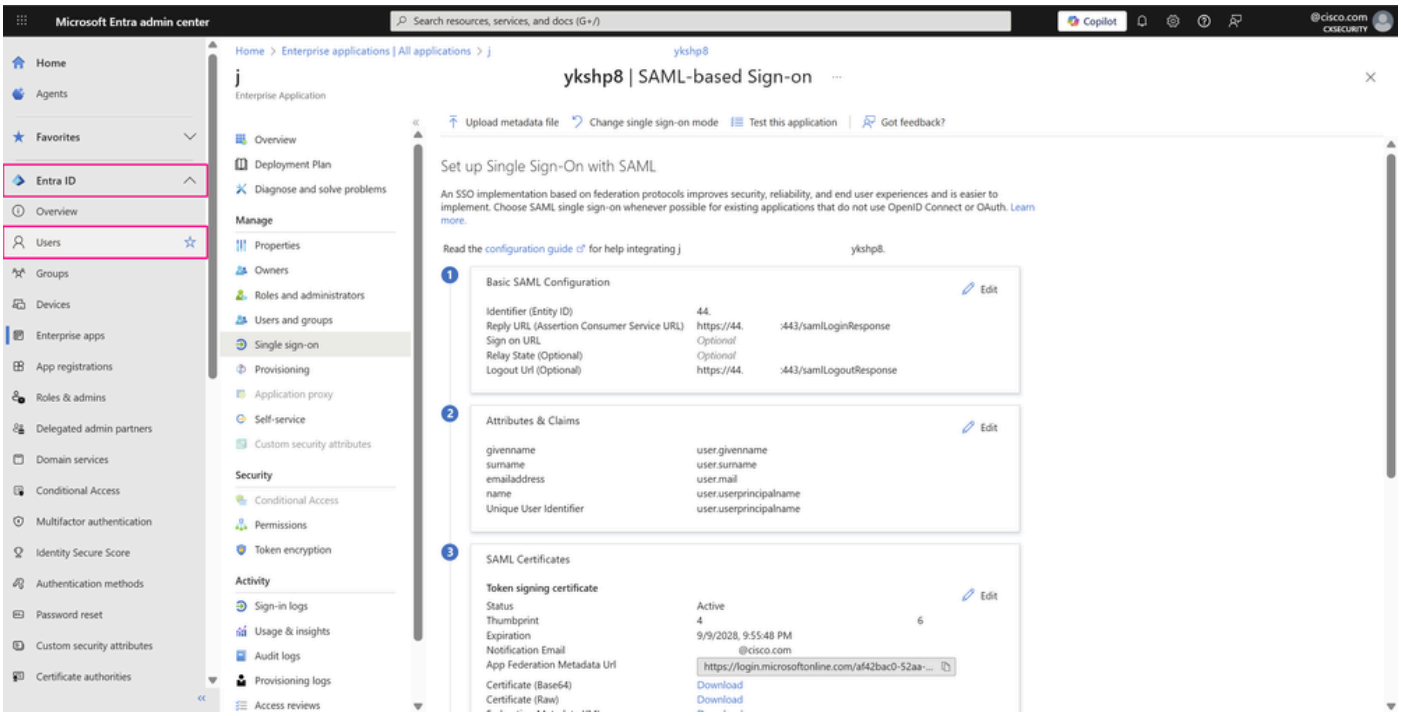
- Dans la fenêtre Configuration SAML de base, l'Identificateur (ID d'entité) est généralement l'URL spécifique à l'application (dans ce cas, le gestionnaire Cisco SD-WAN) avec laquelle vous effectuez l'intégration (comme expliqué à l'étape précédente). Les valeurs URL de réponse et URL de déconnexion sont renseignées automatiquement une fois le fichier téléchargé. Pour continuer, cliquez sur Enregistrer.



Fenêtre Configuration SAML de base

Étape 3. Ajouter un compte d'utilisateur ou de groupe à l'application d'entreprise

- Une fois les paramètres de configuration SAML de l'application définis, vous ajoutez les utilisateurs ou les groupes de l'application d'entreprise qui se connectent à l'application. Pour ce faire, accédez d'abord à Entra ID > Users, ou vous pouvez également accéder à ce service lorsque vous recherchez le nom du service dans la barre de recherche en haut du portail, comme indiqué dans une étape précédente.



Page SSO with SAML Configuration

- Créez un utilisateur que vous associez à un groupe pour illustrer l'authentification SSO avec Cisco SD-WAN Manager et l'un de ses groupes d'utilisateurs, netadmin, qui est le plus courant dans les environnements de production. Pour ce faire, accédez à Saisir un ID > Utilisateurs. Cliquez ensuite sur Nouvel utilisateur et sélectionnez Créer un nouvel utilisateur.

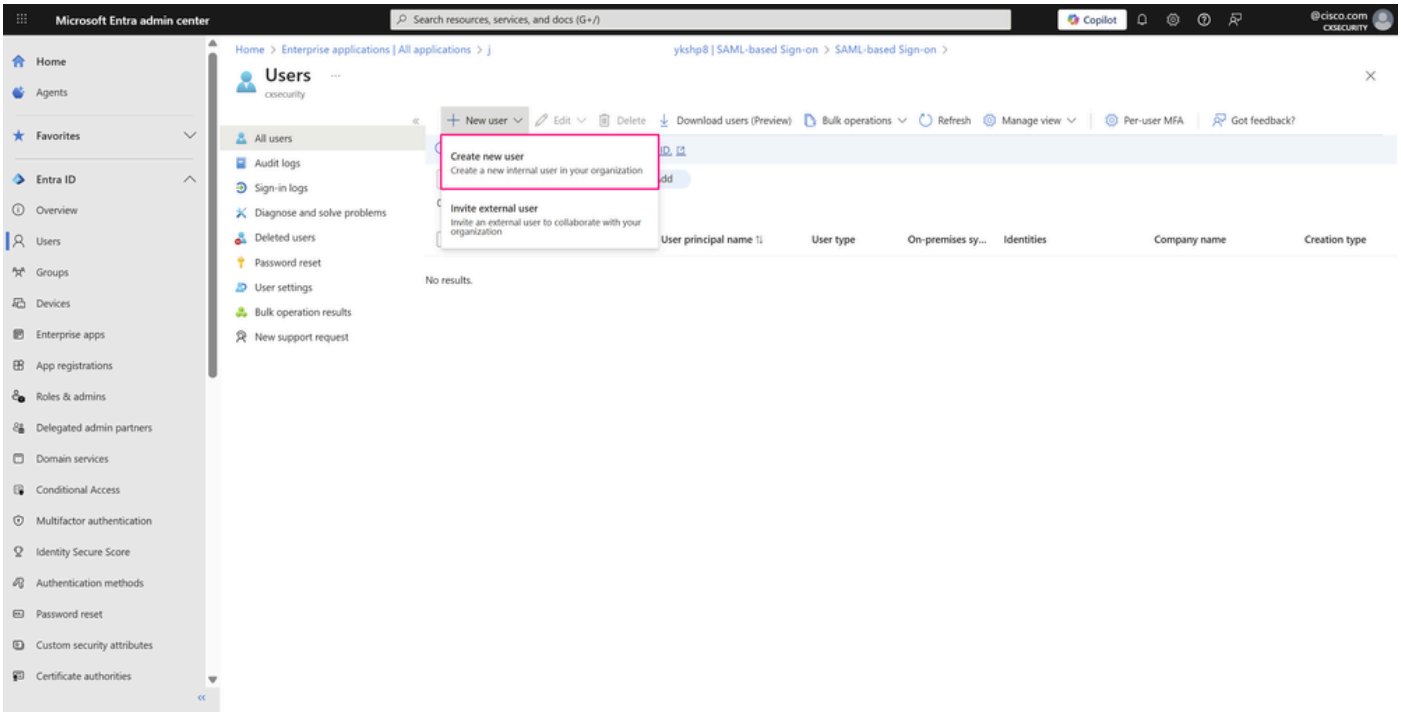
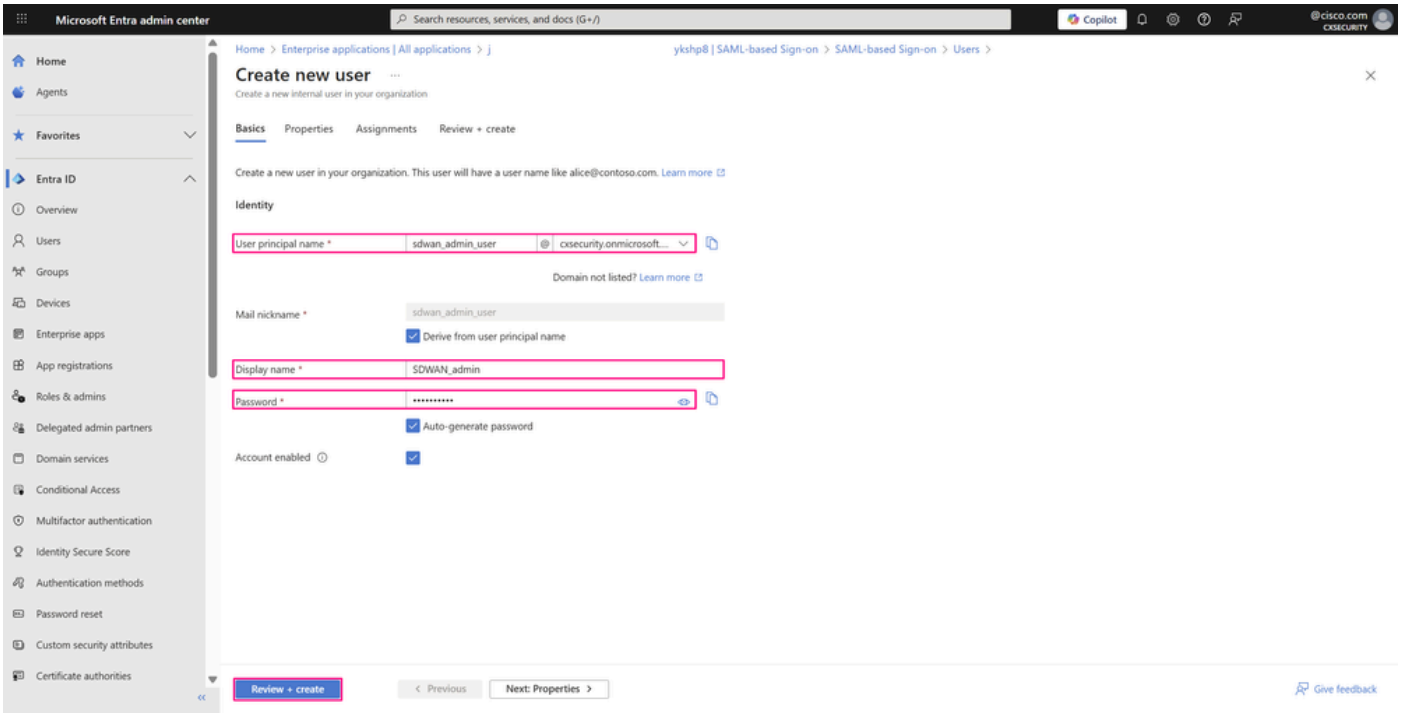


Tableau de bord Utilisateurs

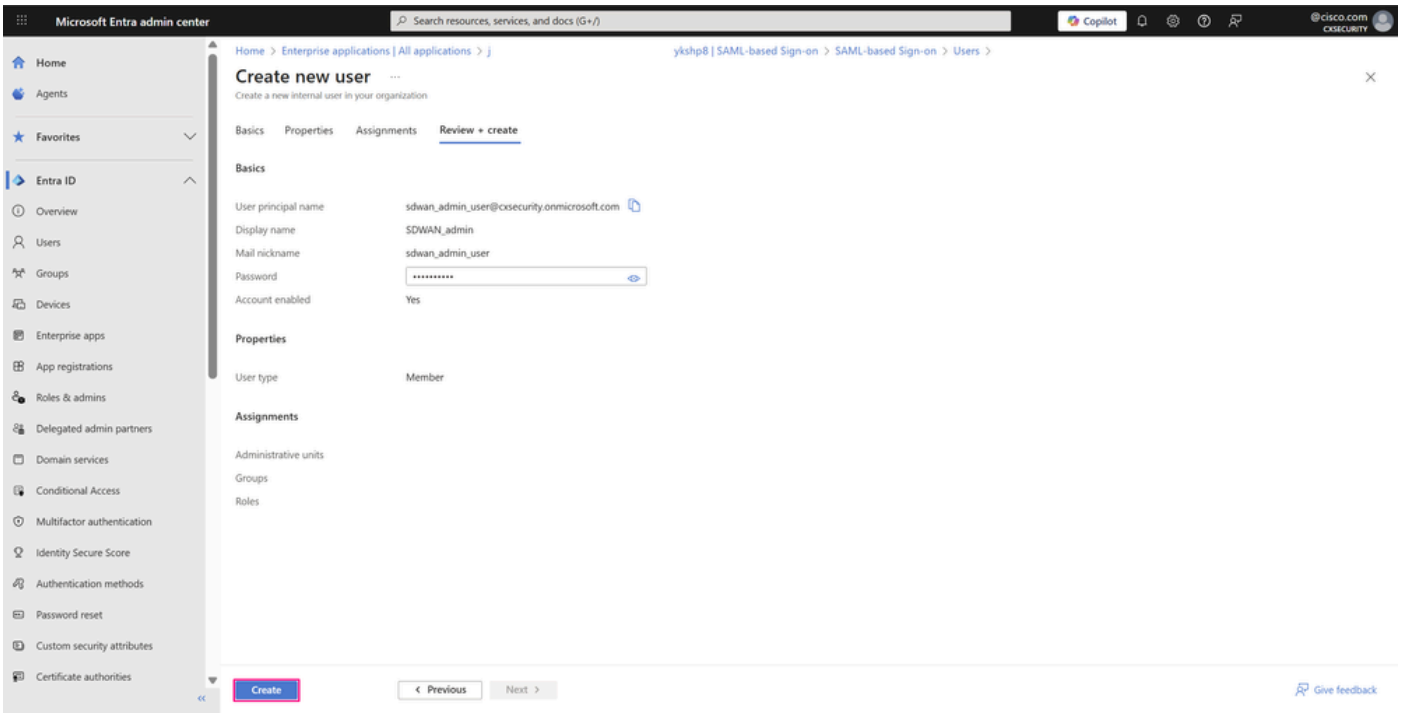
- L'onglet Notions de base contient les champs de base requis pour créer un nouvel utilisateur.

- Pour le nom d'utilisateur principal, entrez un nom d'utilisateur unique et choisissez un domaine dans la liste déroulante des domaines disponibles dans votre organisation.
- Entrez un nom d'affichage pour l'utilisateur.
- Désactivez la case Auto-generate password si vous voulez entrer un mot de passe personnalisé ou laissez cette option cochée pour qu'un mot de passe soit généré automatiquement.
- Vous pouvez ajouter l'utilisateur à un groupe dans l'onglet Assignments, mais comme l'appartenance au groupe n'a pas encore été créée, cliquez sur Review + create.



