Konfigurieren von SSO für SD-WAN mit Microsoft Entra-ID

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der einmaligen Anmeldung (Single Sign-On, SSO) für Cisco Catalyst Software-Defined Wide-Area Networks (SD-WAN) mit Microsoft Entra ID beschrieben.

Voraussetzungen

Anforderungen

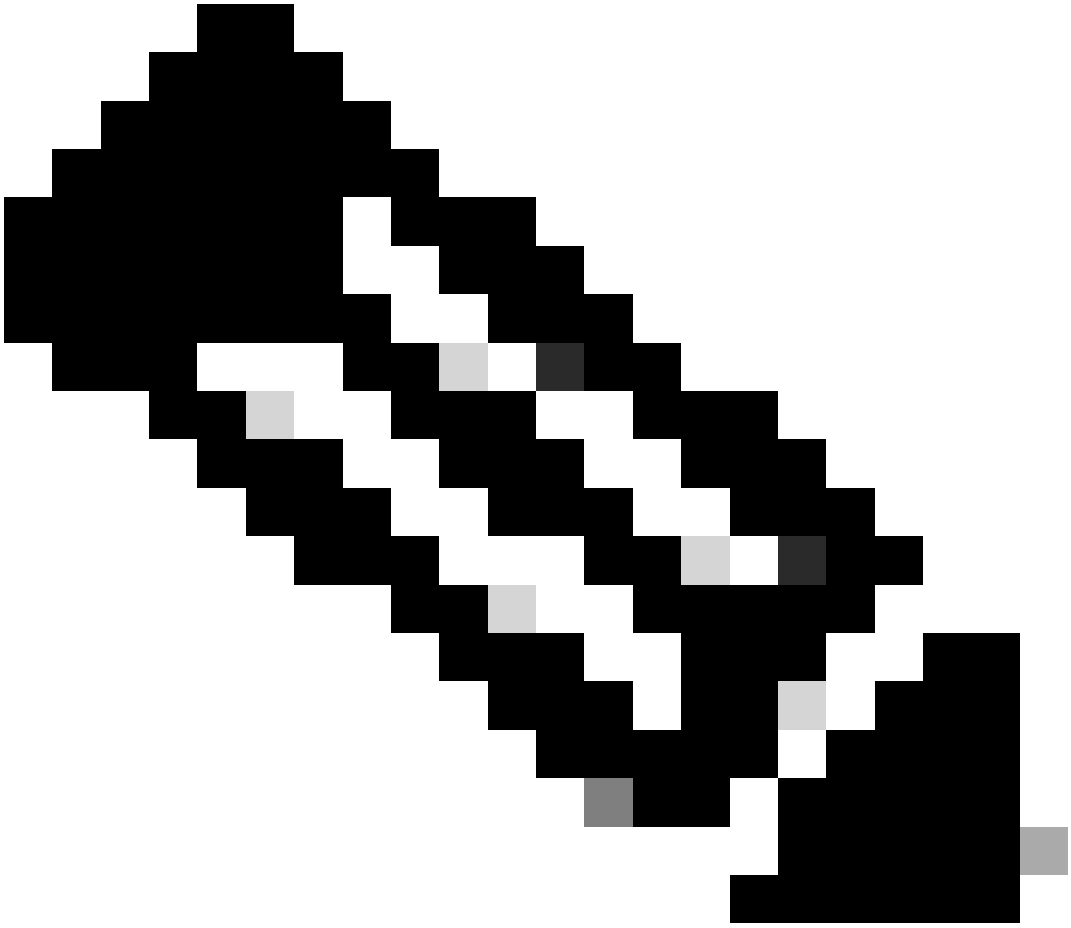
Cisco empfiehlt, dass Sie mit den folgenden Themen allgemein vertraut sind:

- Einmalige Anmeldung
- Cisco Catalyst SD-WAN-Lösung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Cisco Catalyst SD-WAN Manager Version 20.15.3.1
- Microsoft Entra-ID



Anmerkung: Die Lösung, die früher Azure Active Directory (Azure AD) hieß, heißt jetzt Microsoft Entra ID.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Single Sign-On ist eine Authentifizierungsmethode, mit der Benutzer mit einem einzigen Satz von Anmeldeinformationen sicher auf mehrere unabhängige Anwendungen oder Websites zugreifen können. Mit SSO müssen sich Benutzer nicht mehr bei jeder Anwendung separat anmelden. Nach der Authentifizierung können sie nahtlos auf alle zulässigen Ressourcen zugreifen.

Eine gängige Methode zur Implementierung von SSO ist der Verbund, der mithilfe von Protokollen wie SAML 2.0, WS-Federation oder OpenID Connect die Vertrauenswürdigkeit zwischen einem

Identitätsanbieter (IdP) und einem Dienstanbieter (SP) herstellt. Der Verbund verbessert die Sicherheit, Zuverlässigkeit und Benutzerfreundlichkeit durch die Zentralisierung der Authentifizierung.

Microsoft Entra ID ist ein weit verbreiteter Cloud-basierter Identitätsanbieter, der diese Verbundprotokolle unterstützt. In einer SSO-Konfiguration mit Cisco Catalyst SD-WAN fungiert die Microsoft Entra ID als IDp und der Cisco SD-WAN Manager als Service Provider.

Die Integration funktioniert wie folgt:

1. Ein Netzwerkadministrator versucht, sich beim Cisco SD-WAN Manager anzumelden.
2. Der Cisco SD-WAN Manager sendet eine Authentifizierungsanforderung an die Microsoft Entra-ID.
3. Microsoft Entra ID fordert den Administrator auf, sich mit seinem Entra ID (Microsoft)-Konto zu authentifizieren.
4. Nach der Validierung der Anmeldeinformationen sendet die Microsoft Entra ID eine sichere Antwort an den Cisco SD-WAN Manager zurück und bestätigt die Authentifizierung.
5. Der Cisco SD-WAN Manager gewährt den Zugriff ohne separate Anmeldedaten.

In diesem Modell:

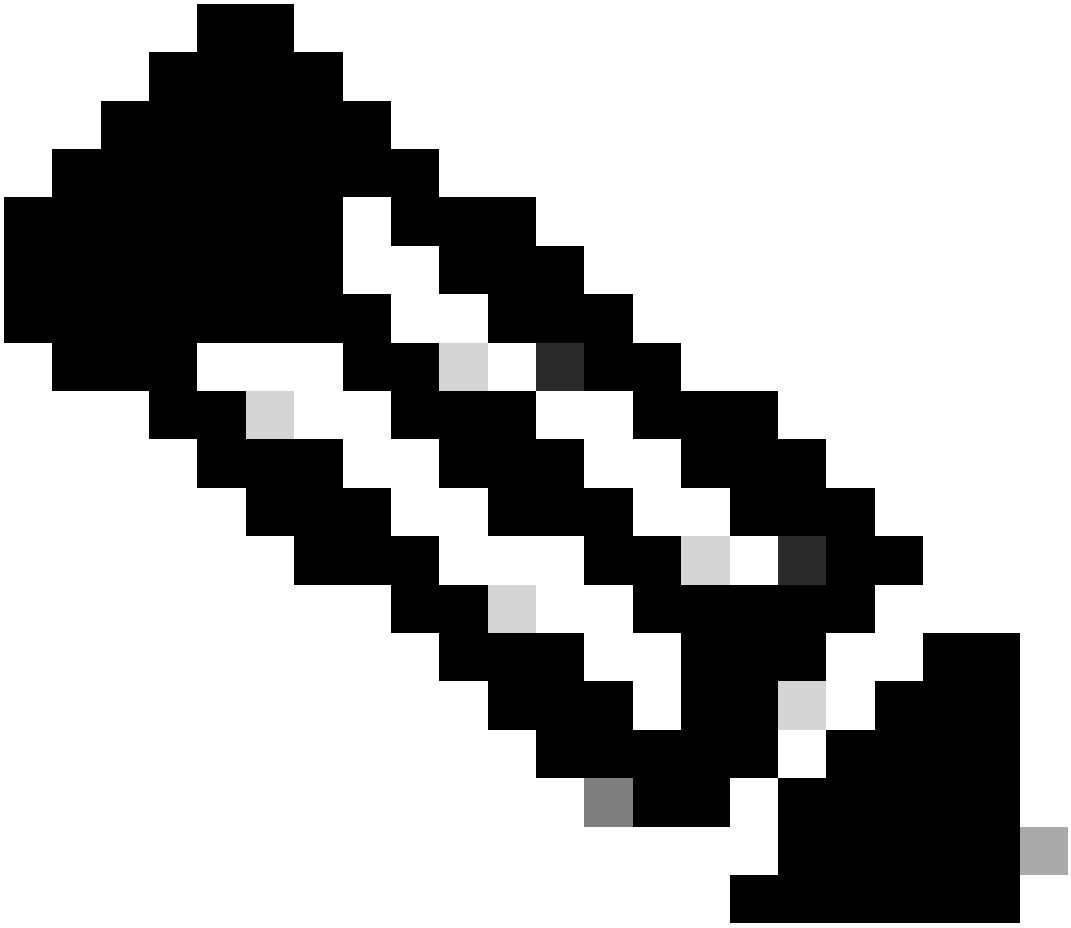
- Identity Provider (IdP) - Speichert Benutzerdaten und validiert Anmeldeinformationen (z. B. Microsoft Entra ID, Okta, PingID, ADFS).
- Service Provider - Hostet die Anwendung, auf die zugegriffen werden soll (z. B. Cisco SD-WAN Manager).
- Benutzer - Verfügen über ein Konto im IdP-Verzeichnis und sind zum Zugriff auf den Dienstanbieter autorisiert.

Cisco Catalyst SD-WAN ist kompatibel mit allen SAML 2.0-kompatiblen IdP, wenn die Konfiguration den Branchenstandards entspricht.

Vorteile der einmaligen Anmeldung

- Zentralisiert die Verwaltung der Anmeldeinformationen über den Identitätsanbieter.
- Stärkt die Authentifizierungssicherheit, indem mehrere schwache Passwörter entfernt werden.
- Optimiert den sicheren Zugriff für Administratoren.
- Ermöglicht den Zugriff per Mausklick auf den Cisco Catalyst SD-WAN Manager und andere autorisierte Anwendungen.

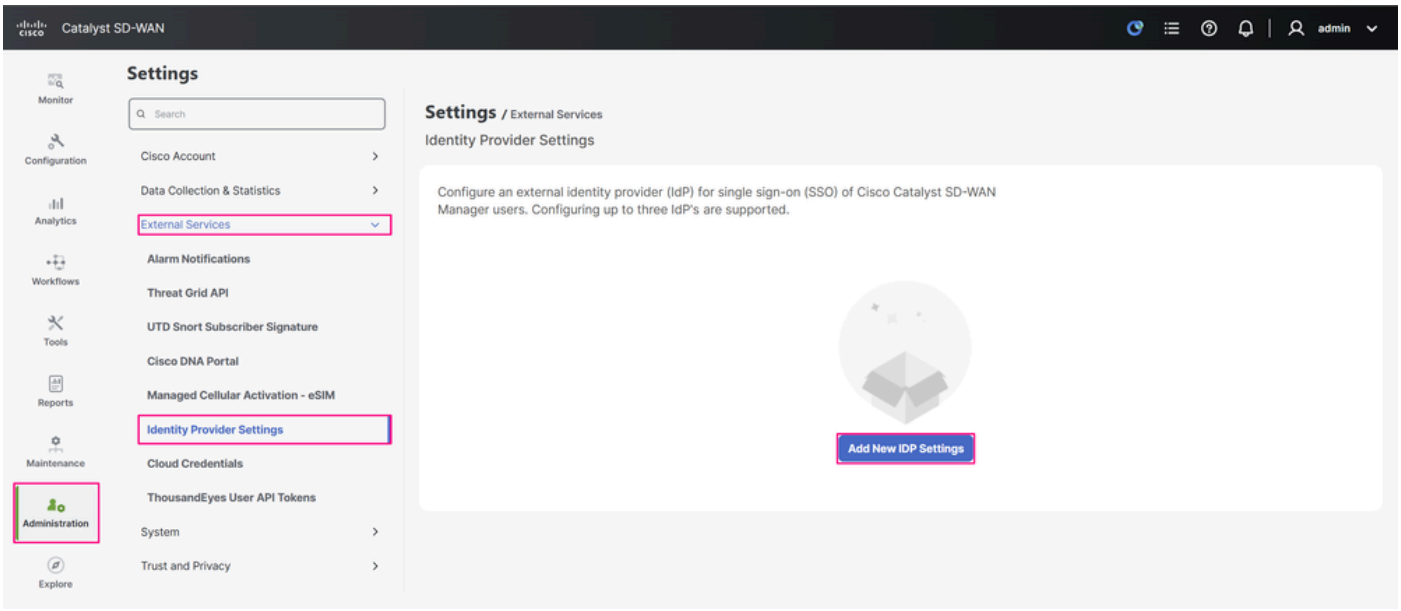
Konfigurieren



Anmerkung: Unterstützte Mindestversion: Cisco Catalyst SD-WAN Manager Version 20.8.1

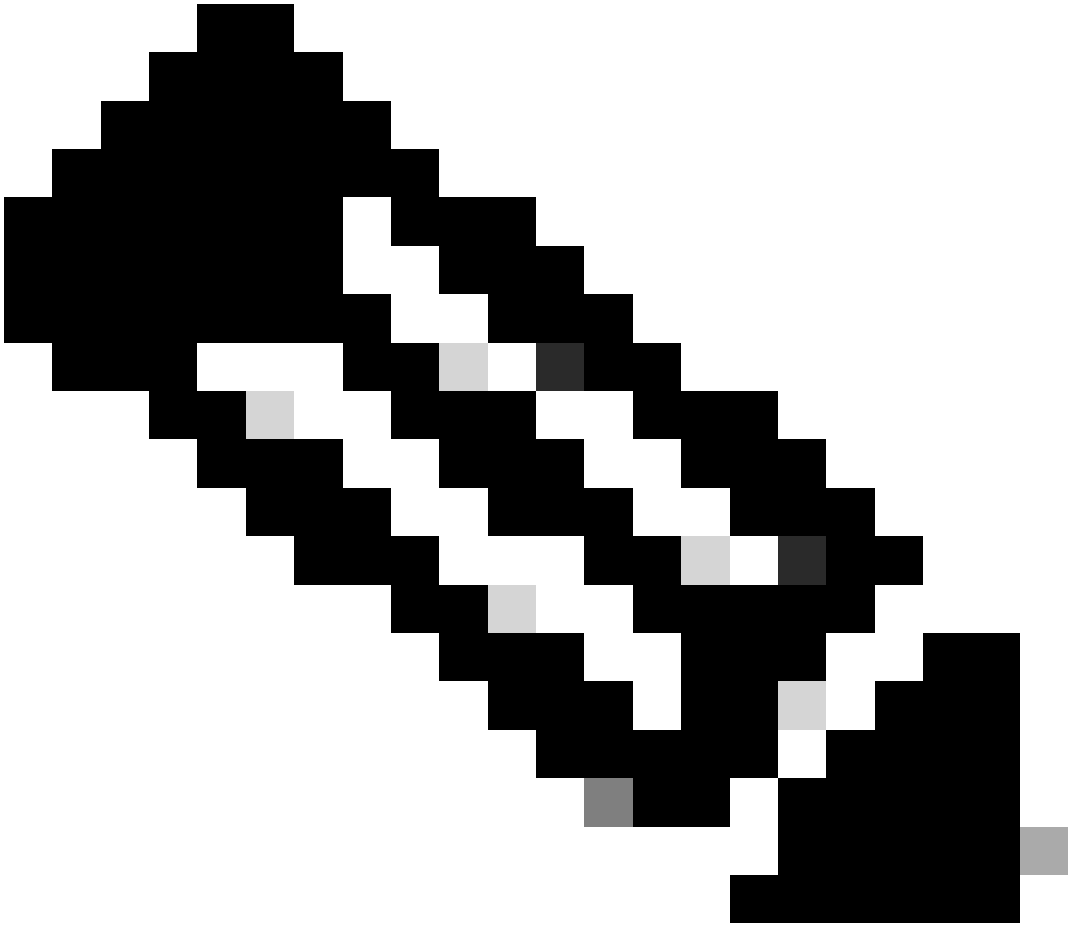
Schritt 1: Abrufen der SAML-Metadaten des Cisco SD-WAN-Managers

- Navigieren Sie im Cisco SD-WAN Manager zu Administration > Settings > External Services > Identity Provider Settings, und klicken Sie auf Add New IDP Settings.



Benutzeroberfläche des Cisco SD-WAN-Managers

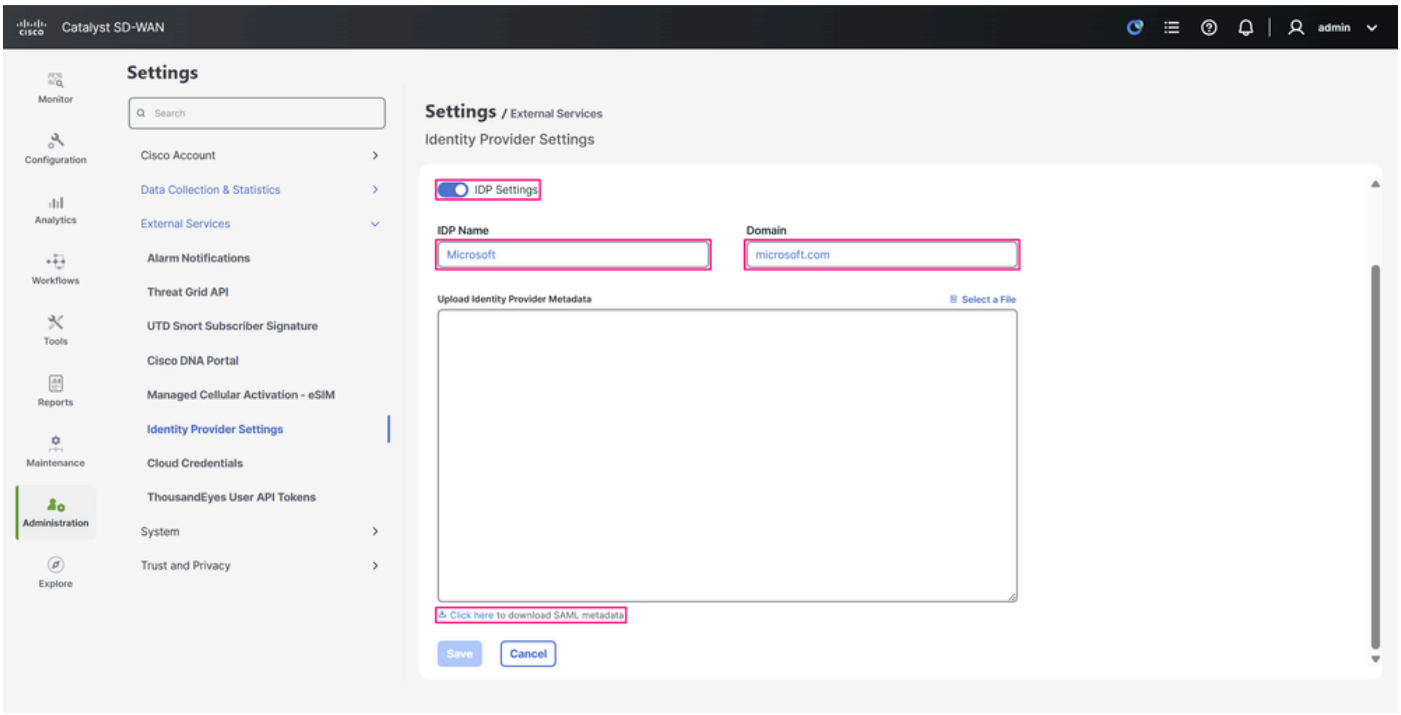
- Schalten Sie die IDP-Einstellungen um, um die Identitätsanbieter-Einstellungen zu aktivieren. Geben Sie im Feld IDP Name einen Namen ein, der auf die von Ihnen verwendete IdP verweist, und geben Sie im Feld Domain eine Domäne ein, die mit den von den Benutzern in der Unternehmensanwendung Ihrer Organisation verwendeten Domänennamen übereinstimmt. Klicken Sie hier, um die SAML-Metadaten herunterzuladen und die XML-Metadatendatei auf Ihrem Computer zu speichern. Diese Datei wird im nächsten Schritt zum Konfigurieren von SSO in der Microsoft Entra-ID verwendet.



Anmerkung: In diesem Beispiel verweist die XML-Datei für Metadaten direkt auf die IP-Adresse des Cisco SD-WAN Managers, in vielen Produktionsumgebungen jedoch auf den vollqualifizierten Domänennamen (FQDN). Bei einem eigenständigen Cisco SD-WAN-Manager stimmt die in den Metadaten enthaltene Element-ID mit der URL überein, die Sie verwenden, um sich beim Cisco SD-WAN-Manager anzumelden, wenn Sie den Manager herunterladen. Dies bedeutet, dass es entweder mit der IP-Adresse oder dem FQDN funktioniert, da es sich um eine Single-Node-Konfiguration handelt.

Für einen Cisco SD-WAN Manager-Cluster gilt derselbe Grundsatz, dass der FQDN auf einen der Cluster-Knoten verweist, und die Metadaten enthalten diese Domäne als Objektkennung. Der Unterschied besteht darin, dass die anderen Knoten nach erfolgreicher SSO-Integration mit der Microsoft Entra-ID, unabhängig davon, ob Sie Metadaten mit dem FQDN des Clusters oder von einem bestimmten Knoten mit seiner IP-Adresse verwenden, ebenfalls zu der IdP-Anmeldeaufforderung umleiten.

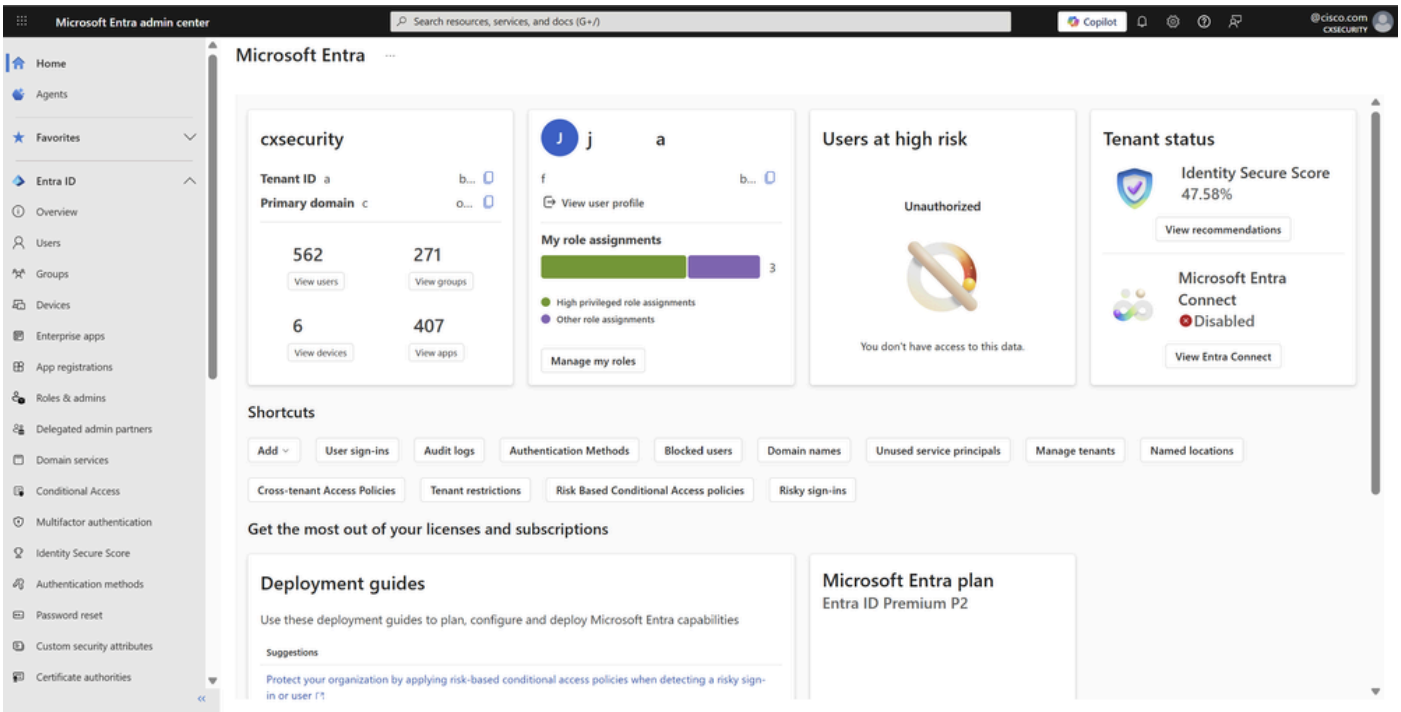
In beiden Szenarien besteht die Hauptanforderung darin, dass die im Cisco SD-WAN Manager verwendete Geräte-ID - ob IP-Adresse oder FQDN - mit der ID übereinstimmt, die auf der IdP-Seite konfiguriert wurde.



Seite "IDp Settings Configuration"

Schritt 2: Konfigurieren einer Enterprise-Anwendung für SSO in Microsoft Entra ID

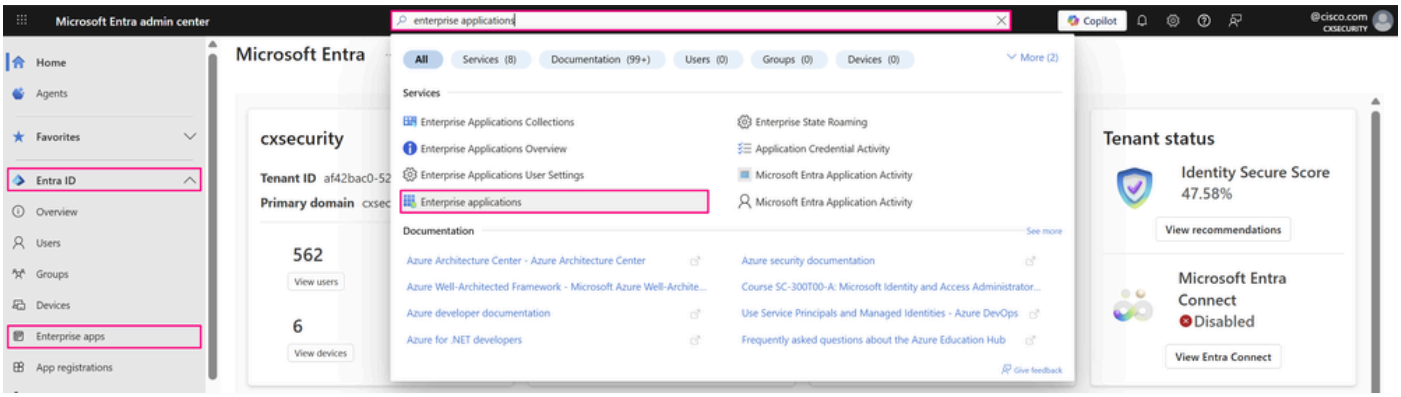
- Melden Sie sich beim Microsoft Entra Admin Center-Portal mit einer der folgenden Rollen an: Administrator der Cloud-Anwendung, Anwendungsadministrator oder Eigentümer des Serviceprinzips.