Page Création d'utilisateur

- Le dernier onglet affiche les détails clés du workflow de création d'utilisateur. Vérifiez les détails et cliquez sur Create pour terminer le processus.



Page Création d'utilisateur

- Le nouvel utilisateur apparaît peu de temps après. Si ce n'est pas le cas, cliquez sur Actualiser et recherchez l'utilisateur à l'aide de la barre de recherche dans le service. Ensuite, accédez à Entra ID > Groups > All groups afin de créer le nouveau groupe.

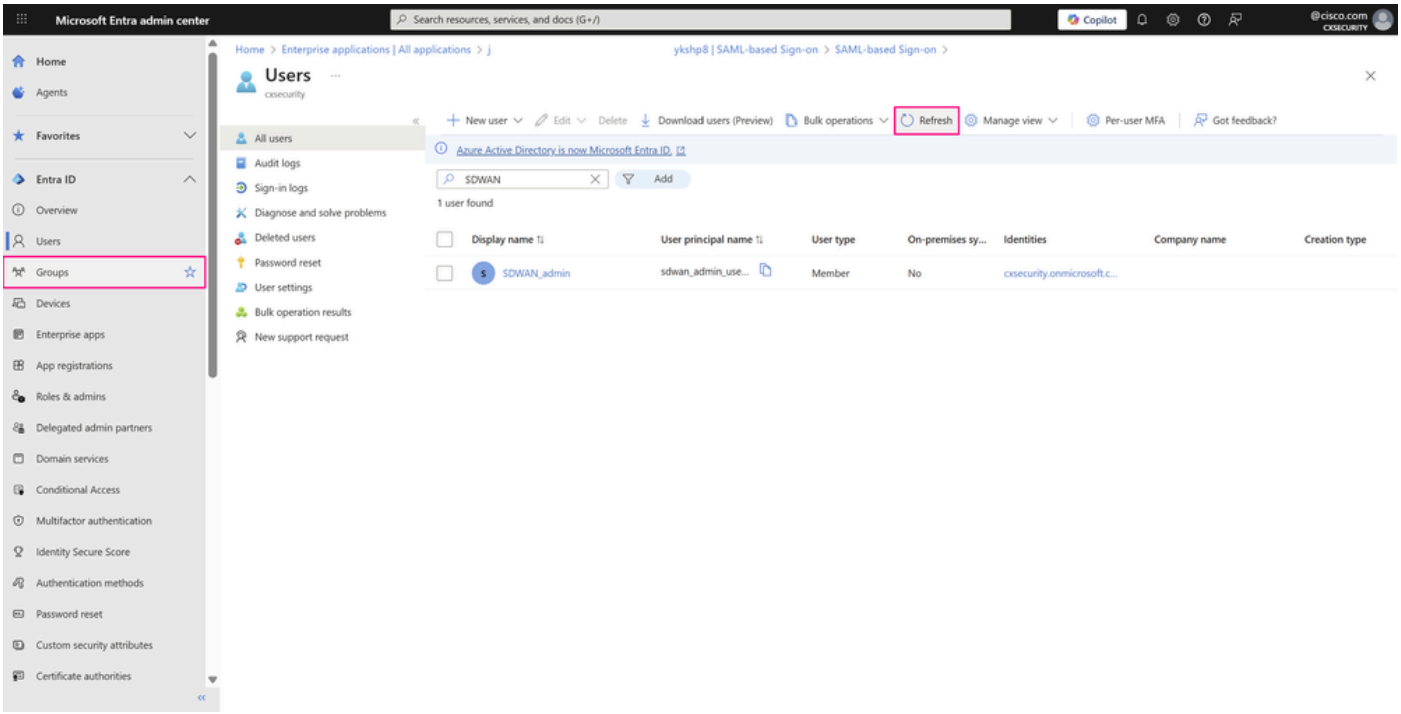
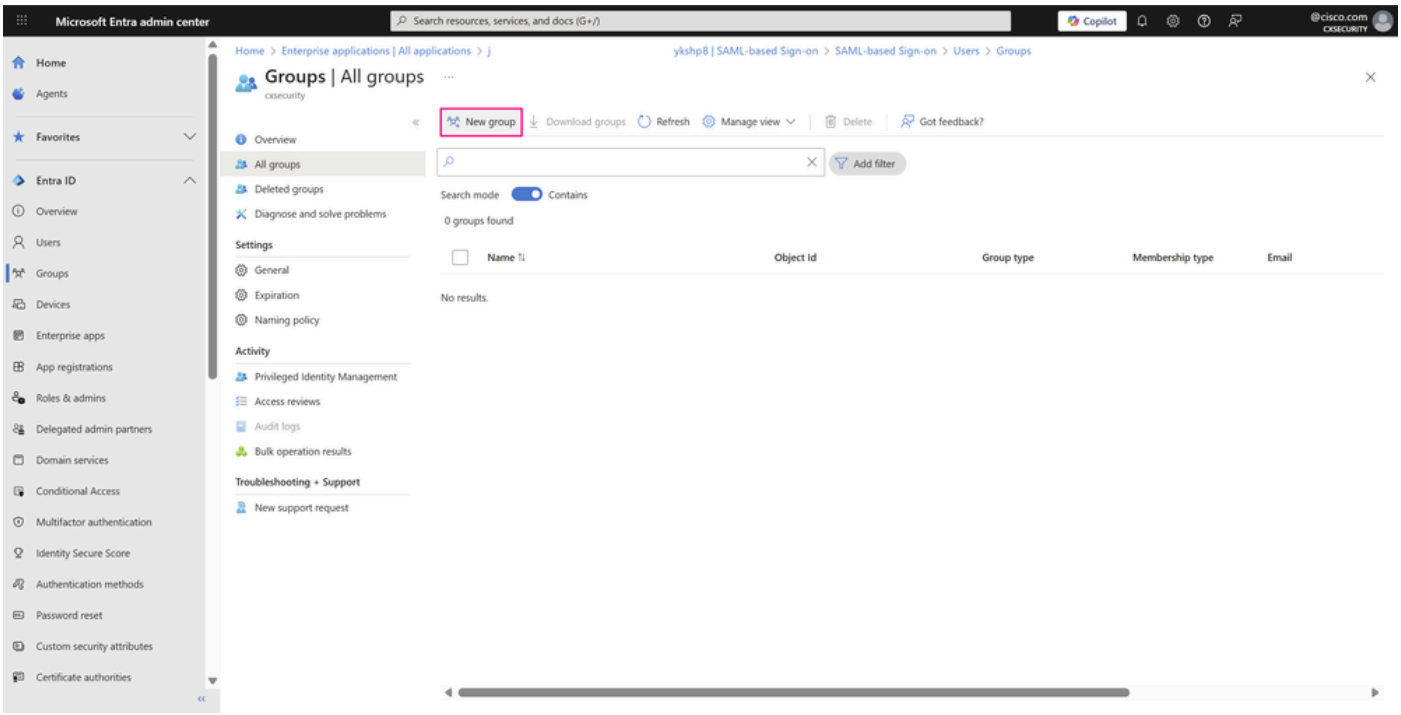


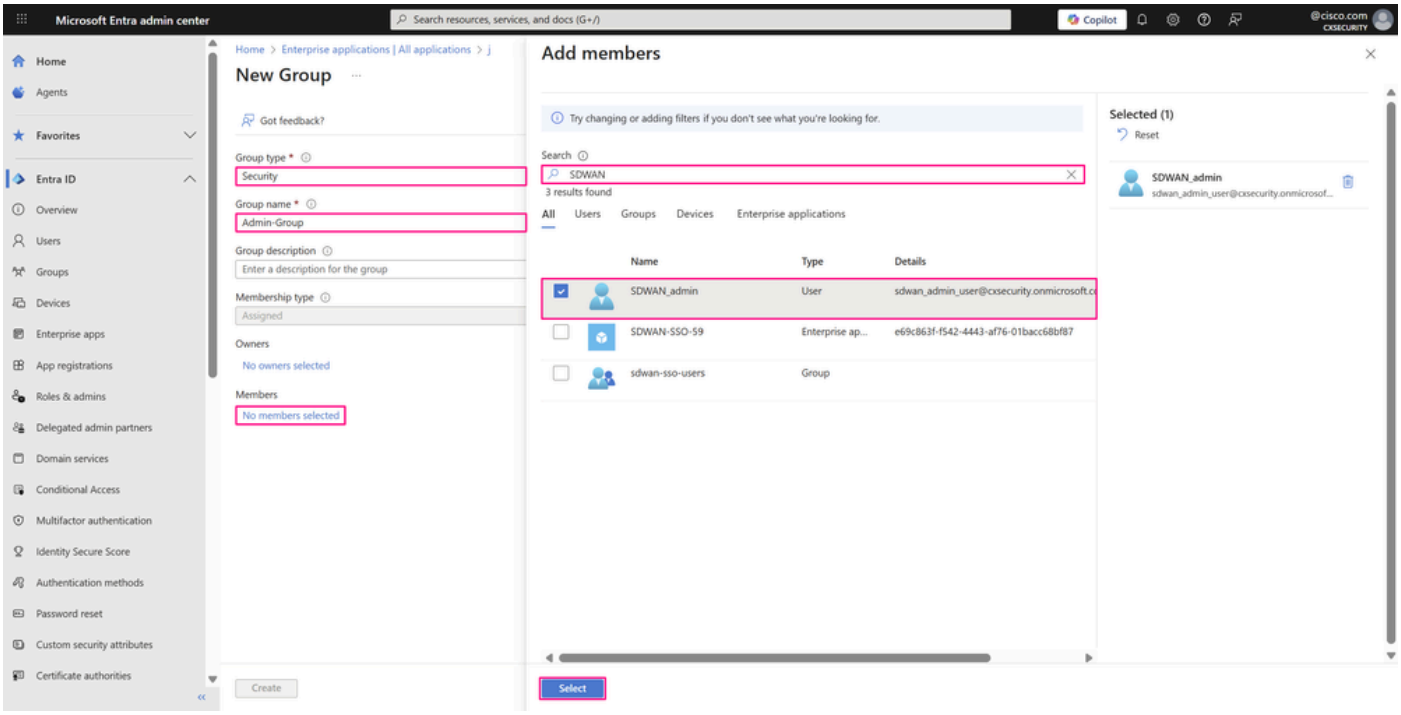
Tableau de bord Utilisateurs

- Sur cette page, vous gérez les différents groupes et leurs autorisations au sein de votre organisation. Cliquez sur Nouveau groupe pour créer le groupe disposant de privilèges d'administrateur réseau.



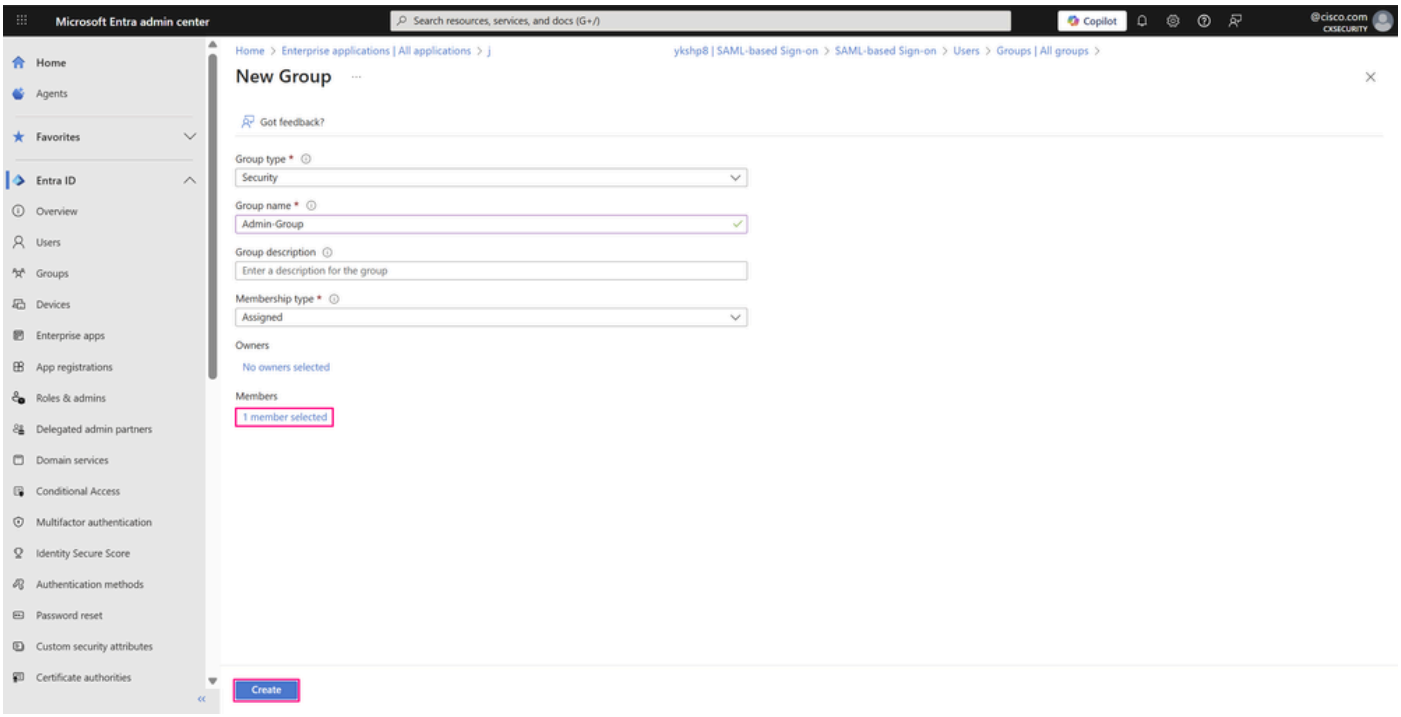
Page Tous les groupes

- Sélectionnez un type de groupe dans la liste déroulante (dans ce cas, Sécurité, car seul l'accès aux ressources partagées est requis). Entrez un nom de groupe de votre choix qui fait référence au rôle ou aux autorisations du groupe. À ce stade, associez des utilisateurs au groupe lorsque vous cliquez sur les membres sélectionnés dans le champ Membres.
    - Dans la fenêtre Ajouter des membres, recherchez et sélectionnez les utilisateurs que vous souhaitez ajouter (dans notre exemple, l'utilisateur que vous venez de créer), puis cliquez sur Sélectionner.