Microsoft Entra Admin Center-Portal

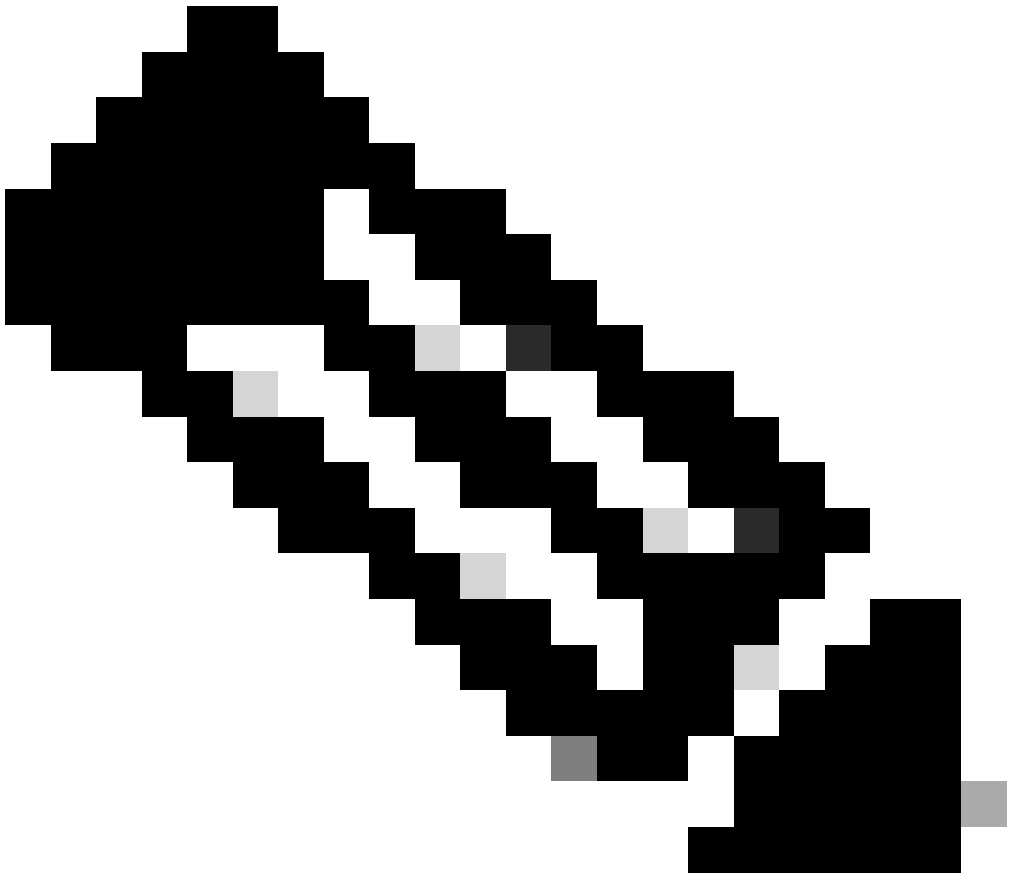
- Navigieren Sie zu Entra ID > Enterprise apps, oder Sie können auf diesen Service auch zugreifen, wenn Sie Enterprise-Anwendungen in der Suchleiste oben im Portal eingeben und

dann Enterprise-Anwendungen auswählen.



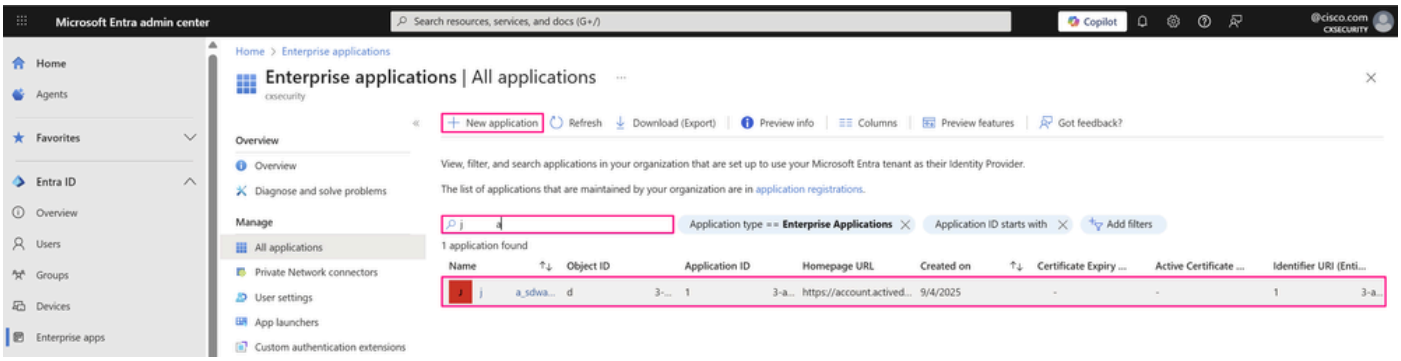
Microsoft Entra Admin Center-Portal

- Die Seite Alle Anwendungen wird geöffnet. Geben Sie den Namen der vorhandenen Anwendung in das Suchfeld ein, und wählen Sie dann die Anwendung aus den Suchergebnissen aus.



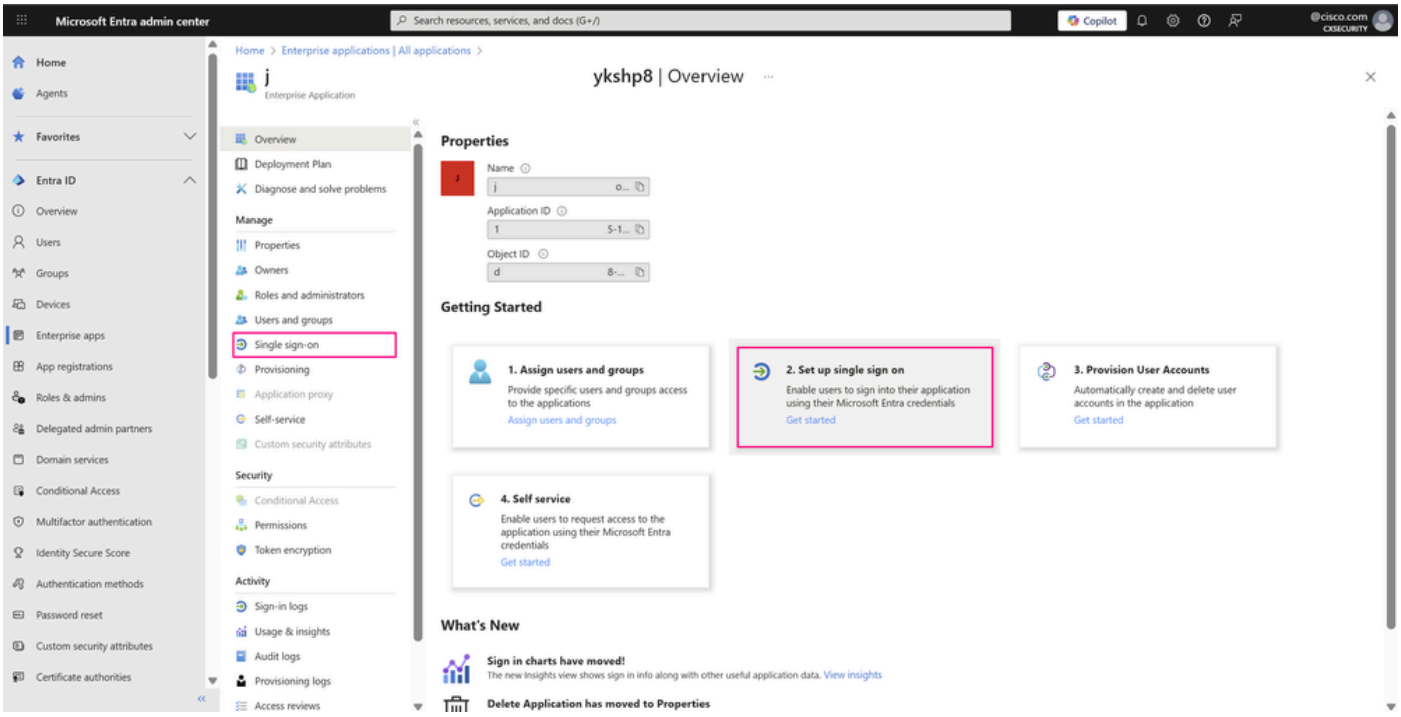
Anmerkung: Auf dieser Seite können Sie eine benutzerdefinierte Enterprise-

Anwendung erstellen, die auf den Anforderungen Ihrer Organisation basiert, und sie mit SSO-Authentifizierung konfigurieren, wenn dies noch nicht der Fall ist, wenn Sie auf Neue Anwendung klicken.



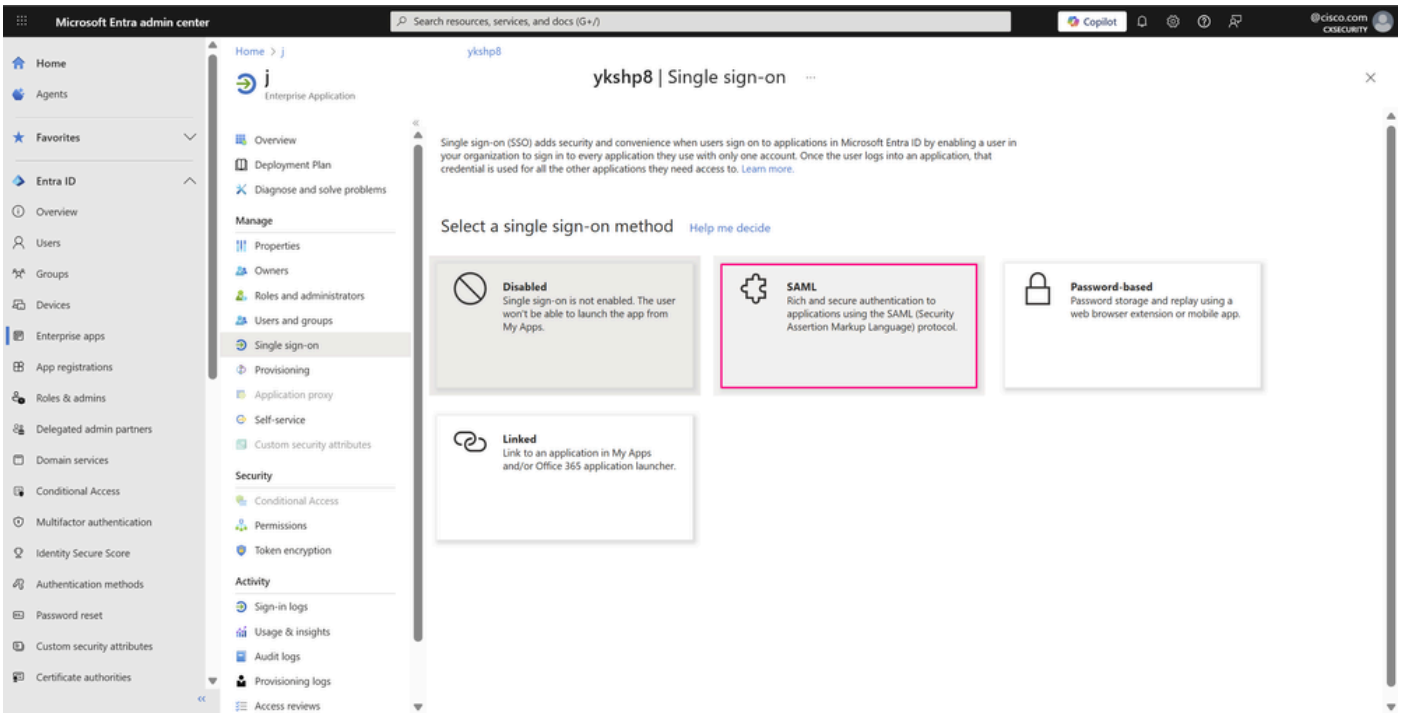
Dashboard für Enterprise-Anwendungen

- Klicken Sie im linken Menü im Abschnitt Verwalten auf Einmalanmeldung, oder klicken Sie im Bereich Erste Schritte des Abschnitts Überblick auf 2. Richten Sie die Einmalanmeldung ein, um den Bereich für die Einmalanmeldung zur Bearbeitung zu öffnen.



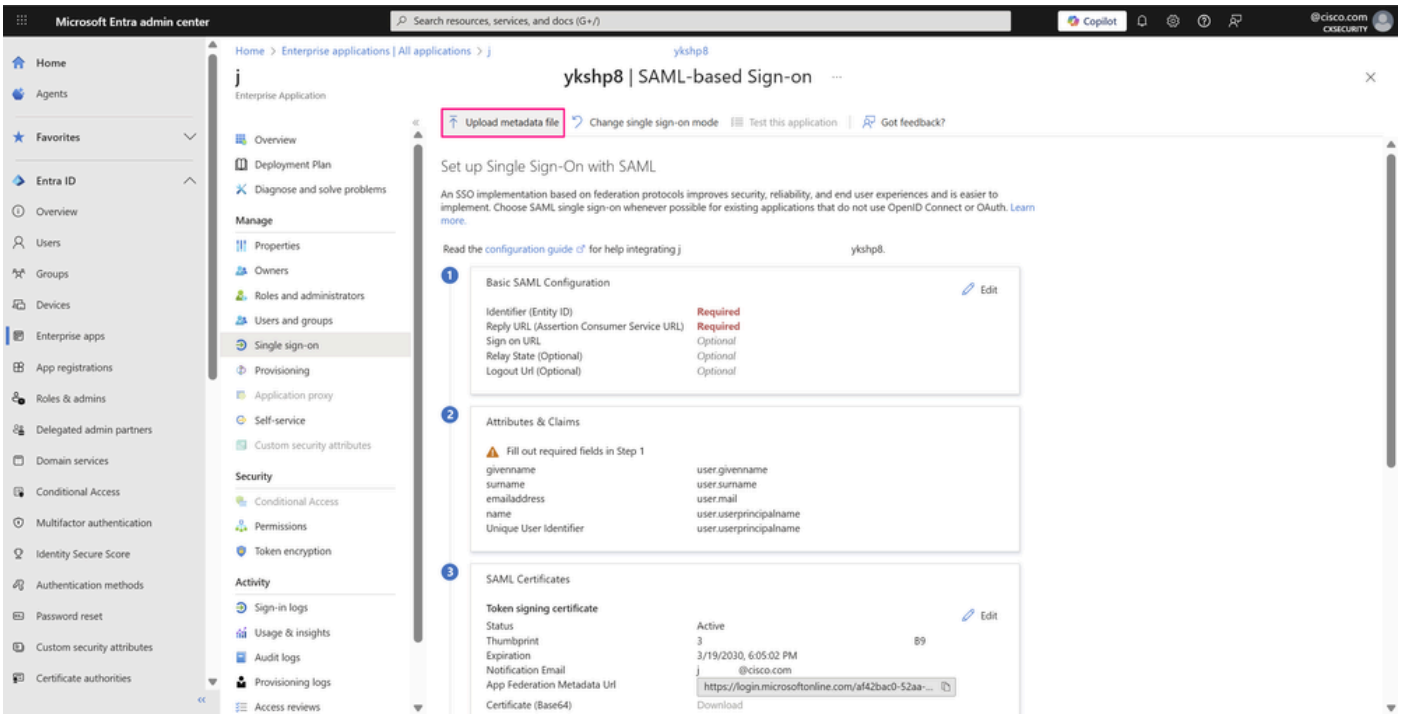
Übersicht über Enterprise-Anwendungen

- Wählen Sie SAML aus, um die SSO-Konfigurationsseite zu öffnen.



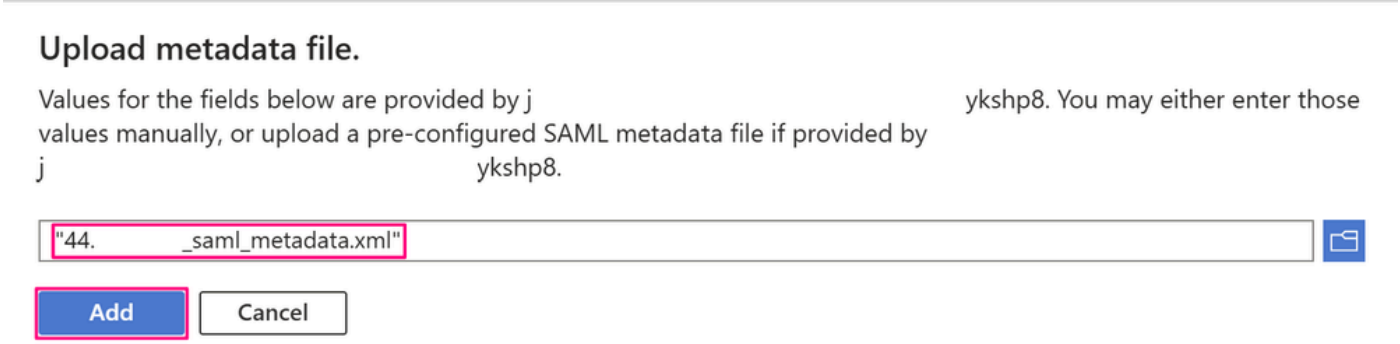
Bereich für einmalige Anmeldung

- Klicken Sie auf der Seite Einmaliges Anmelden mit SAML einrichten auf Metadatendatei hochladen.



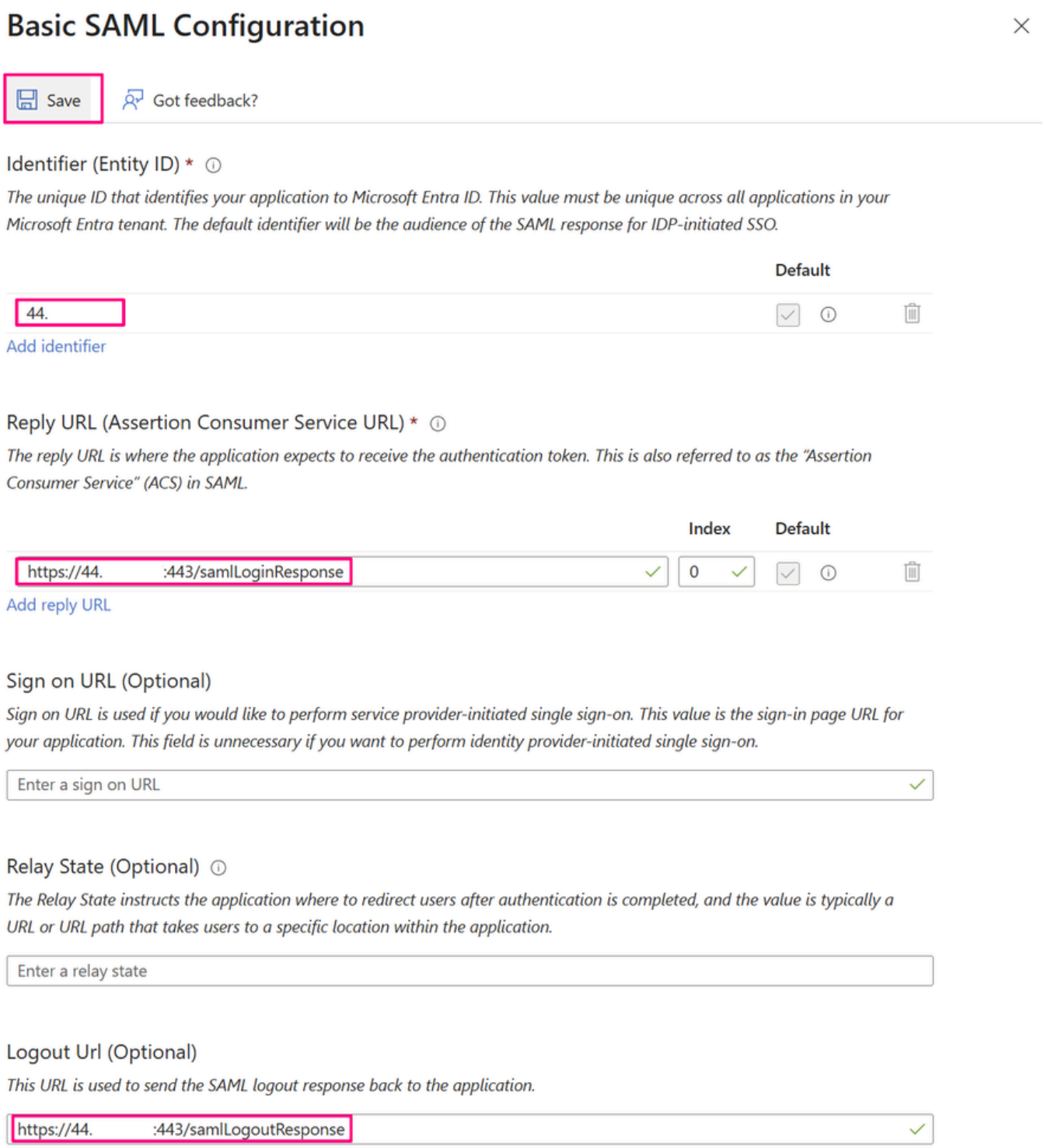
SSO mit SAML-Konfigurationsseite

- Navigieren Sie im Fenster Metadatendatei hochladen zu der zuvor heruntergeladenen XML-Metadatendatei, klicken Sie auf diese, und klicken Sie dann auf Hinzufügen.



Fenster "Metadatendatei hochladen"

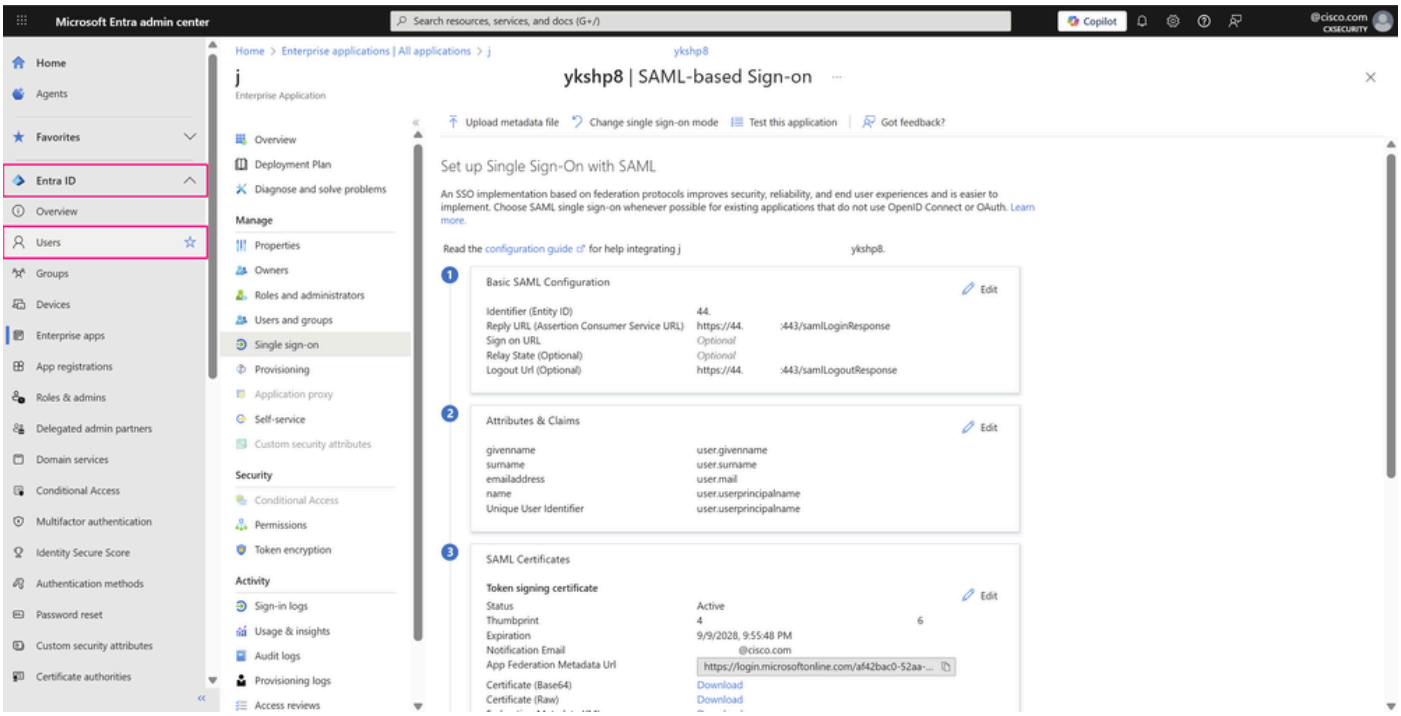
- Im Fenster "SAML-Basiskonfiguration" ist der Identifier (Entity ID) in der Regel die anwendungsspezifische URL - in diesem Fall der Cisco SD-WAN Manager -, mit der Sie die Integration vornehmen (wie im vorherigen Schritt erläutert). Die Werte für Reply URL und Logout URL werden automatisch eingetragen, sobald die Datei erfolgreich hochgeladen wurde. Klicken Sie zum Fortfahren auf Speichern.



Fenster "Basic SAML Configuration"

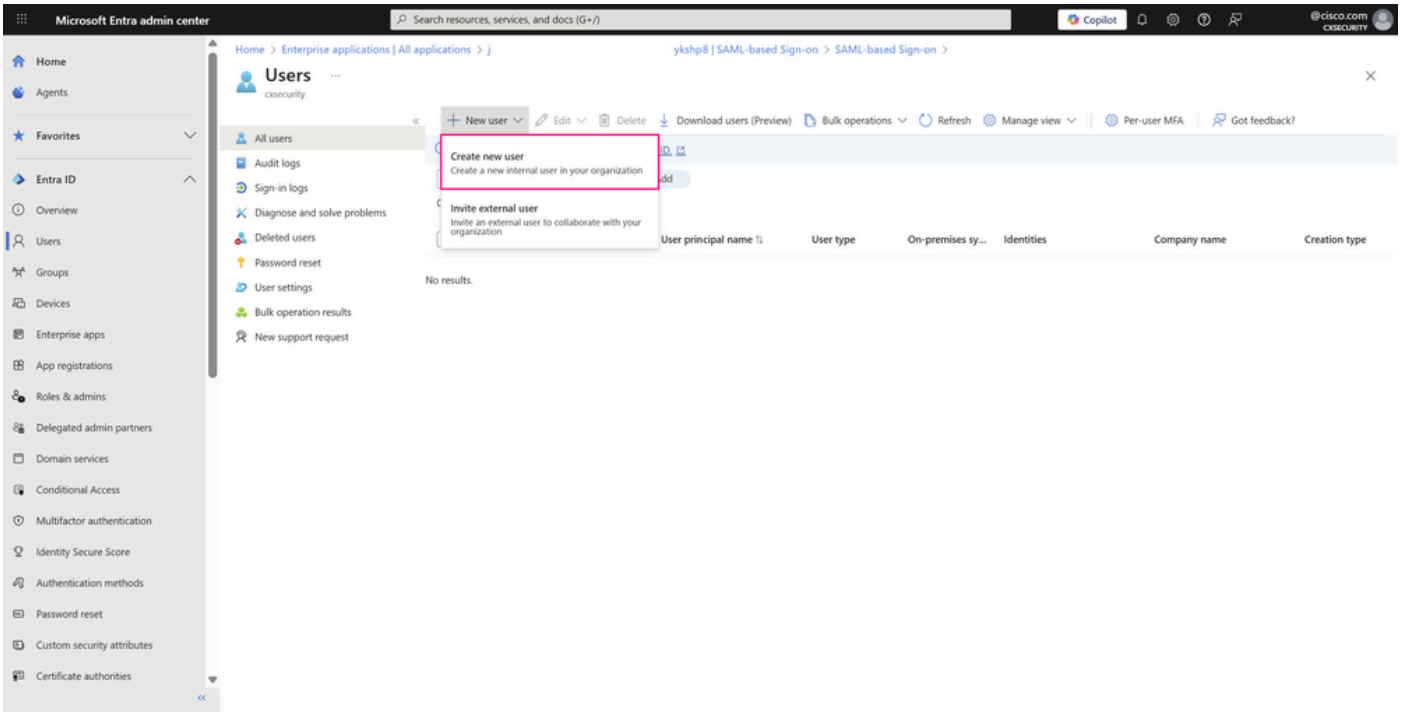
Schritt 3: Hinzufügen eines Benutzer- oder Gruppenkontos zur Enterprise-Anwendung

- Wenn die SAML-Konfigurationsparameter der Anwendung definiert sind, fügen Sie die Benutzer oder Gruppen in der Unternehmensanwendung hinzu, die sich bei der Anwendung anmelden. Navigieren Sie dazu zunächst zu Entra ID > Users, oder Sie können auch auf diesen Dienst zugreifen, wenn Sie den Dienstnamen in der Suchleiste oben im Portal durchsuchen, wie in einem vorherigen Schritt gezeigt.