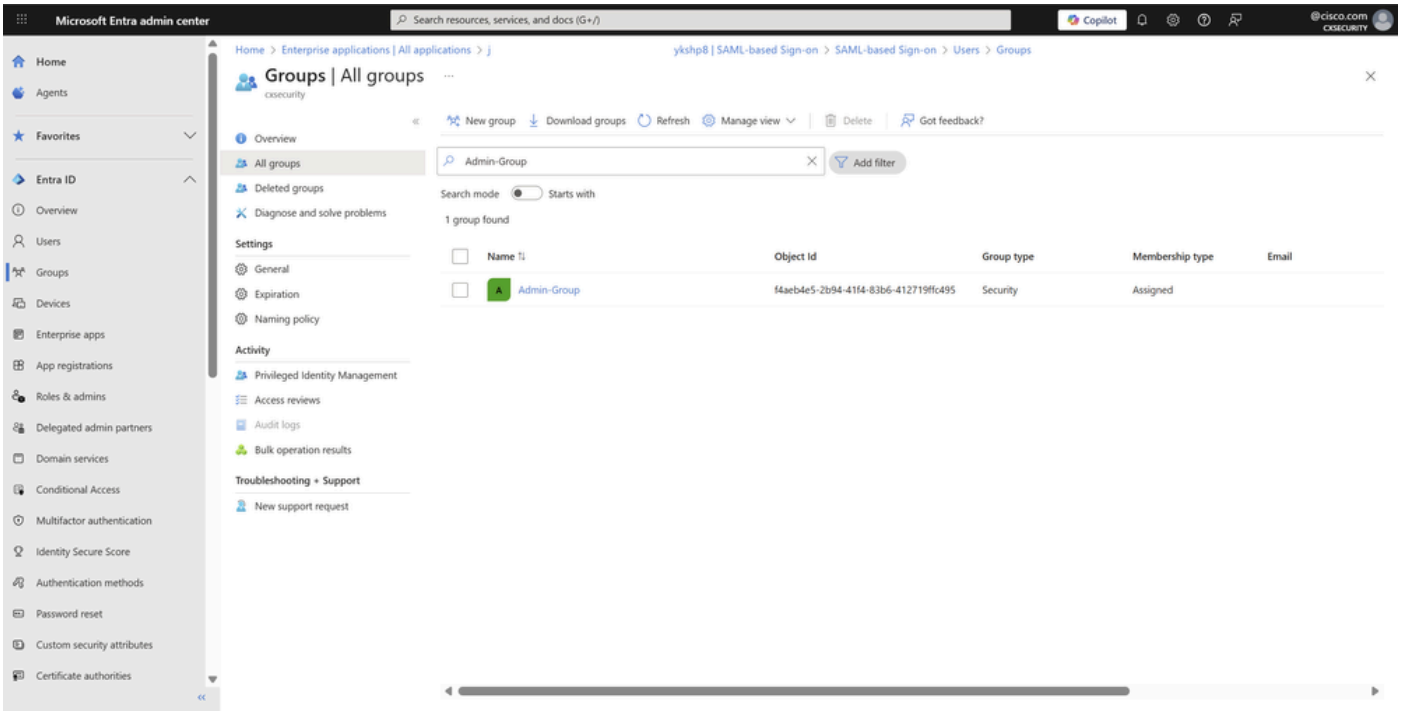
Page Création de groupe

- Cliquez sur Create pour créer le groupe.



Page Création de groupe

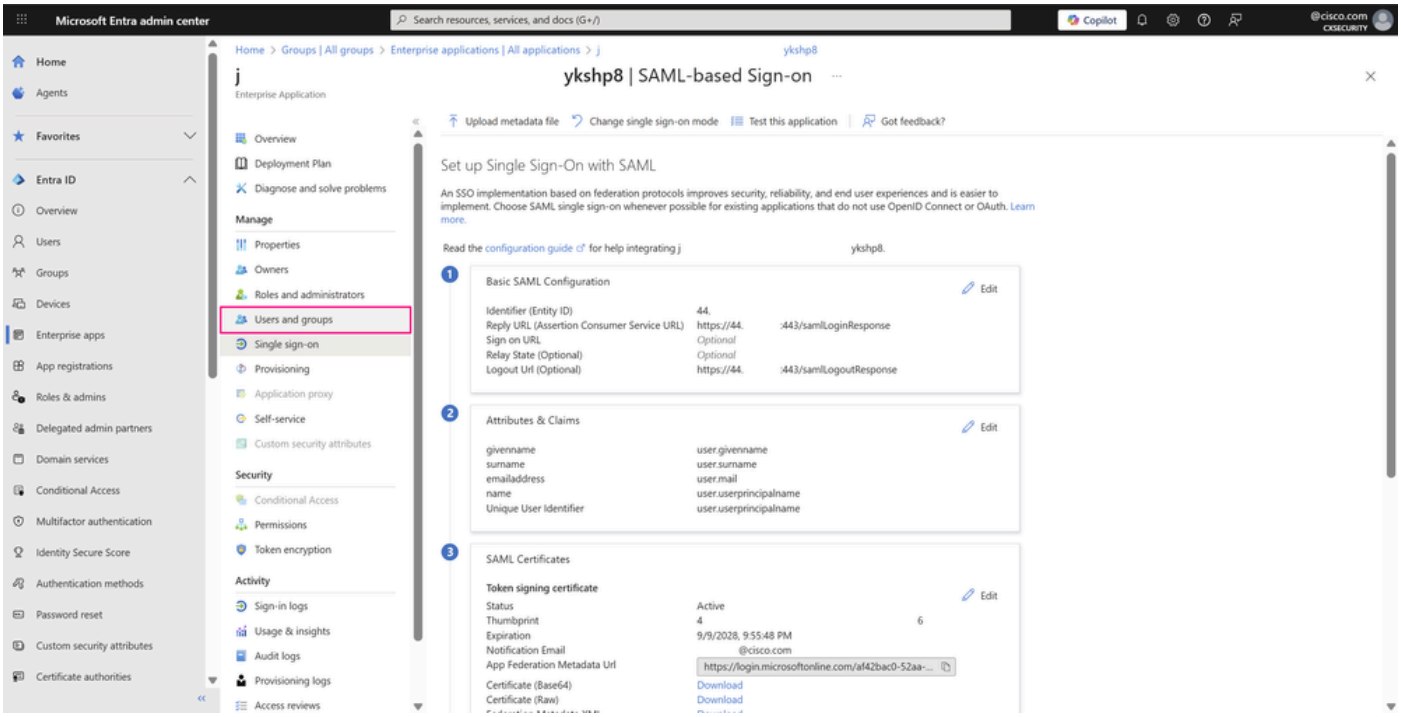
- Le nouveau groupe apparaît peu de temps après. Si ce n'est pas le cas, cliquez sur Actualiser et recherchez le nom du groupe avec la barre de recherche dans le service. Répétez les étapes précédentes pour créer un autre utilisateur et l'ajouter à une autre appartenance au groupe pour valider la connexion SSO avec l'application et l'un de ses autres groupes d'utilisateurs, tel qu'un opérateur.



Page Tous les groupes

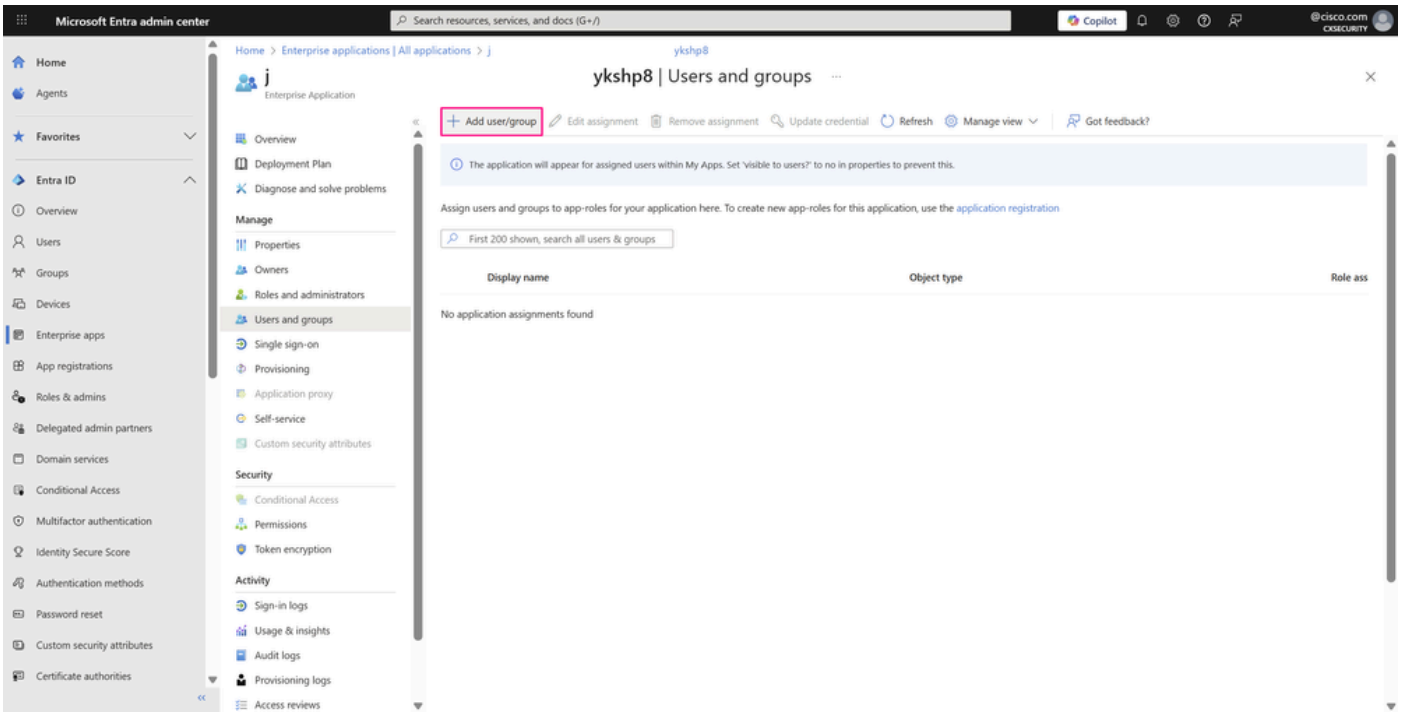
Étape 4. Configuration de la mise en service de groupe SAML pour Microsoft Entra ID

- Pour mettre en service les groupes ou les utilisateurs qui leur sont associés dans la configuration SAML, vous devez les affecter à votre application d'entreprise afin qu'ils disposent des autorisations de connexion pour votre application, par exemple, Cisco SD-WAN Manager. Revenez à Entra ID > Applications d'entreprise et ouvrez votre application d'entreprise. Dans la section Manage du menu de gauche, cliquez sur Users and groups.



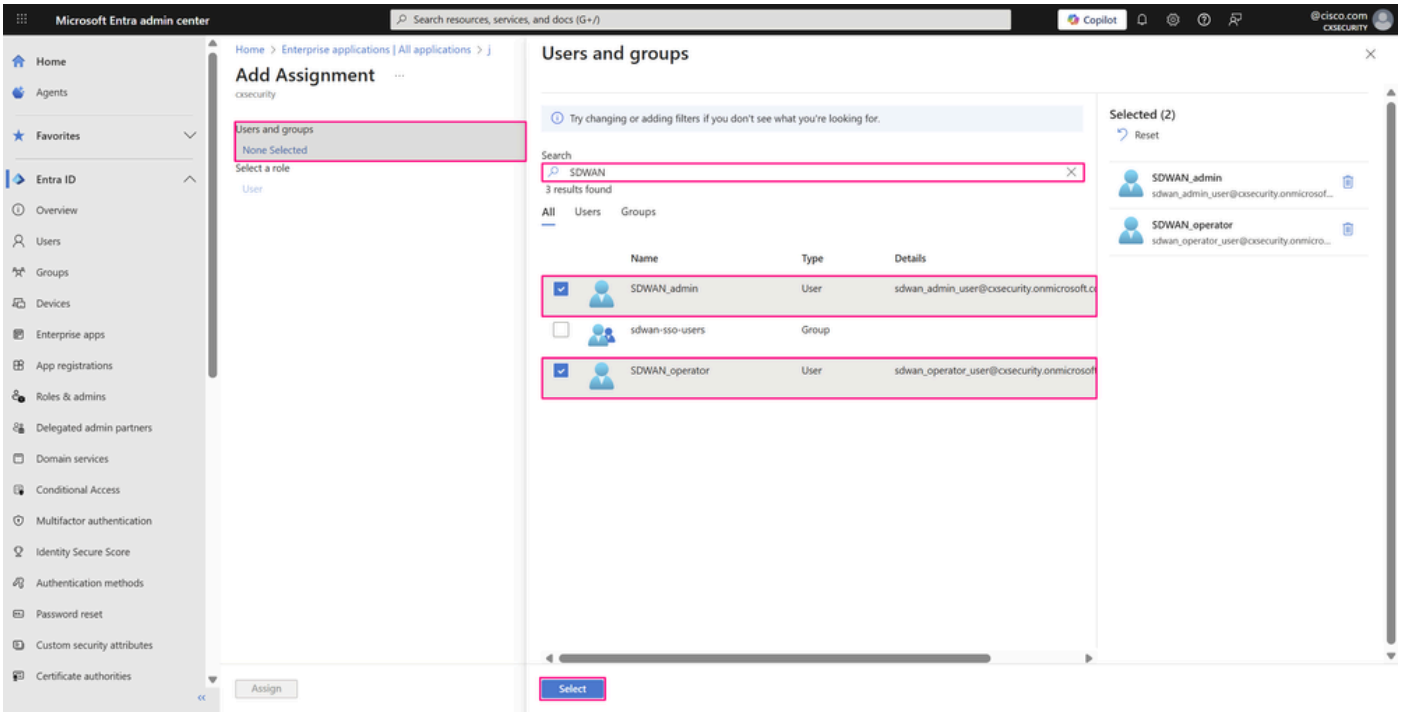
Page SSO with SAML Configuration

- Cliquez ensuite sur Add user/group.