SSO mit SAML-Konfigurationsseite

- Erstellen Sie einen Benutzer, den Sie einer Gruppe zuordnen, um die SSO-Authentifizierung mit Cisco SD-WAN Manager und einer der Benutzergruppen, netadmin, zu veranschaulichen. Dies ist die häufigste in Produktionsumgebungen. Navigieren Sie dazu zu Entra ID > Users. Klicken Sie dann auf New user und wählen Sie Create new user.

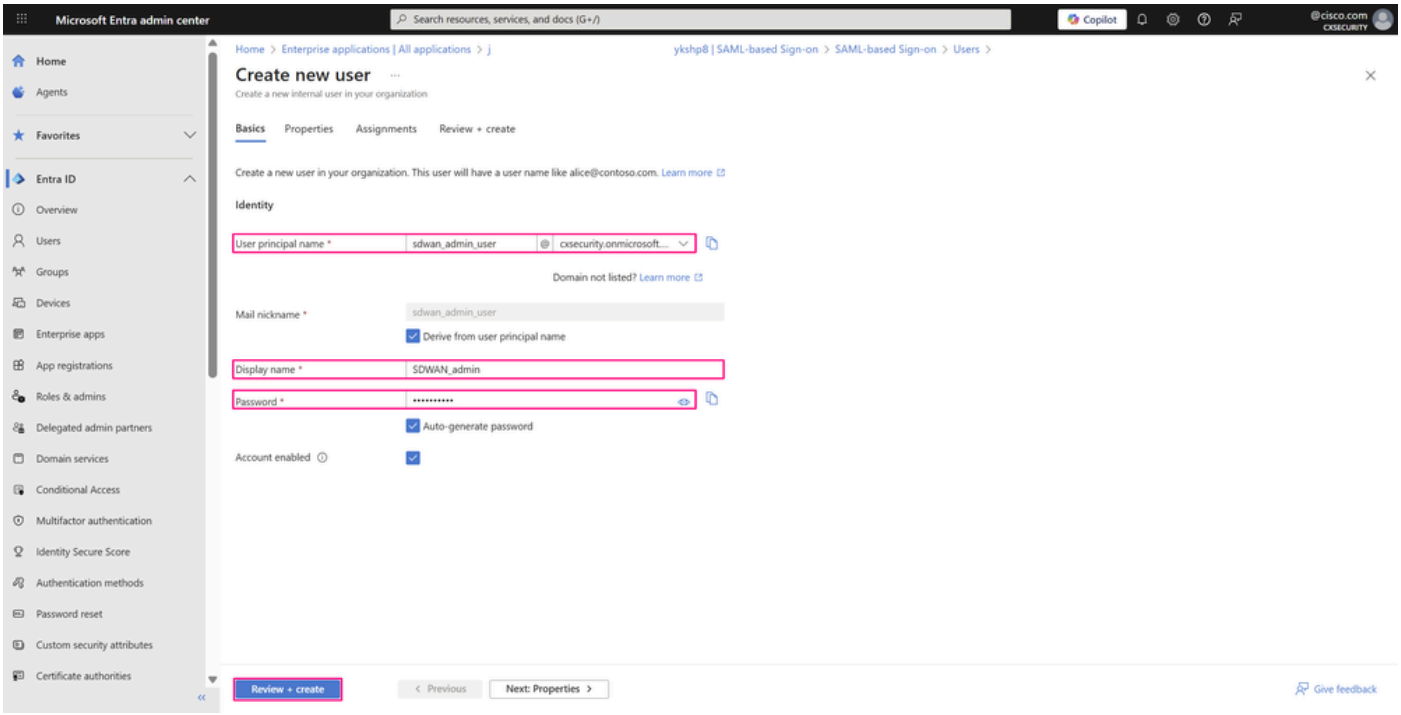


Benutzer-Dashboard

- Die Registerkarte Grundlagen enthält die Kernfelder, die zum Erstellen eines neuen Benutzers erforderlich sind.
    - Geben Sie als Prinzipalnamen des Benutzers einen eindeutigen Benutzernamen ein, und wählen Sie eine Domäne aus der Dropdown-Liste der Domänen aus, die in Ihrer

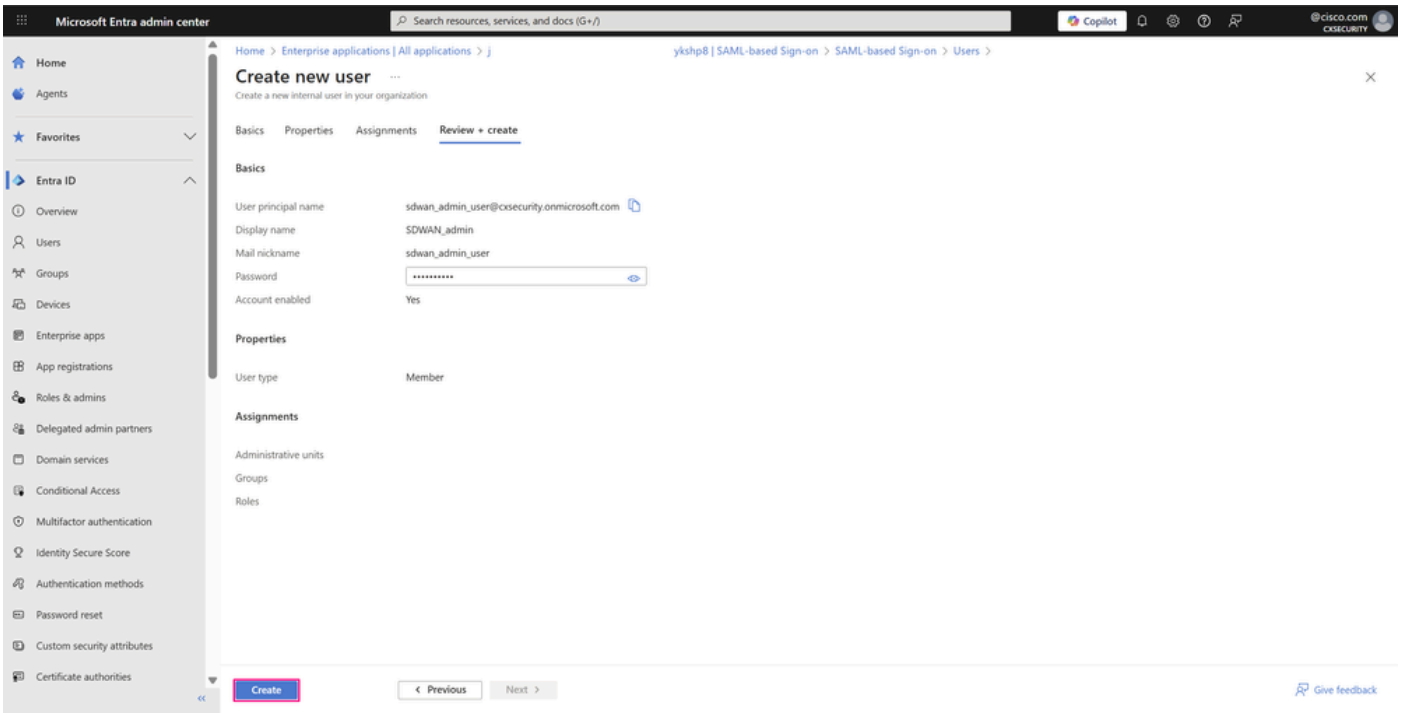
Organisation verfügbar sind.

- Geben Sie einen Anzeigenamen für den Benutzer ein.
- Deaktivieren Sie Kennwort automatisch generieren, wenn Sie ein benutzerdefiniertes Kennwort eingeben möchten, oder lassen Sie diese Option aktiviert, damit ein Kennwort automatisch generiert wird.
- Sie können den Benutzer auf der Registerkarte "Assignments" (Aufgaben) zu einer Gruppe hinzufügen. Da die Gruppenmitgliedschaft jedoch noch nicht erstellt wurde, klicken Sie auf Review + create.



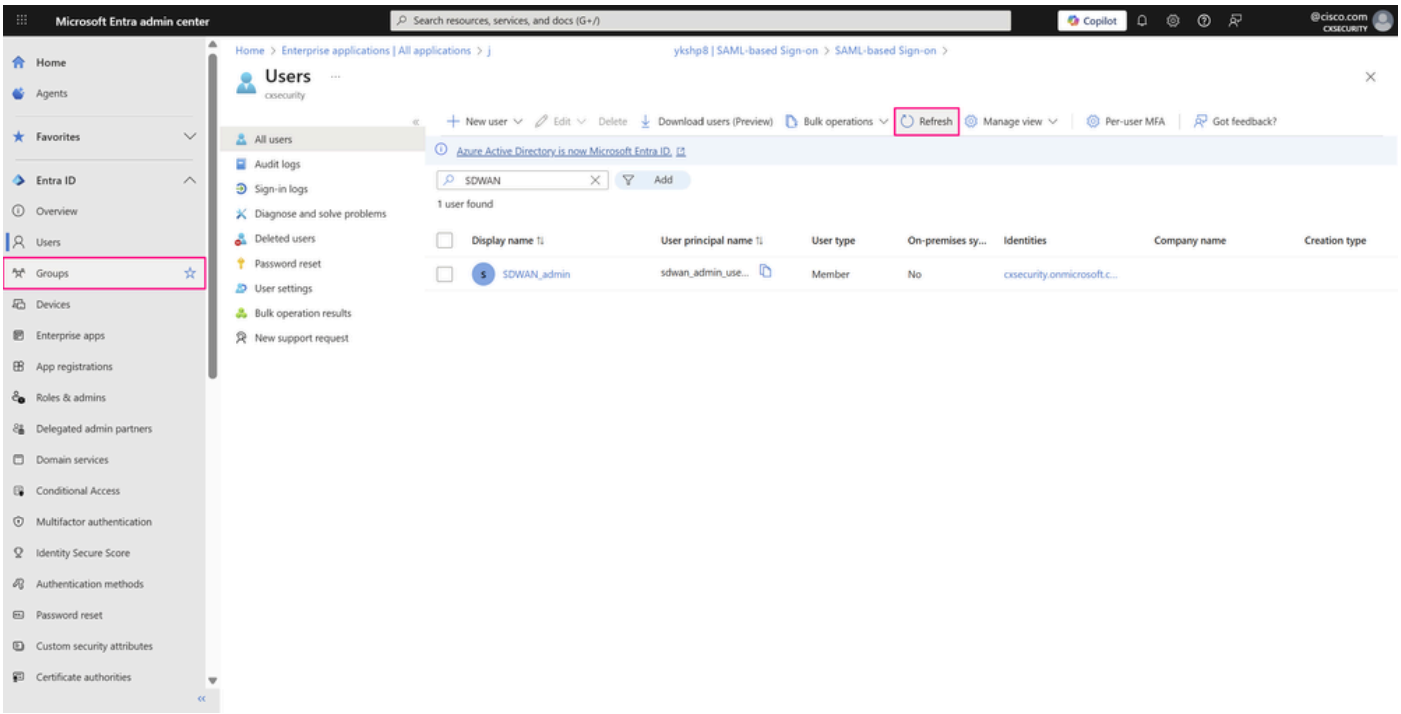
Seite "Benutzererstellung"

- Die letzte Registerkarte enthält die wichtigsten Details aus dem Benutzererstellungs-Workflow. Überprüfen Sie die Details, und klicken Sie auf Erstellen, um den Vorgang abzuschließen.



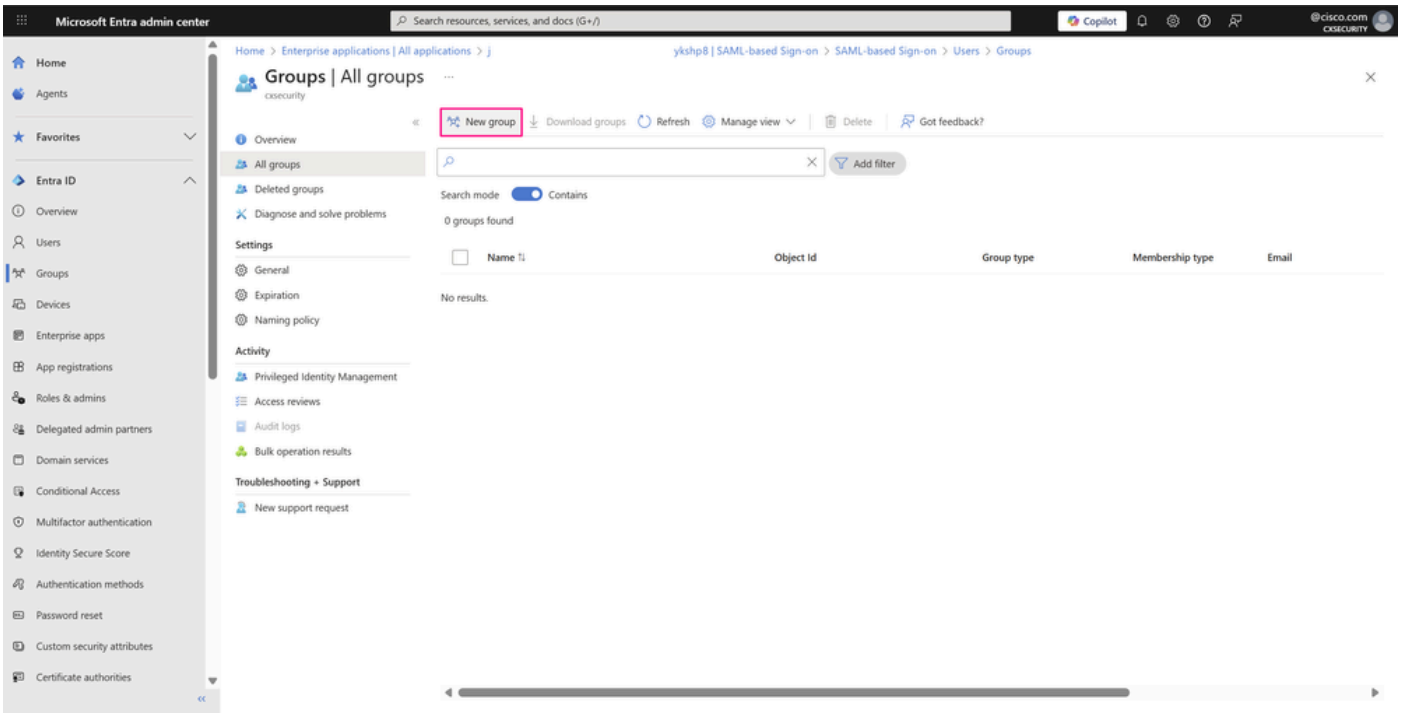
Seite "Benutzererstellung"

- Der neue Benutzer wird kurz darauf angezeigt. Ist dies nicht der Fall, klicken Sie auf Aktualisieren, und suchen Sie in der Suchleiste des Dienstes nach dem Benutzer. Navigieren Sie anschließend zu Entra ID > Groups > All groups, um die neue Gruppe zu erstellen.



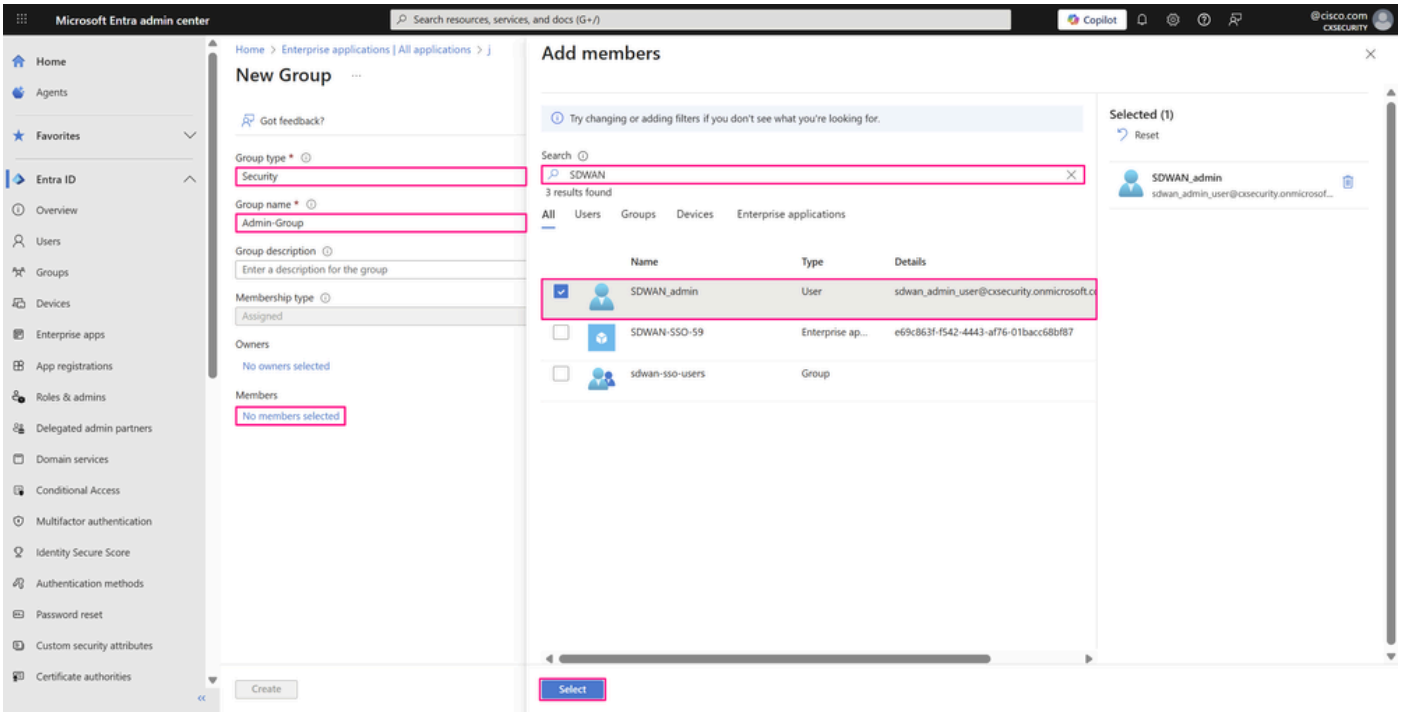
Benutzer-Dashboard

- Auf dieser Seite verwalten Sie die verschiedenen Gruppen und ihre Berechtigungen innerhalb Ihrer Organisation. Klicken Sie auf Neue Gruppe, um die Gruppe mit Netzwerkadministratorrechten zu erstellen.



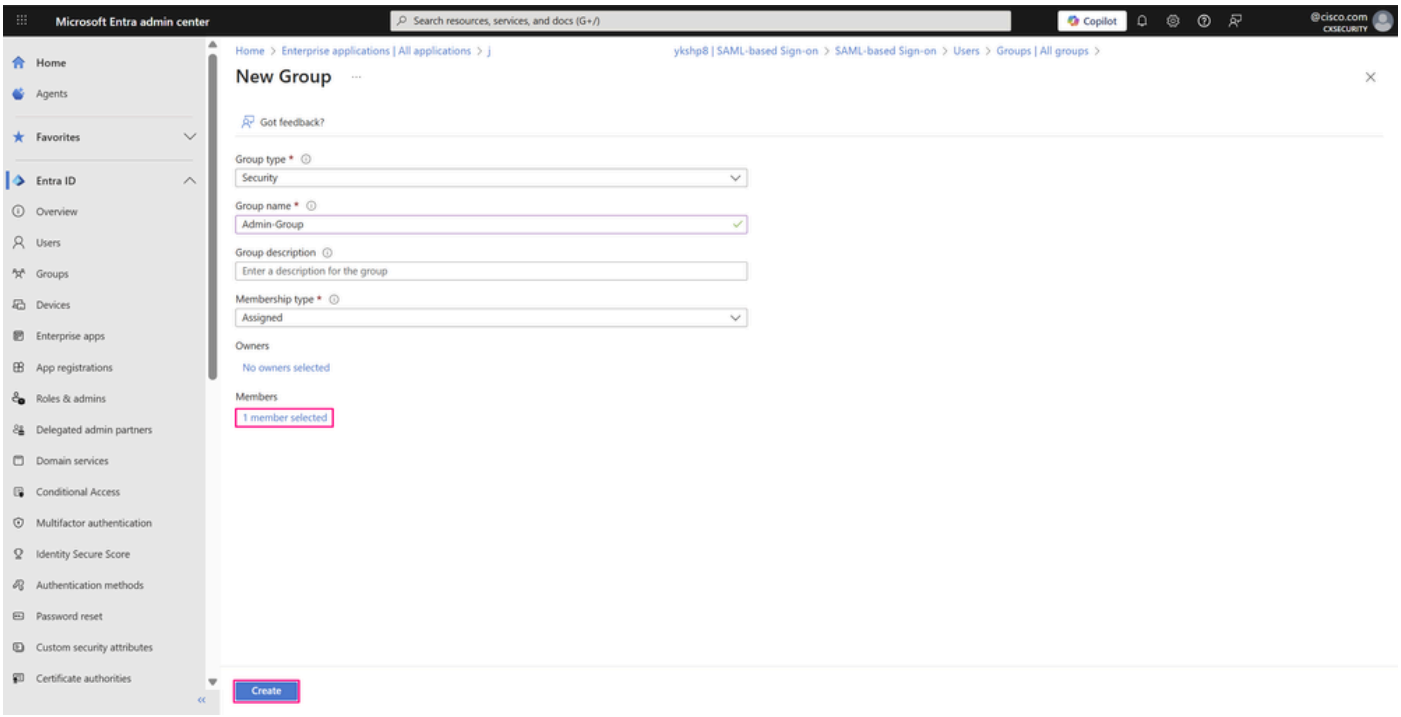
Seite Alle Gruppen

- Wählen Sie einen Gruppentyp aus der Dropdown-Liste aus - in diesem Fall Sicherheit, da nur Zugriff auf freigegebene Ressourcen erforderlich ist. Geben Sie einen Gruppennamen Ihrer Wahl ein, der auf die Rolle oder Berechtigungen der Gruppe verweist. Ordnen Sie an dieser Stelle der Gruppe Benutzer zu, wenn Sie im Feld Mitglieder auf die ausgewählten Mitglieder klicken.
    - Durchsuchen Sie im Fenster Mitglieder hinzufügen die Benutzer, die Sie hinzufügen möchten (in unserem Beispiel der gerade erstellte Benutzer), und wählen Sie sie aus, und klicken Sie dann auf Auswählen.



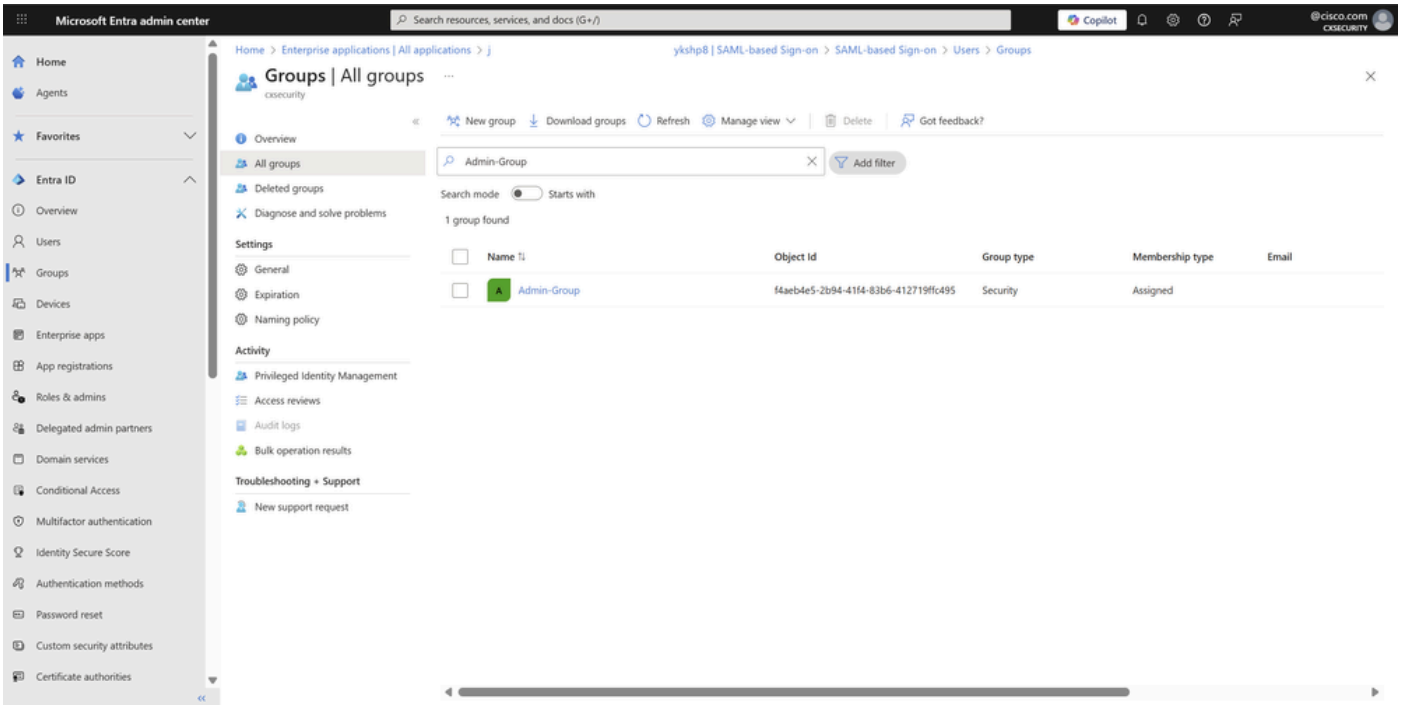
Seite Gruppenerstellung

- Klicken Sie auf Erstellen, um die Gruppe zu erstellen.