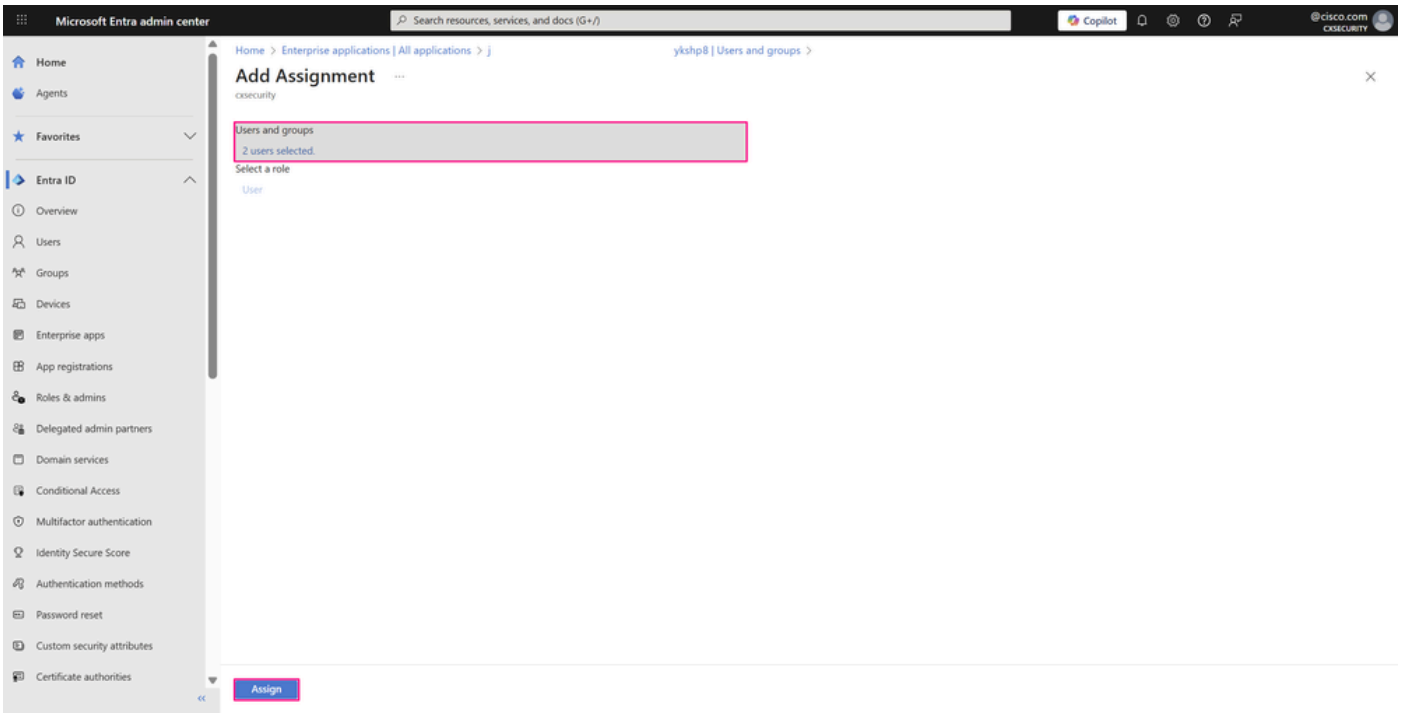
Page Utilisateur et groupes

- Dans le volet Ajouter une affectation, cliquez sur Aucun sélectionné sous le champ Utilisateurs et groupes. Recherchez et sélectionnez l'utilisateur ou le groupe que vous souhaitez affecter à votre application (dans notre exemple, les deux utilisateurs créés aux étapes précédentes), puis cliquez sur Sélectionner.



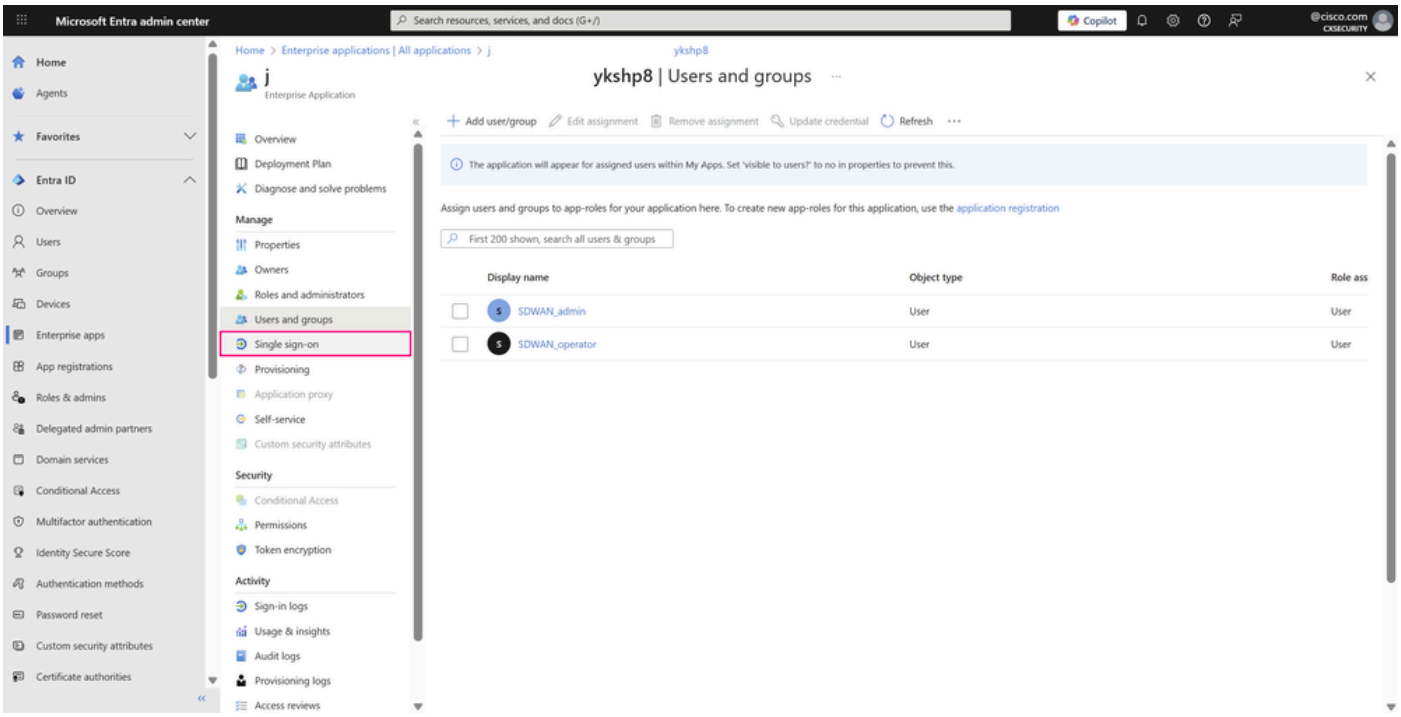
Volet Affectation d'utilisateurs/de groupes

- Cliquez sur Assign pour affecter l'utilisateur ou le groupe à l'application.



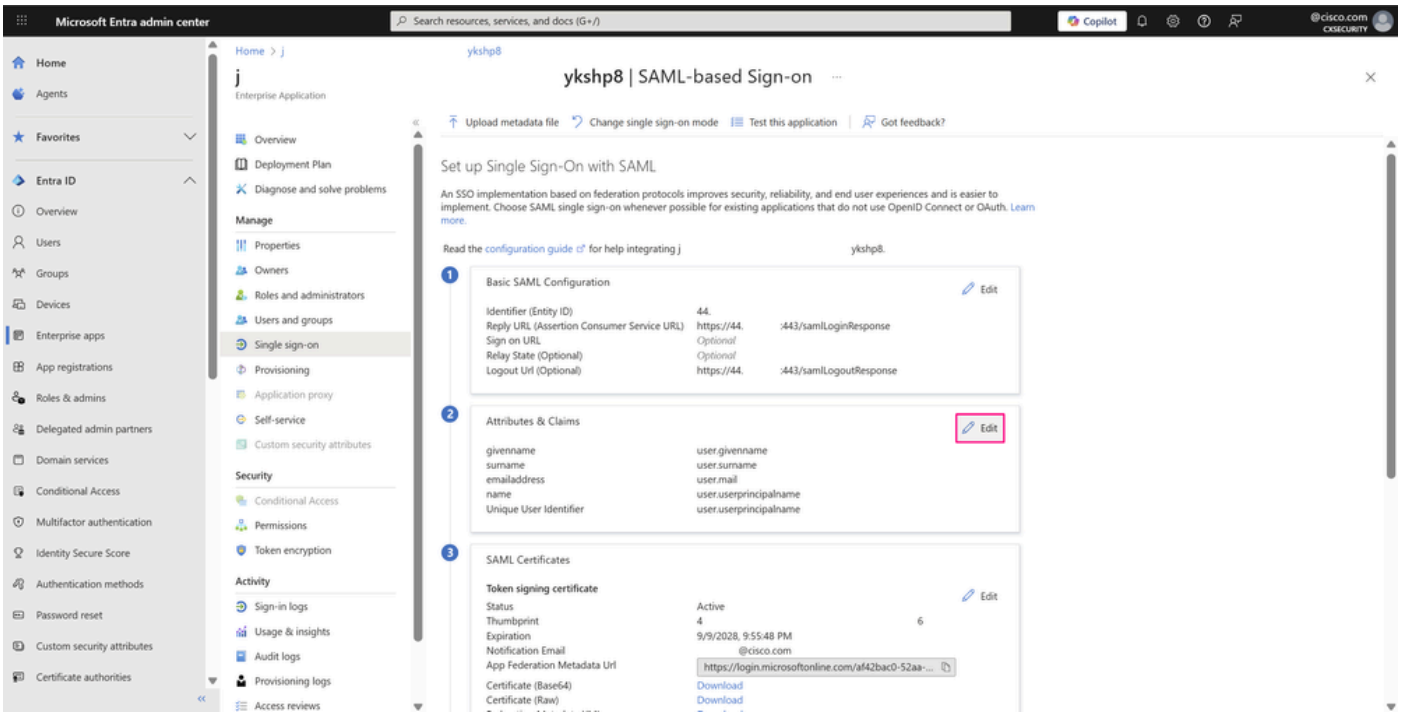
Volet Affectation d'utilisateurs/de groupes

- Les utilisateurs affectés à votre application d'entreprise sont répertoriés peu de temps après l'affectation. Cliquez sur Single sign-on dans la section Manage du menu de gauche pour accéder à la configuration SSO SAML de votre application et compléter la configuration requise restante.



Page Utilisateur et groupes

- Sur la page Configurer l'authentification unique avec SAML, sous Attributs et revendications, cliquez sur Modifier.

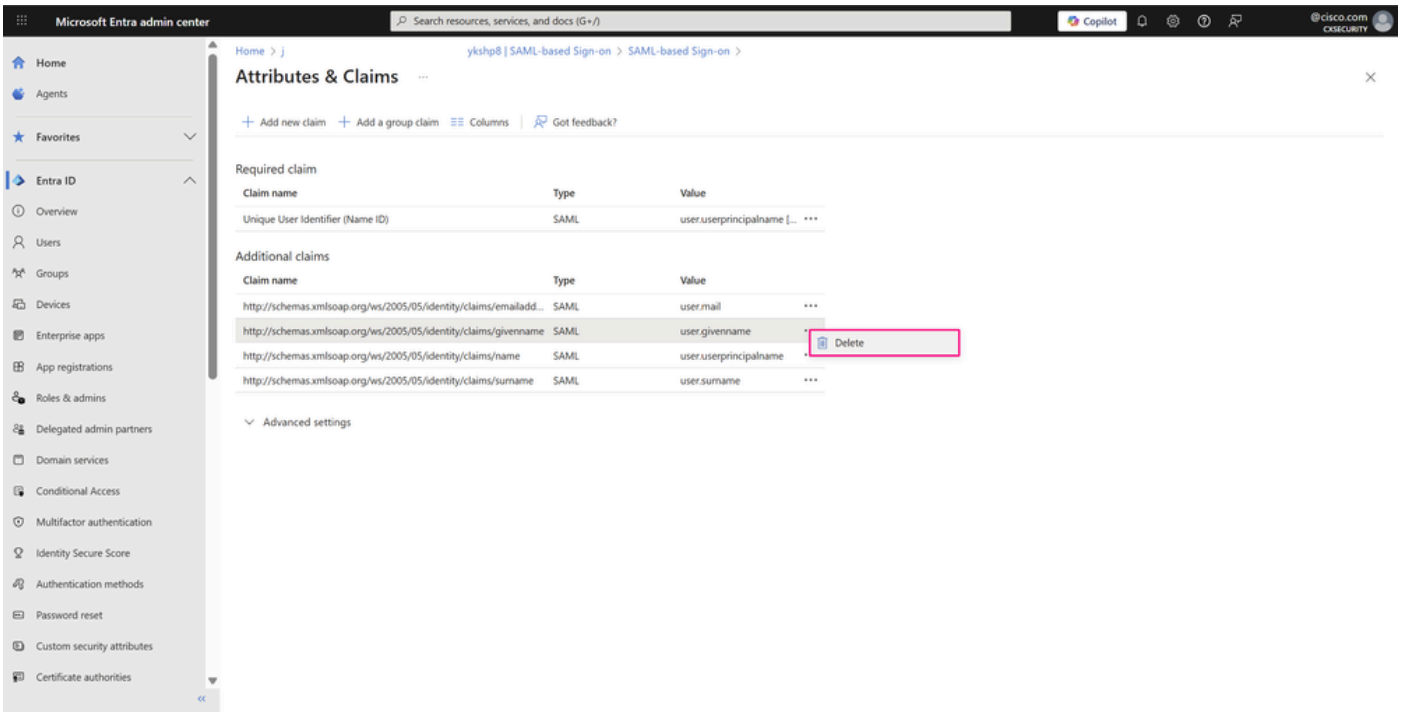


Page SSO with SAML Configuration

- Sur la page Attributs et revendications, cliquez sur l'icône en trois points, puis sur Supprimer pour supprimer la revendication avec la valeur user.givenname et la revendication avec la valeur user.surname, car elles ne sont pas nécessaires pour cet exemple.Seules les revendications suivantes sont requises pour l'authentification SSO de base avec votre application :
    - Adresse e-mail de l'utilisateur -user.mail
    - Nom d'utilisateur principal (UPN) de l'utilisateur -user.userprincipalname

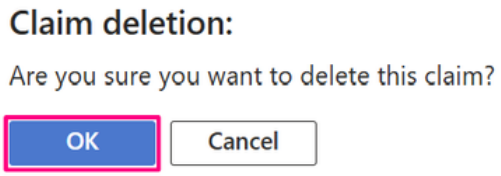
---

Remarque : Votre entreprise peut demander des demandes supplémentaires en fonction de ses besoins spécifiques.