Seite Gruppenerstellung

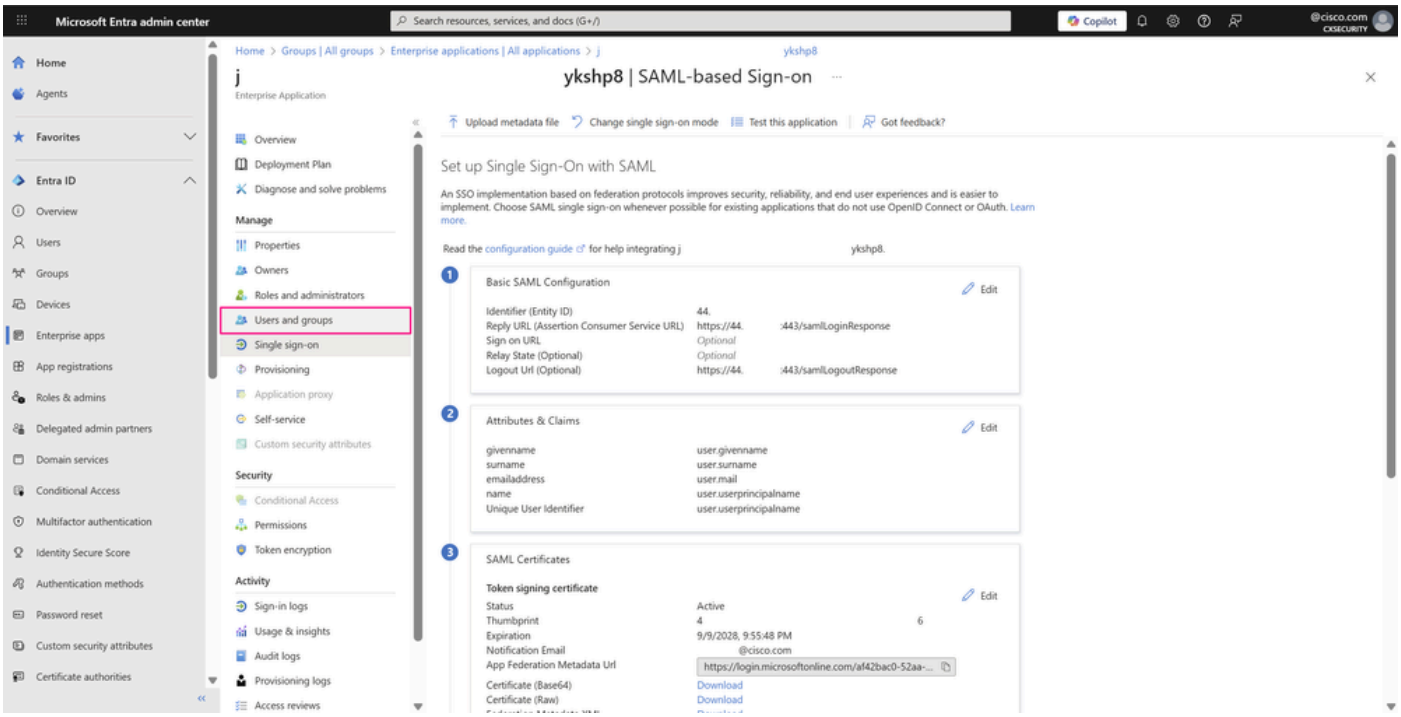
- Die neue Gruppe erscheint kurz darauf. Wenn dies nicht der Fall ist, klicken Sie auf Aktualisieren, und suchen Sie nach dem Gruppennamen mit der Suchleiste im Dienst. Wiederholen Sie die vorherigen Schritte, um einen weiteren Benutzer zu erstellen und ihn einer anderen Gruppenmitgliedschaft hinzuzufügen, um die SSO-Anmeldung mit der Anwendung und einer der anderen Benutzergruppen, z. B. Operator, zu validieren.



Seite Alle Gruppen

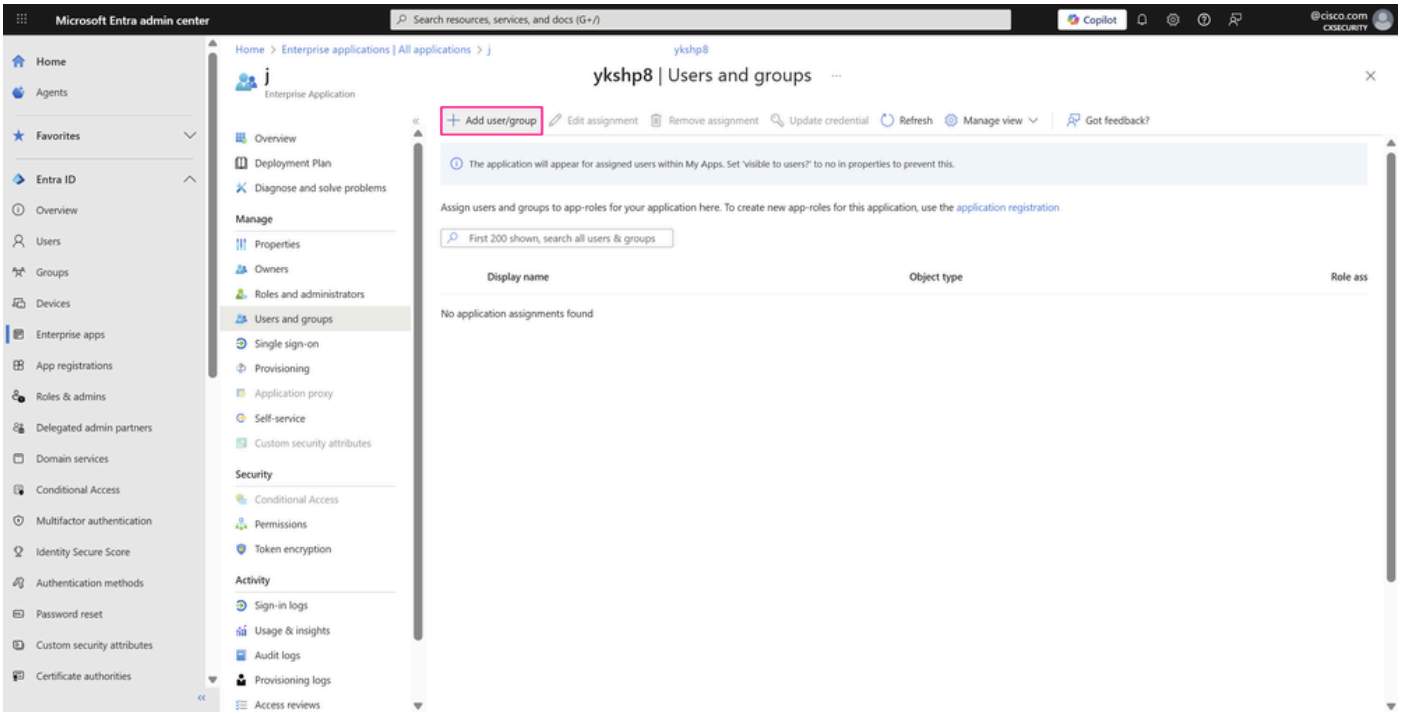
Schritt 4: Konfiguration der SAML-Gruppenbereitstellung für Microsoft Entra ID

- Um die Gruppen oder Benutzer bereitzustellen, die ihnen in der SAML-Konfiguration zugeordnet sind, müssen Sie sie Ihrer Unternehmensanwendung zuweisen, damit sie über Anmeldeberechtigungen für Ihre Anwendung verfügen, z. B. für den Cisco SD-WAN Manager. Navigieren Sie zurück zu Entra ID > Enterprise apps und öffnen Sie Ihre Enterprise-Anwendung. Klicken Sie im linken Menü im Abschnitt Verwalten auf Benutzer und Gruppen.



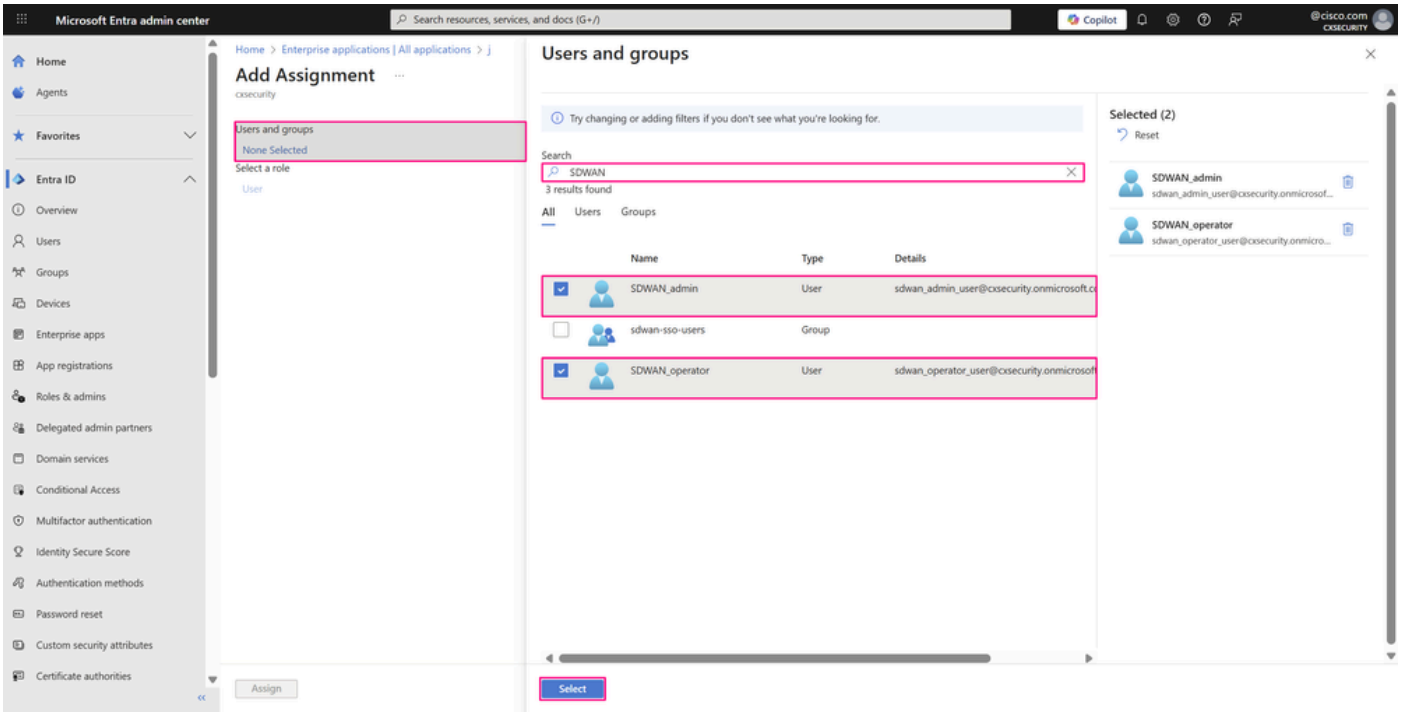
SSO mit SAML-Konfigurationsseite

- Klicken Sie anschließend auf Benutzer/Gruppe hinzufügen.



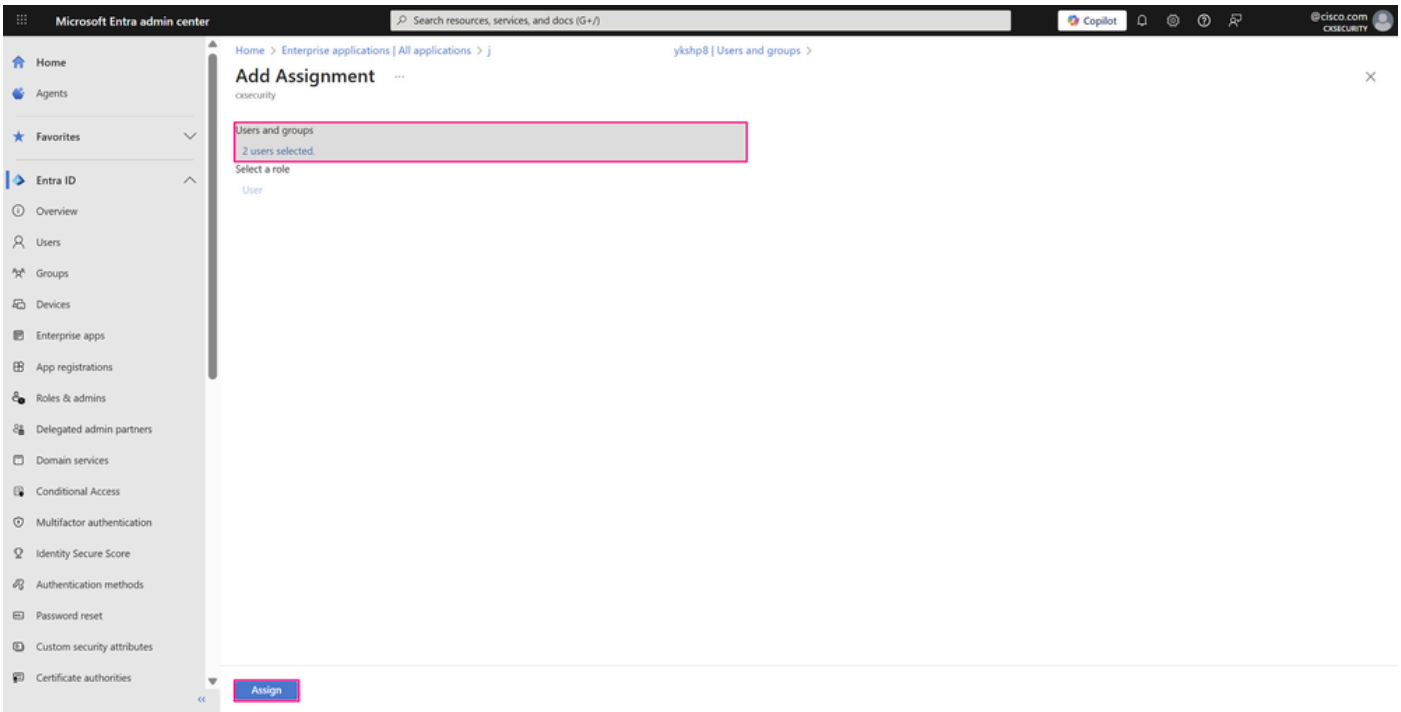
Seite Benutzer und Gruppen

- Klicken Sie im Bereich Zuweisung hinzufügen unter Benutzer und Gruppen auf Keine ausgewählt. Suchen Sie nach dem Benutzer oder der Gruppe, den Sie der Anwendung zuweisen möchten (in unserem Beispiel die beiden Benutzer, die in den vorherigen Schritten erstellt wurden), und klicken Sie dann auf Auswählen.