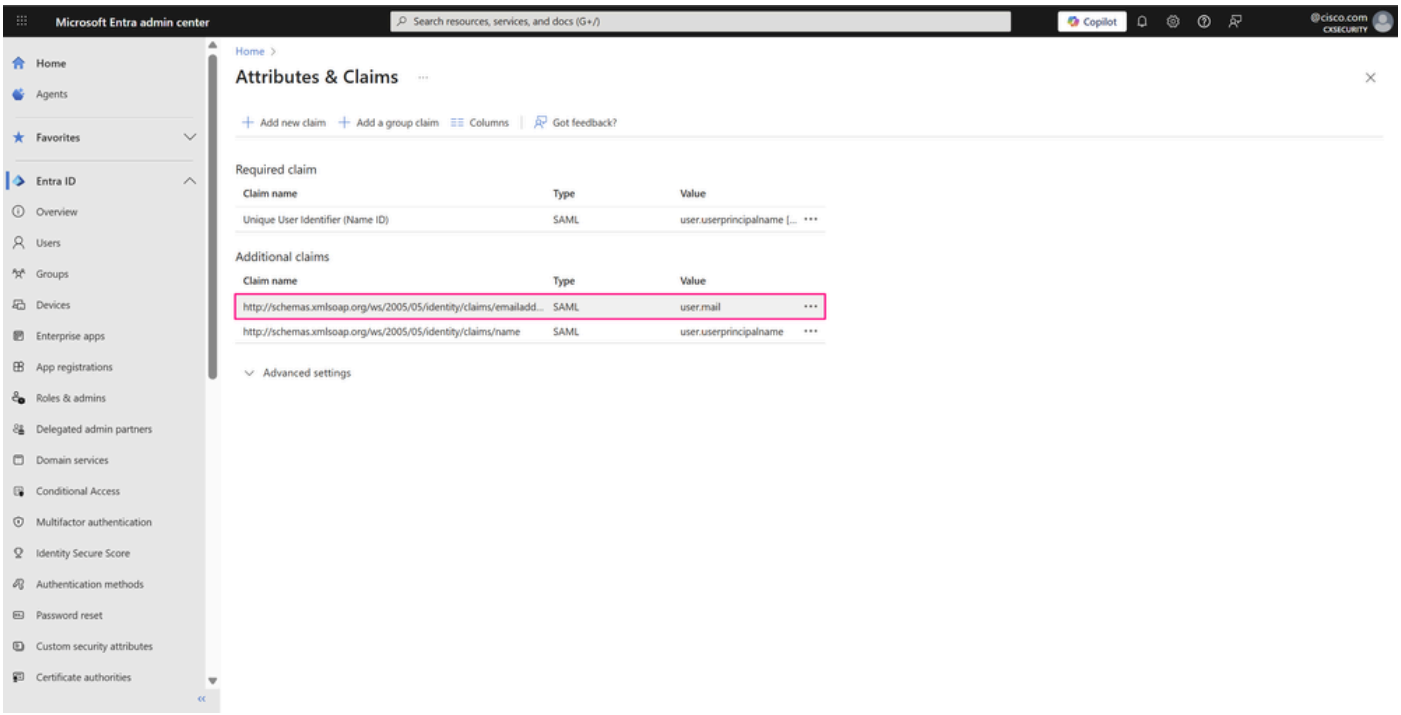
Page Attributs et revendications

- Dans la fenêtre Suppression de la demande, cliquez sur OK pour supprimer la demande.



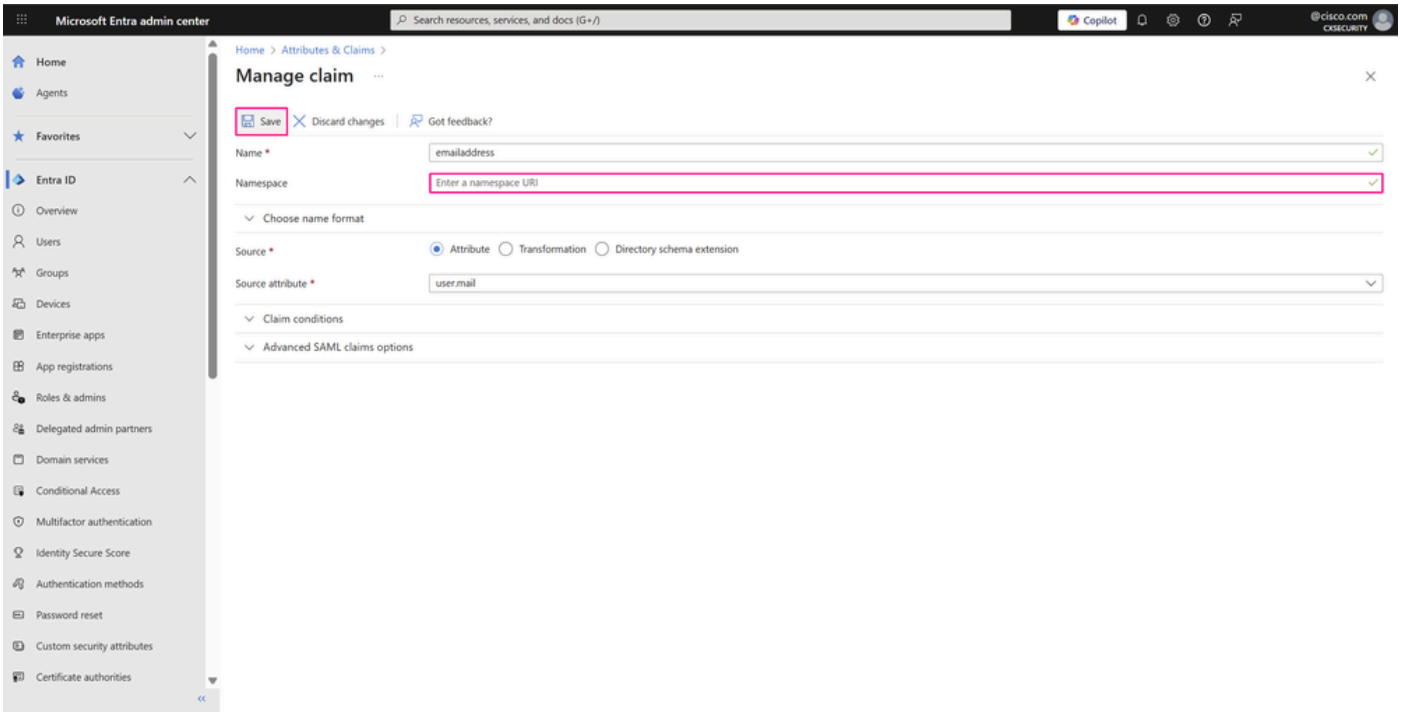
Fenêtre Suppression de demande

- Ensuite, supprimez l'espace de noms du nom de la revendication dans les deux revendications restantes, car ce champ est facultatif. Cette modification permet d'afficher sur cette page le nom réel de chaque élément afin de faciliter son identification. Passez le curseur sur chaque revendication et cliquez dessus pour accéder à ses paramètres.



Page Attributs et revendications

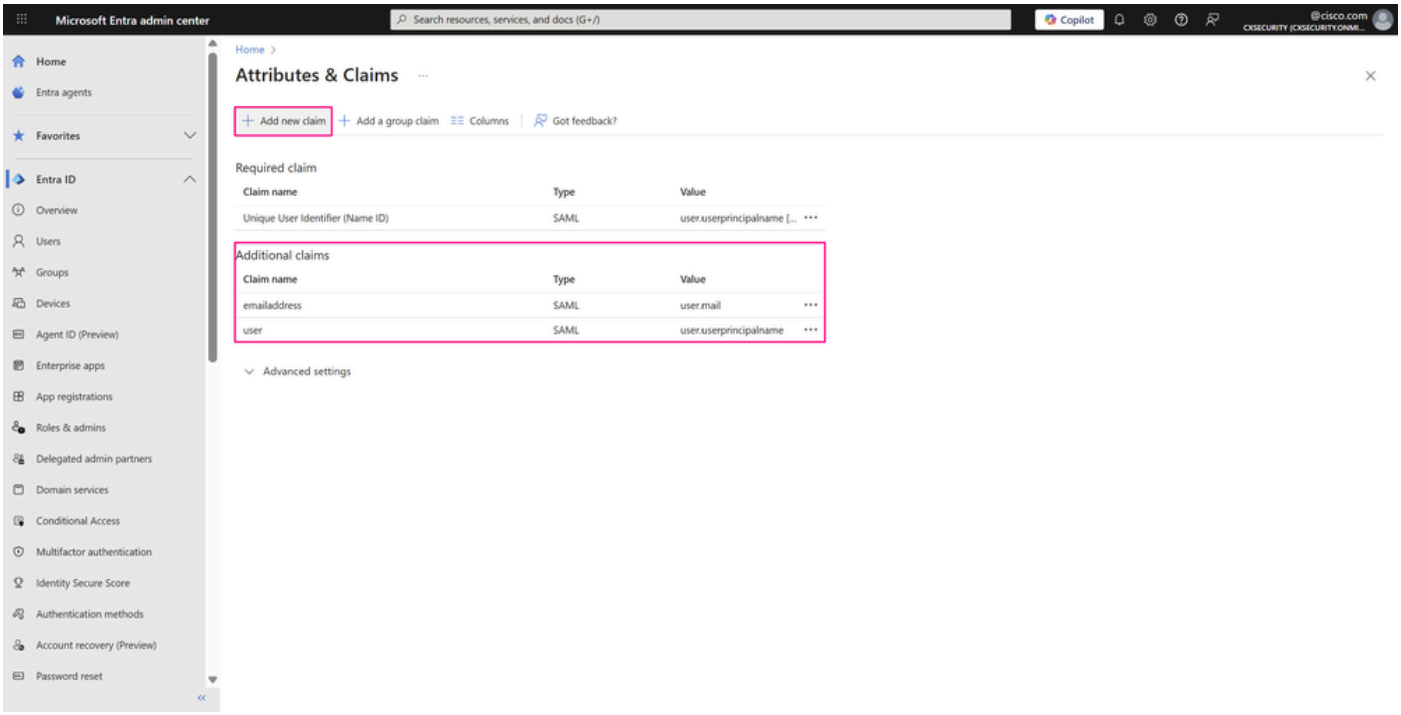
- Sur la page Gérer la revendication, supprimez le champ Espace de noms et cliquez sur Enregistrer pour appliquer les modifications.



Page Gérer la demande

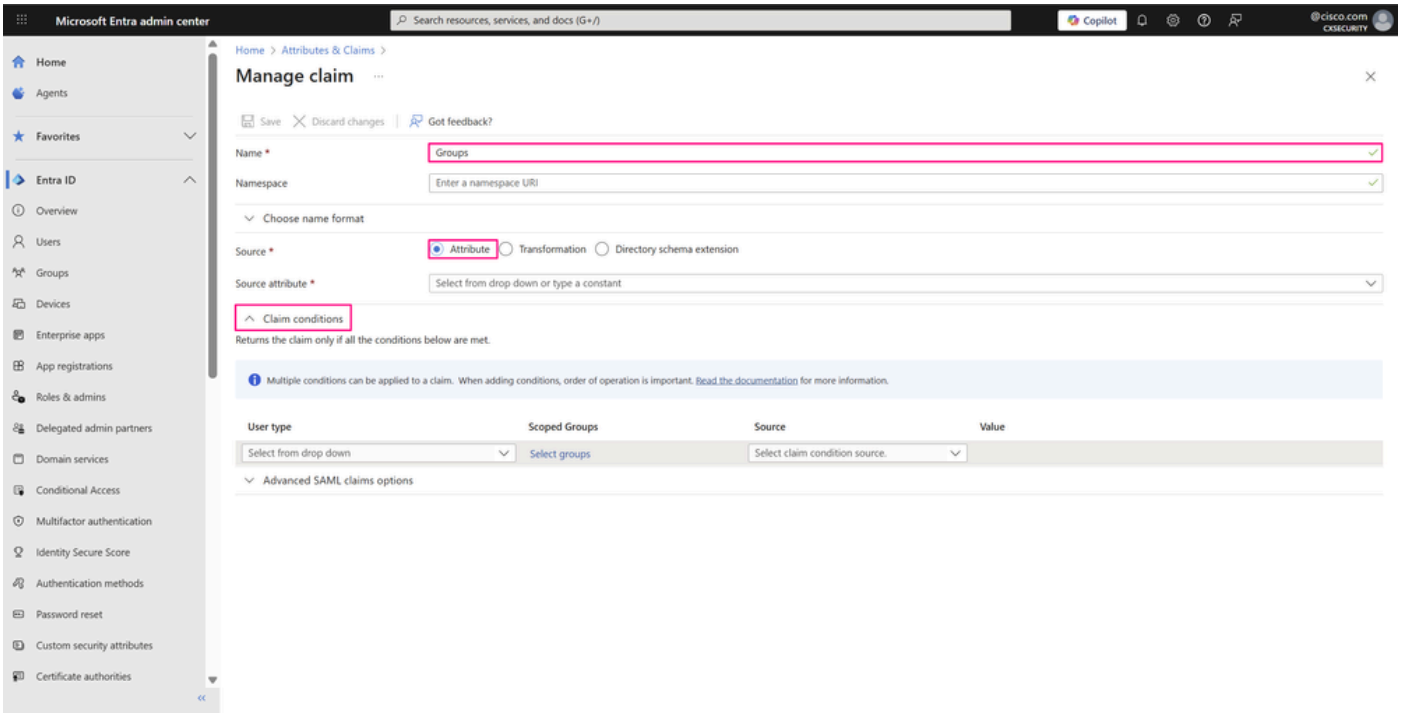
- Les noms des deux revendications requises sont maintenant visibles. Cependant, une autre revendication supplémentaire est toujours requise pour définir les groupes auxquels les utilisateurs appartiennent et qui sont autorisés à accéder aux ressources d'application. Pour ce faire, cliquez sur Ajouter une nouvelle demande.

Remarque : Dans cet exemple, user est choisi comme nom de demande UPN pour afficher l'adresse e-mail de l'utilisateur au lieu du format SAML NameID dans les détails du profil dans l'interface utilisateur de Cisco SD-WAN Manager.



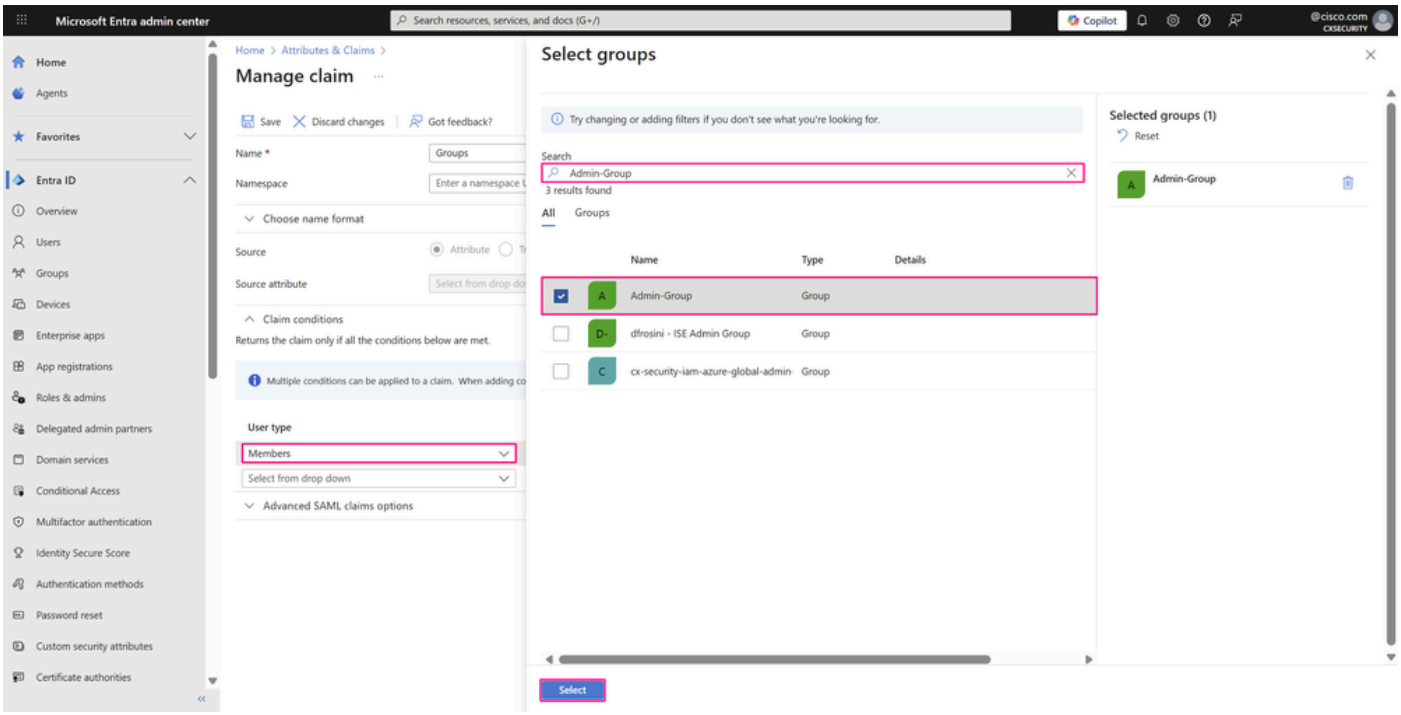
Page Attributs et revendications

- Entrez un nom pour identifier cette demande. En regard de Source, sélectionnez Attribute. Cliquez ensuite sur Réclamer des conditions pour développer les options et configurer plusieurs conditions.



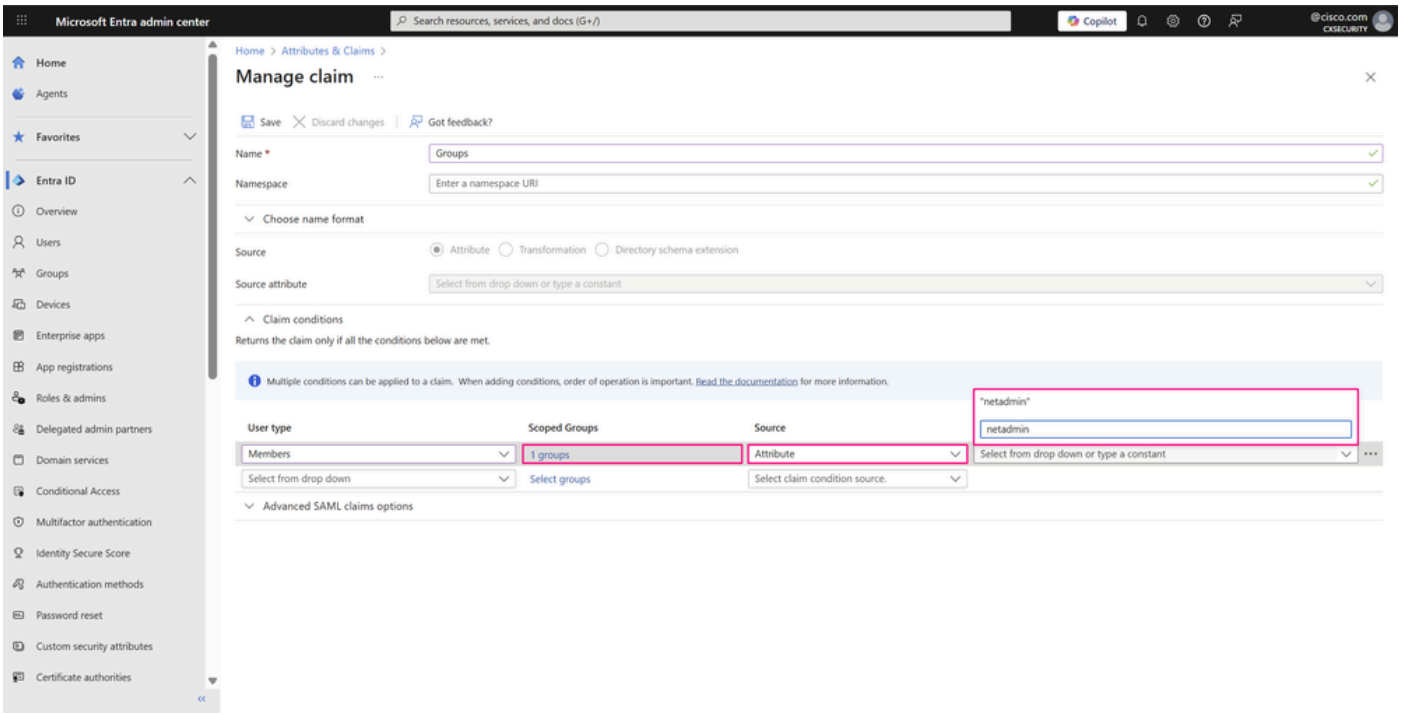
Page Gérer la demande

- Dans la condition de demande, choisissez Members dans la liste déroulante User type et cliquez sur Select Groups pour choisir le ou les groupes auxquels l'utilisateur doit appartenir, puis cliquez sur Select.



Page Gérer la demande

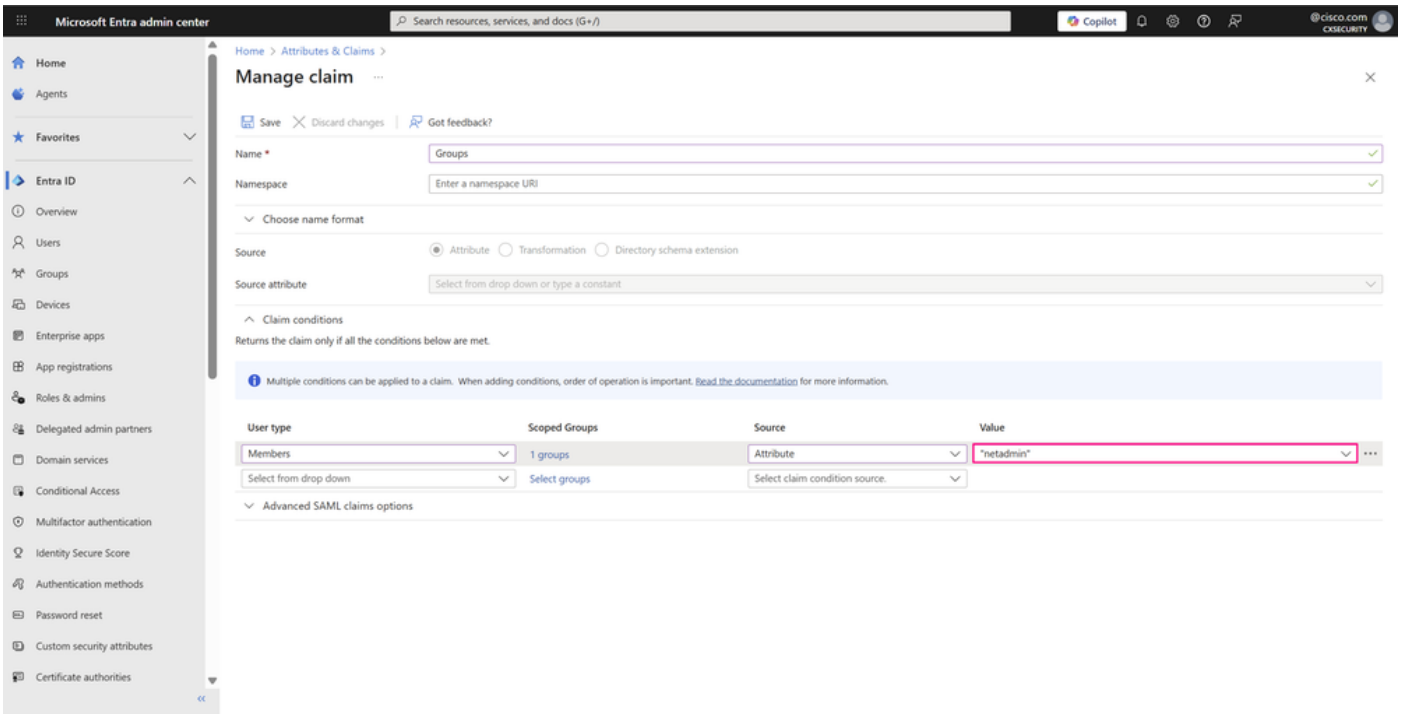
- Choisissez Attribut dans la liste déroulante Source où la revendication récupère sa valeur. Dans le champ Valeur, entrez l'attribut personnalisé de l'utilisateur qui référence le groupe d'utilisateurs défini dans votre application. Dans cet exemple, netadmin est l'un des groupes d'utilisateurs standard dans Cisco SD-WAN Manager. Entrez la valeur d'attribut sans guillemets et appuyez sur Entrée.



Page Gérer la demande

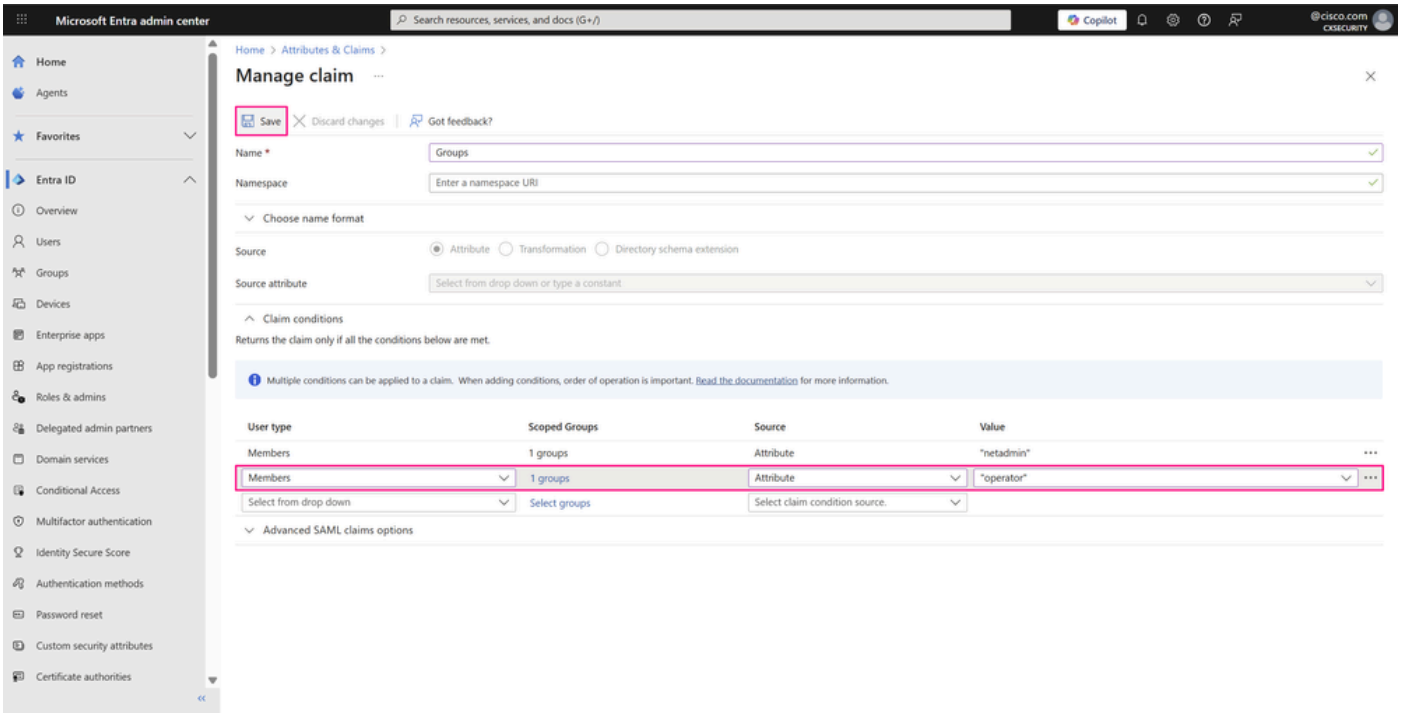
- Immédiatement après, la valeur de l'attribut apparaît entre guillemets car Microsoft Entra ID traite cette valeur sous forme de chaîne.

Remarque : Ces paramètres dans les conditions de demande sont très pertinents dans la configuration SSO SAML de l'application d'entreprise, car ces attributs personnalisés doivent toujours correspondre aux groupes d'utilisateurs définis dans Cisco SD-WAN Manager. Cette correspondance détermine les privilèges ou autorisations accordés aux utilisateurs en fonction du groupe auquel ils appartiennent sur l'ID Microsoft Entra.



Page Gérer la demande

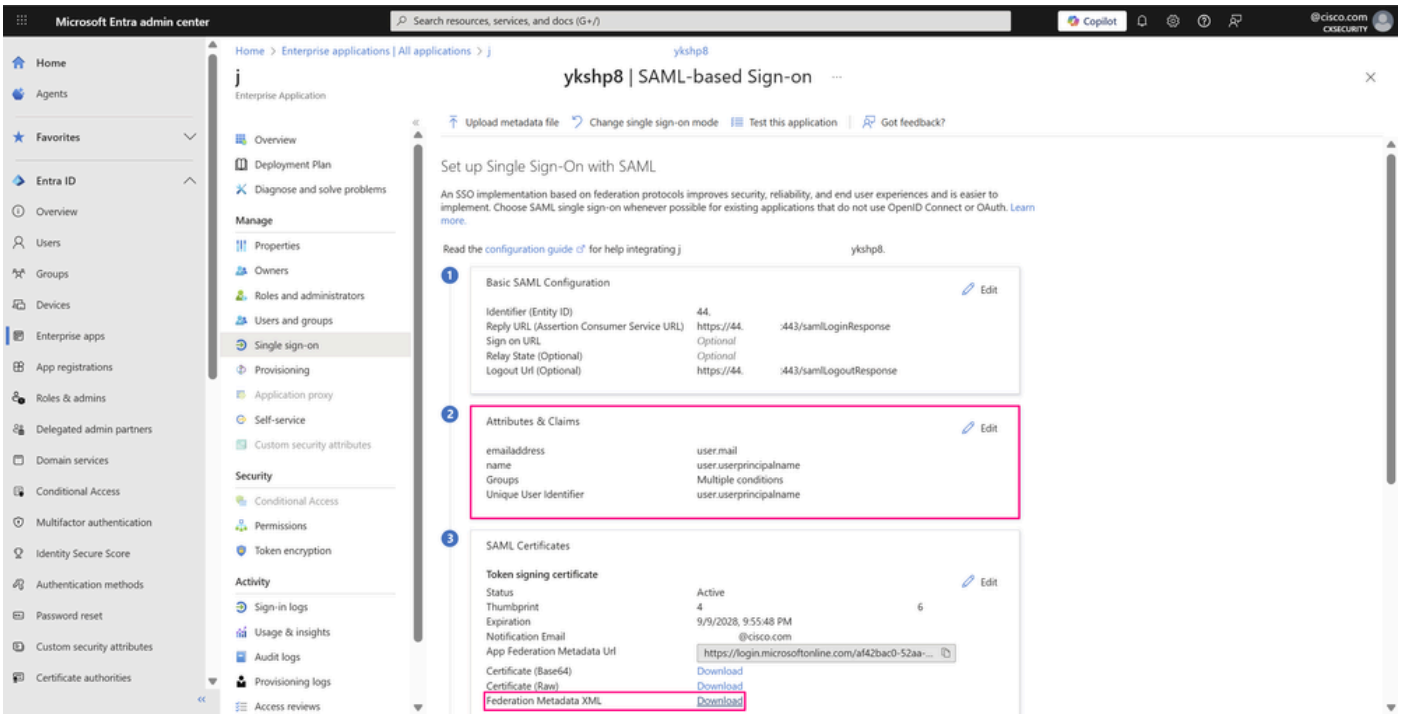
- Répétez les mêmes étapes pour une deuxième condition de revendication pour le deuxième groupe créé, qui correspond au groupe d'utilisateurs opérateur dans Cisco SD-WAN Manager. Ce processus est requis pour chaque groupe différent disposant d'autorisations spécifiques que vous souhaitez connecter à l'application. Vous pouvez également ajouter plusieurs groupes dans une seule condition. Cliquez sur Save pour enregistrer les modifications.



Page Gérer la demande

- Sur la page Configurer l'authentification unique avec SAML, la section Attributs et

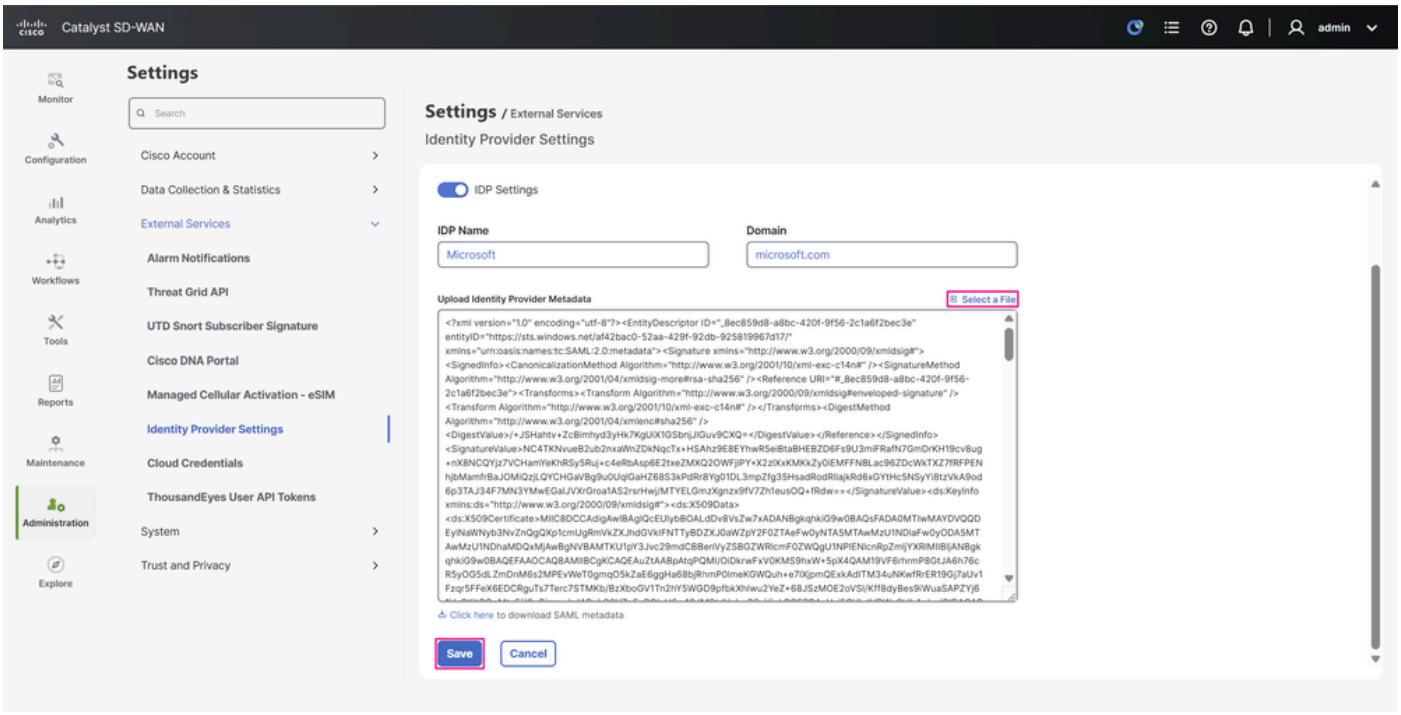
revendications affiche les nouvelles modifications apportées. Pour terminer la configuration dans l'ID Microsoft Entra, sous Certificats SAML, cliquez sur Télécharger en regard de Métadonnées de fédération XML pour télécharger le fichier XML qui fournit des services d'identité à l'application.



Page SSO with SAML Configuration

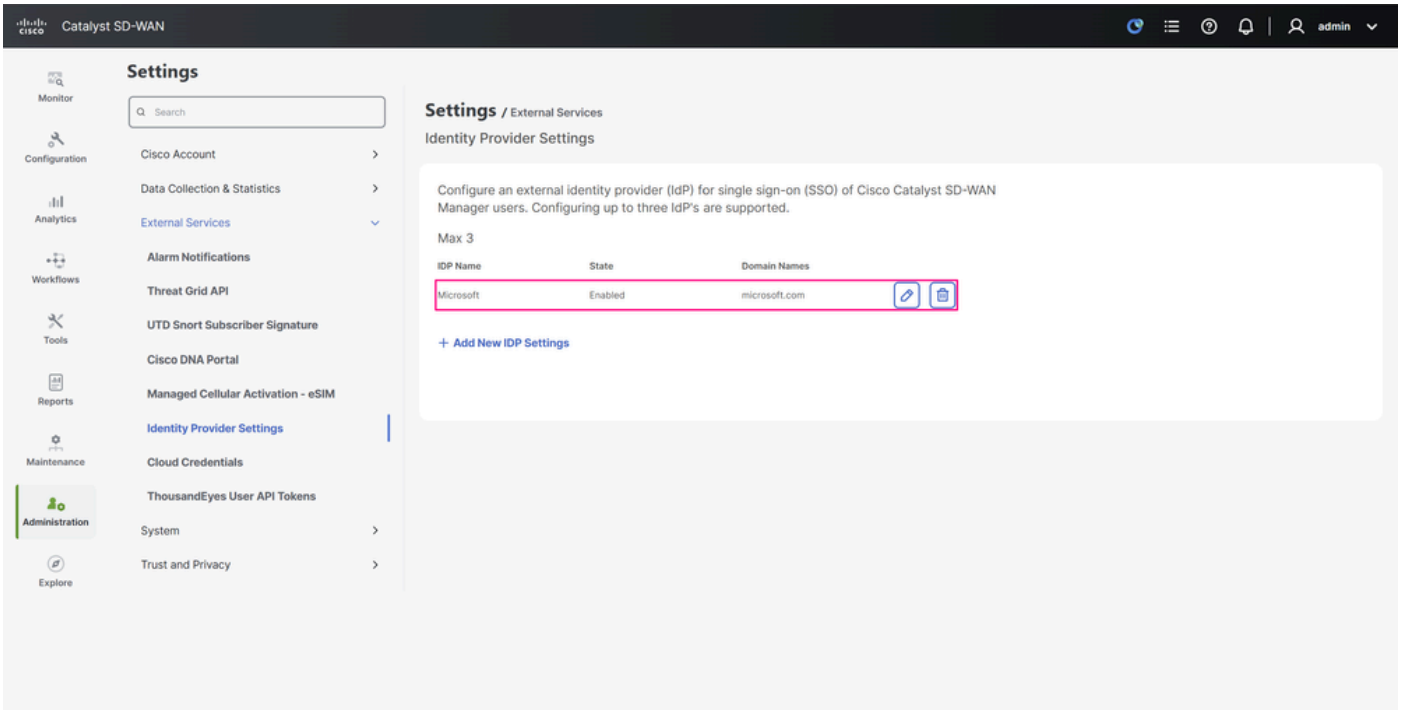
Étape 5. Importation du fichier de métadonnées SAML Microsoft Entra ID dans Cisco SD-WAN Manager

- Pour télécharger les métadonnées de fédération dans Cisco SD-WAN Manager, accédez à Administration > Settings > External Services > Identity Provider Settings et cliquez sur Select a file. Choisissez le fichier que vous venez de télécharger à partir de Microsoft Entra ID, puis cliquez sur Enregistrer.



Page Configuration des paramètres IdP

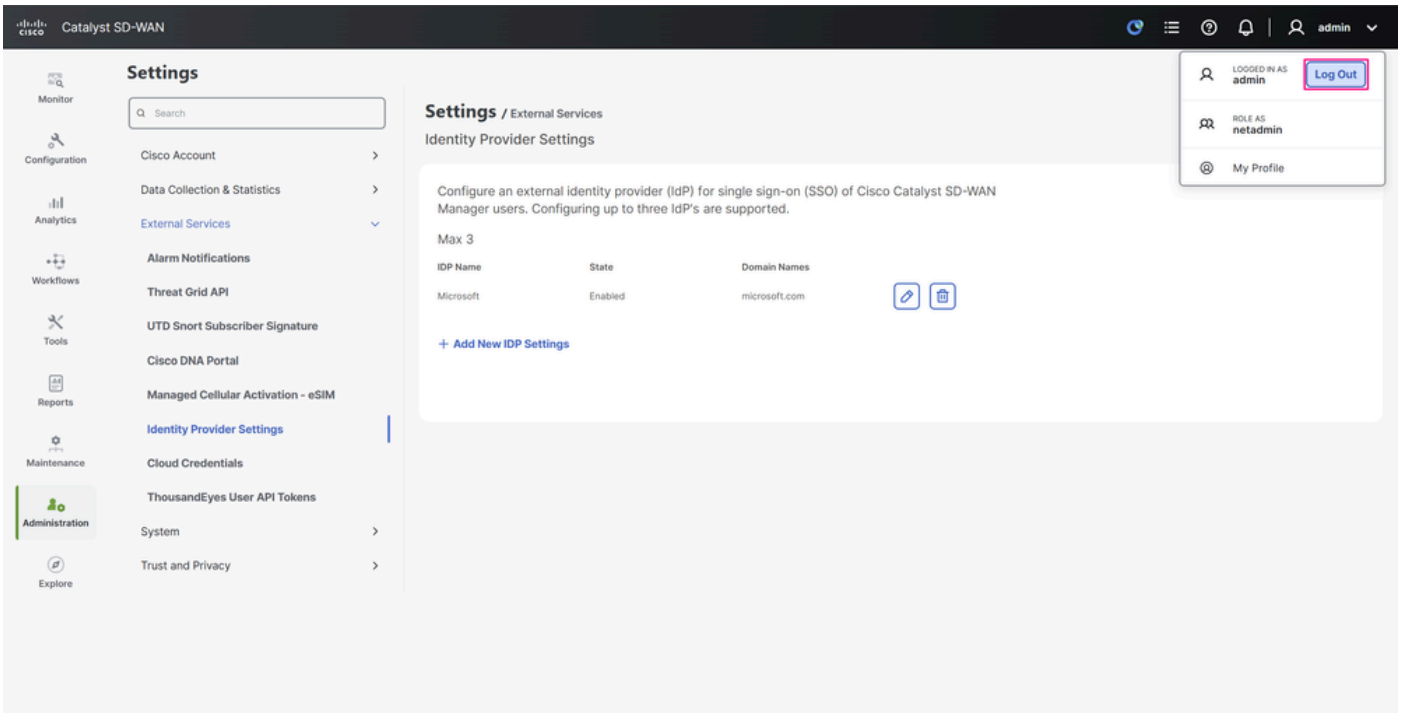
- Les paramètres et métadonnées du fournisseur d'identité sont maintenant enregistrés.



Page Configuration des paramètres IdP

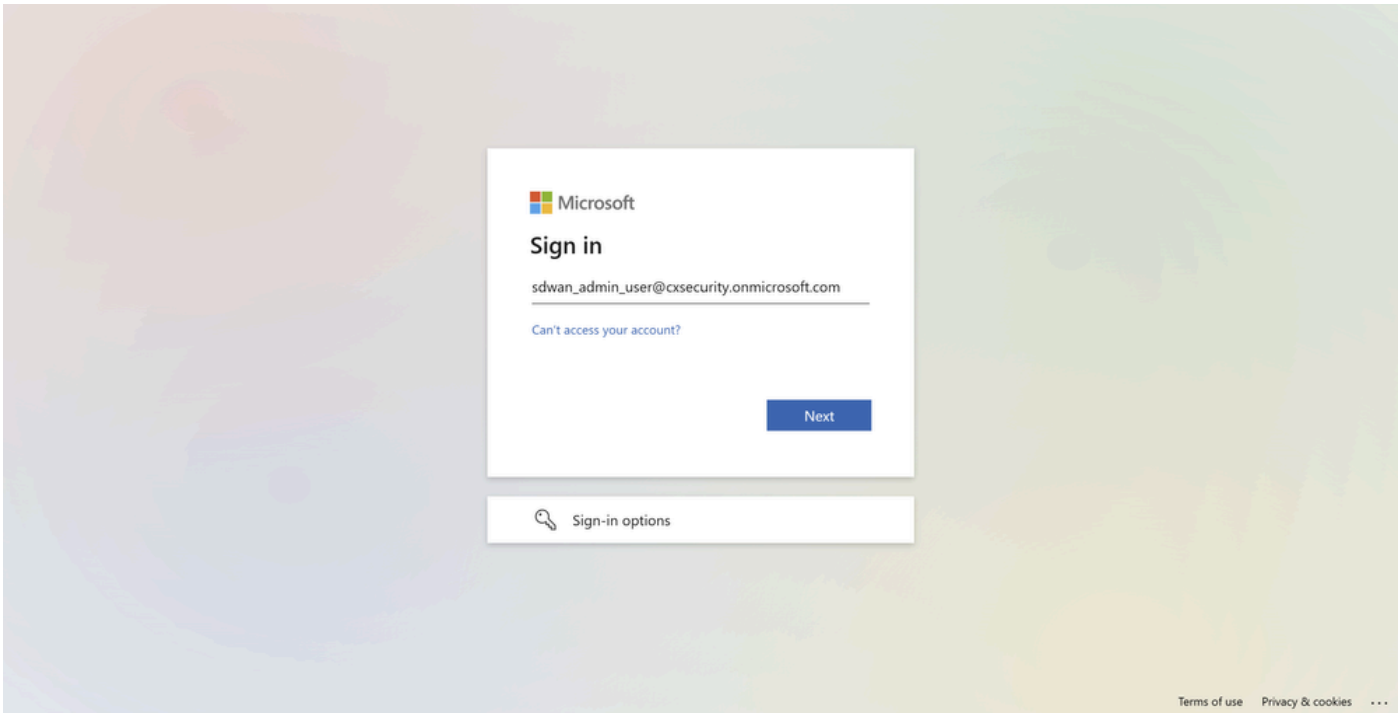
Vérifier

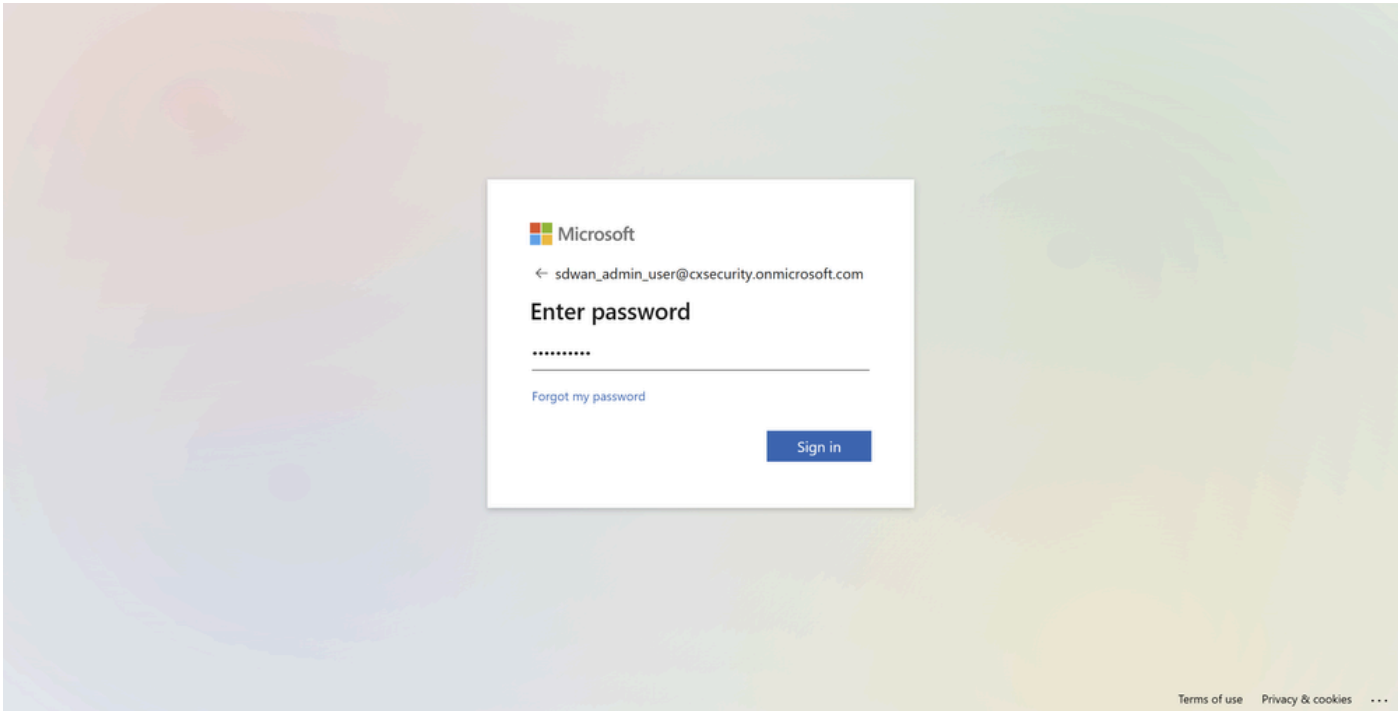
- Cliquez sur le nom de votre profil dans le coin supérieur droit de l'interface utilisateur pour développer les options, puis cliquez sur Déconnexion pour vous déconnecter du portail.



Menu Profil

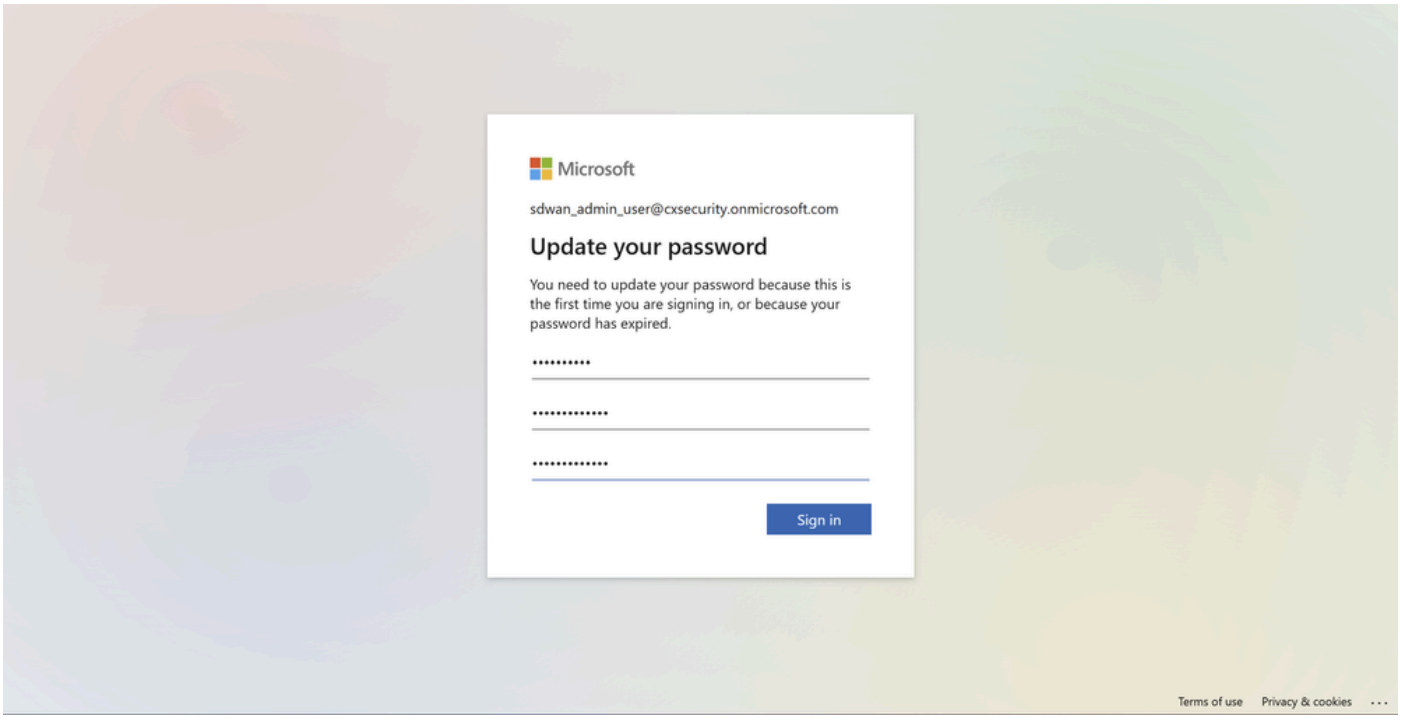
- Vous êtes immédiatement redirigé vers l'écran d'authentification Microsoft, où vous vous connectez avec les informations d'identification des utilisateurs SSO Microsoft Entra ID.





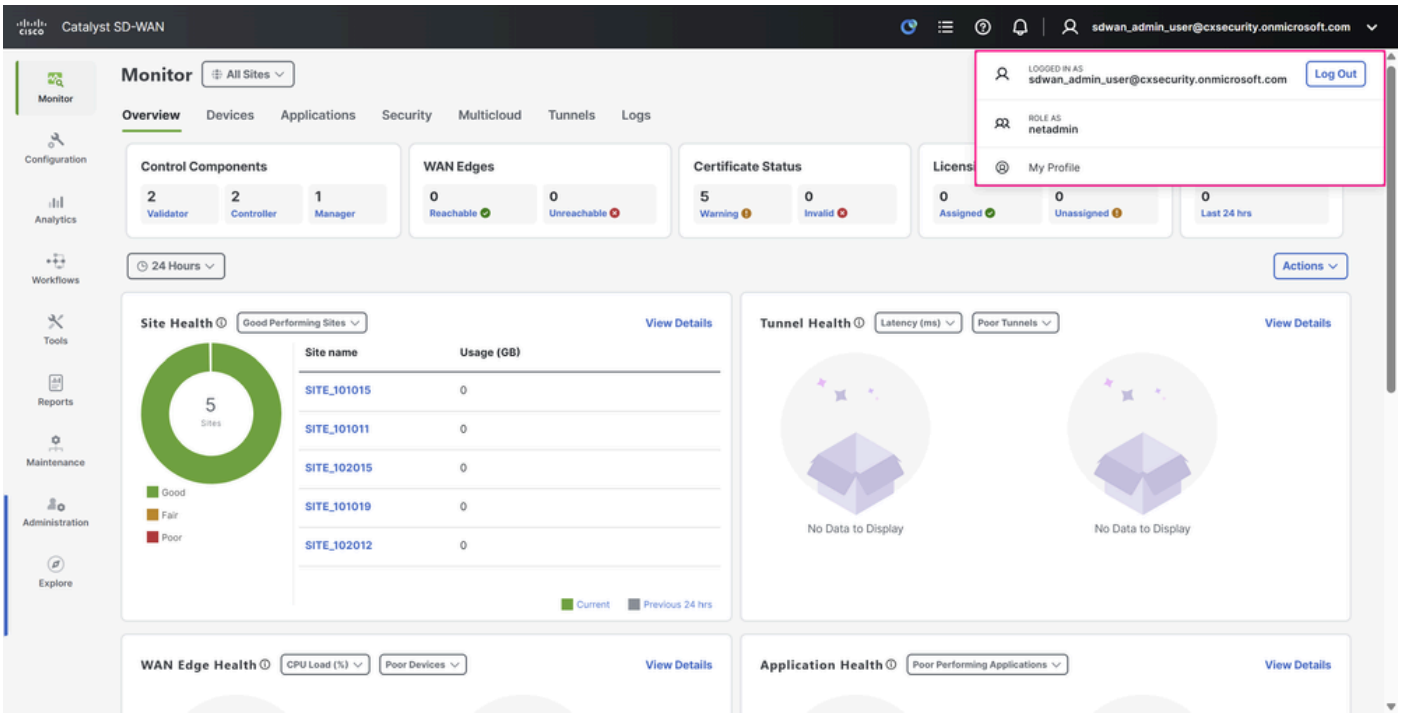
Écran de connexion Microsoft

- Étant donné que c'est la première fois que l'utilisateur SSO se connecte, l'invite demande un changement de mot de passe.



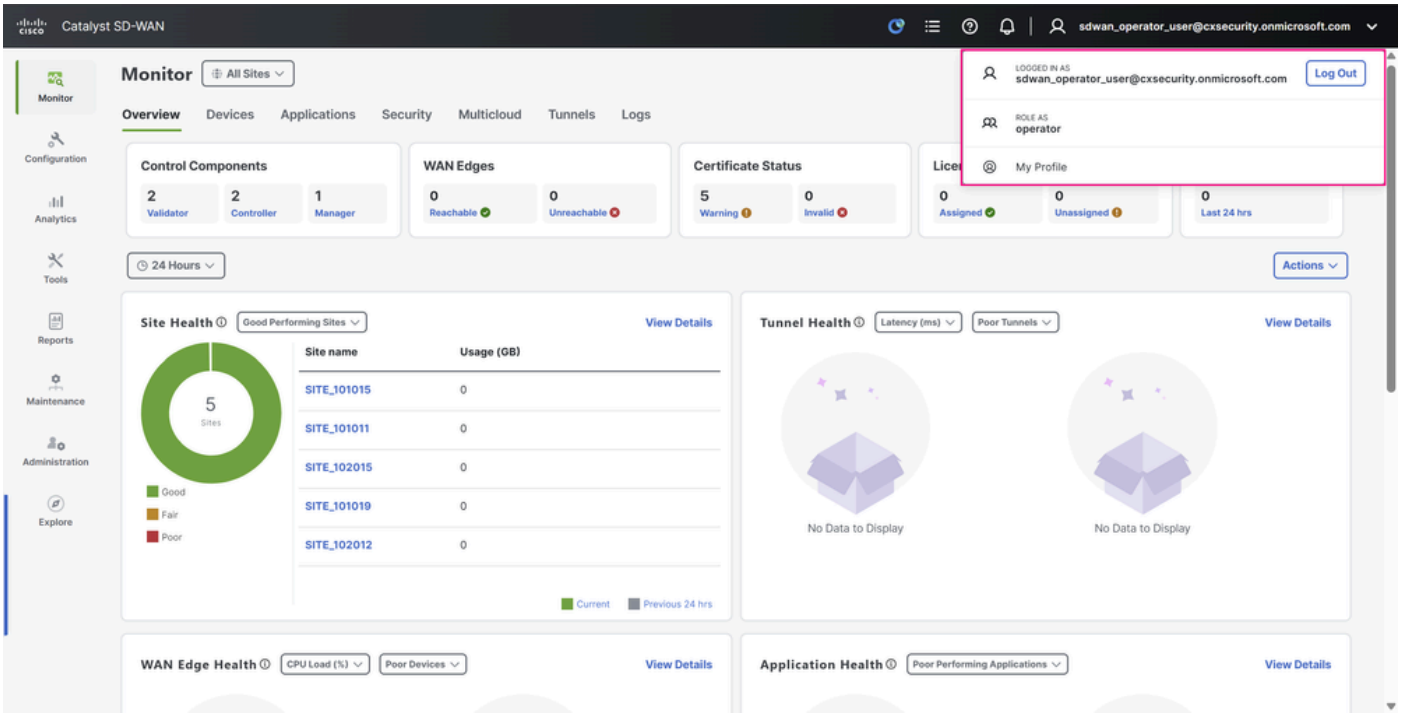
Écran de connexion Microsoft

- Après une connexion réussie, développez à nouveau les détails de votre profil dans le coin supérieur droit du tableau de bord, et vous pouvez confirmer que l'utilisateur est détecté avec un rôle netadmin, exactement comme configuré dans l'ID Microsoft Entra.



Interface utilisateur de Cisco SD-WAN Manager

- Enfin, effectuez le même test de connexion avec l'autre utilisateur. Vous voyez le même comportement : l'utilisateur est maintenant identifié avec le rôle opérateur.



Interface utilisateur de Cisco SD-WAN Manager

Informations connexes

- [Configuration de l'authentification unique sur Cisco IOS XE Catalyst SD-WAN]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.