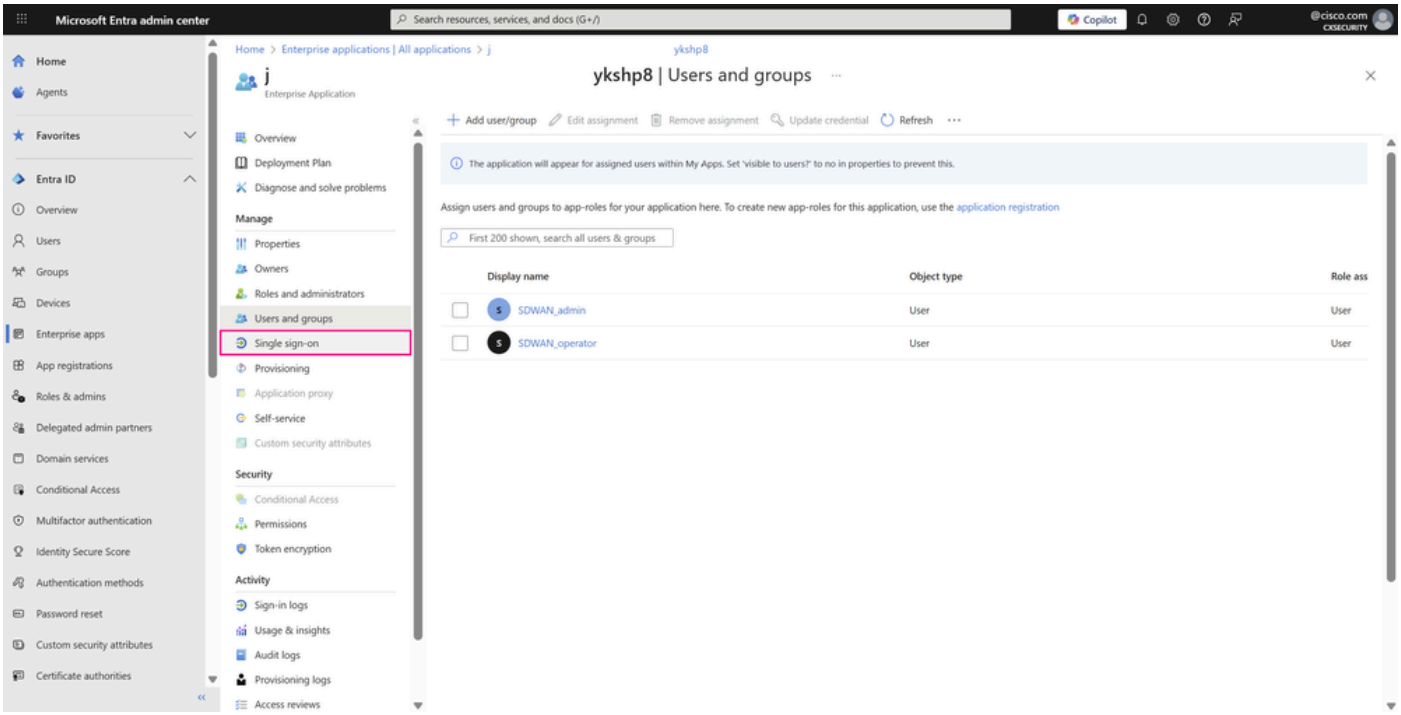
Bereich "Benutzer-/Gruppenzuweisung"

- Klicken Sie auf Zuweisen, um den Benutzer oder die Gruppe der Anwendung zuzuweisen.



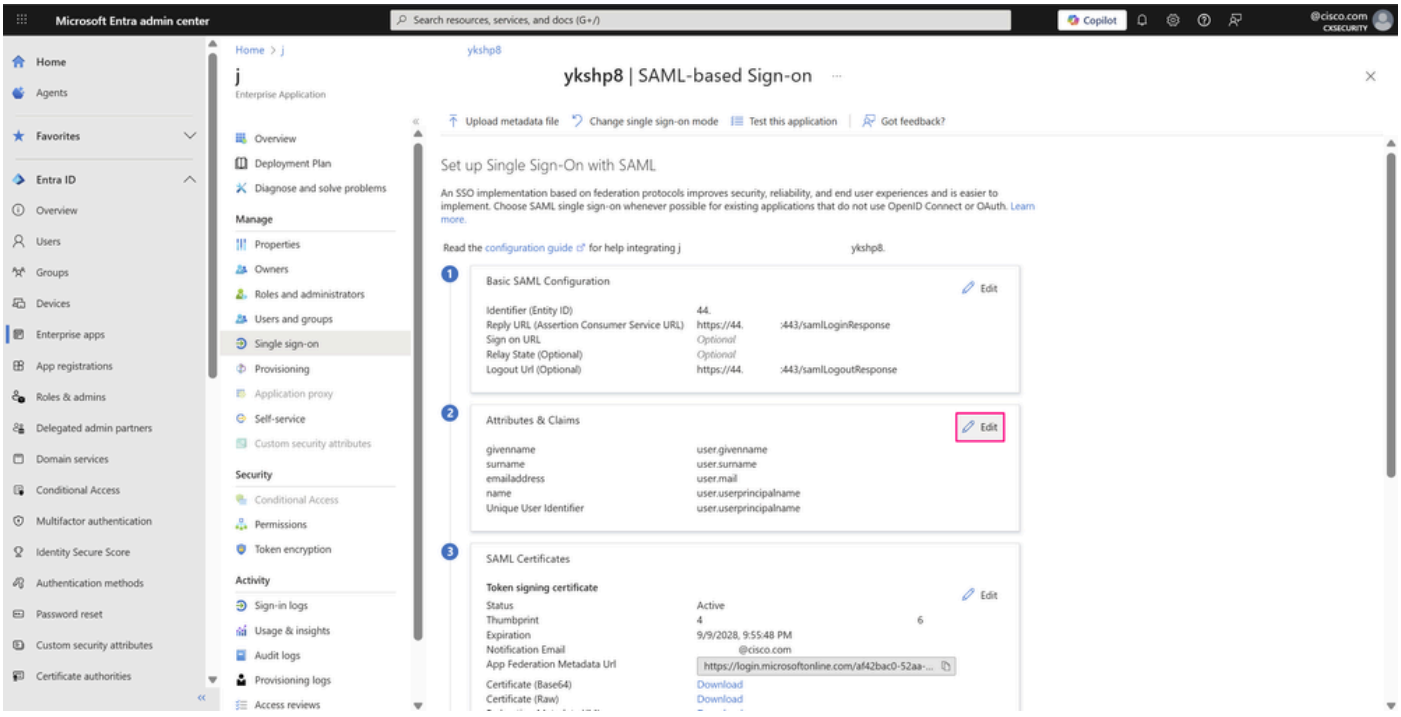
Bereich "Benutzer-/Gruppenzuweisung"

- Die Ihrer Unternehmensanwendung zugewiesenen Benutzer werden kurz nach der Zuweisung aufgeführt. Klicken Sie im linken Menü im Abschnitt Verwalten auf Single Sign-on, um auf die SSO SAML-Konfiguration der Anwendung zuzugreifen und die verbleibende erforderliche Konfiguration abzuschließen.



Seite Benutzer und Gruppen

- Klicken Sie auf der Seite Einmalige Anmeldung mit SAML einrichten unter Attribute & Ansprüche auf Bearbeiten.



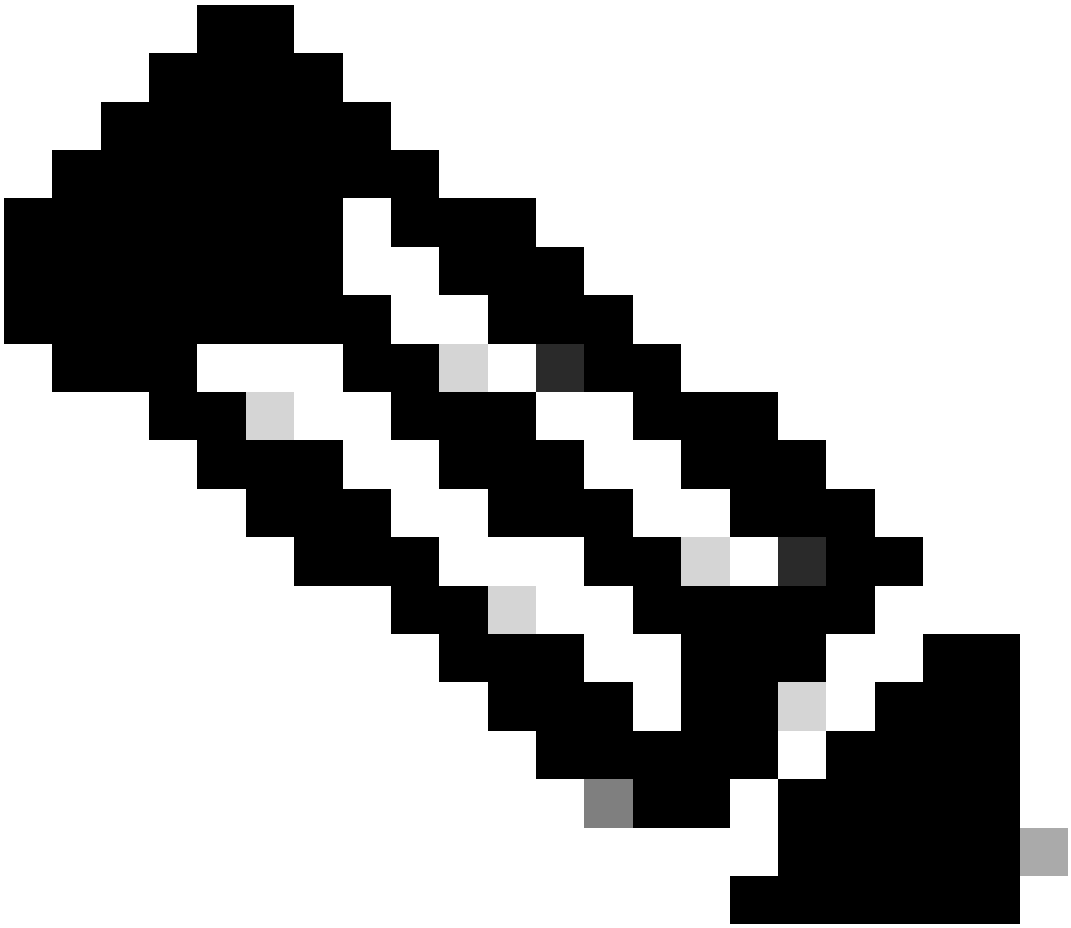
SSO mit SAML-Konfigurationsseite

- Klicken Sie auf der Seite Attribute & Ansprüche auf das Drei-Punkte-Symbol und dann auf

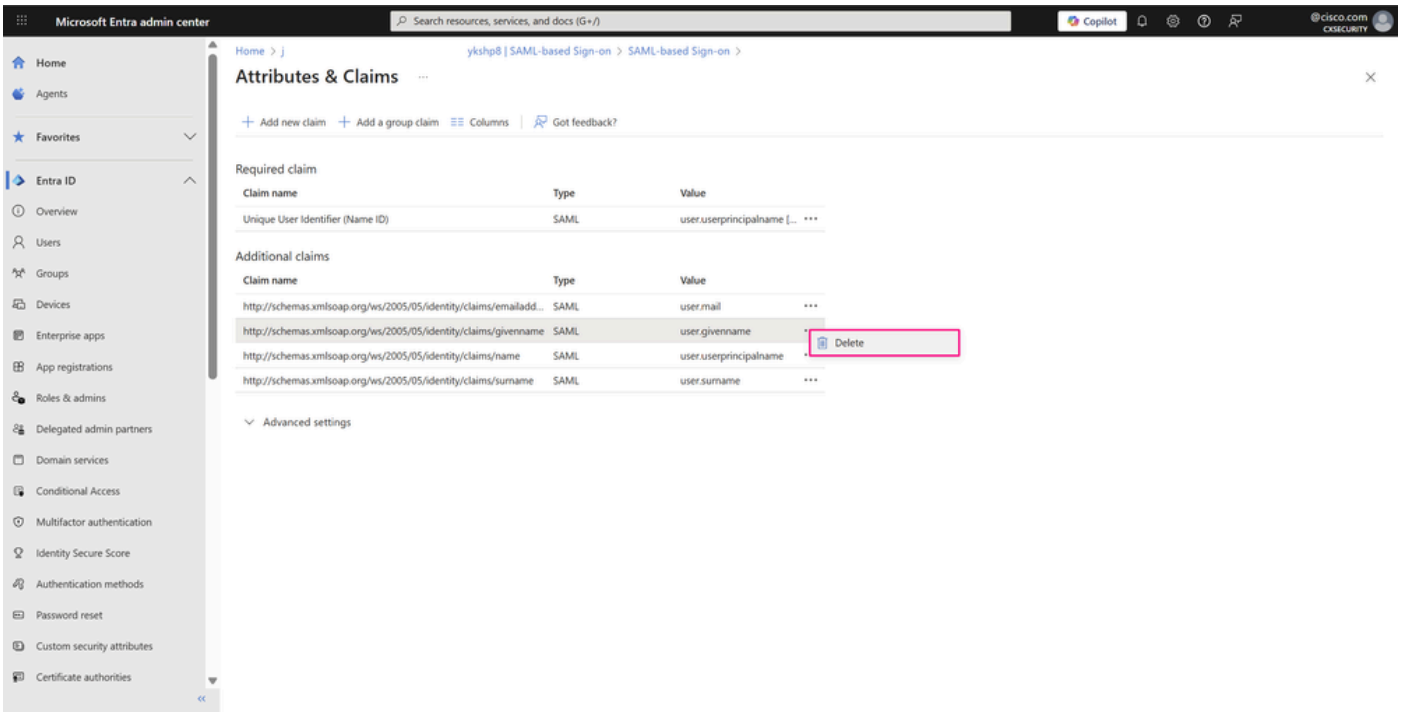
Löschen, um den Anspruch mit dem Wert user.givenname und den Anspruch mit dem Wert user.surname zu entfernen, da sie für dieses Beispiel nicht benötigt werden.Nur die nächsten Ansprüche sind für die grundlegende SSO-Authentifizierung mit der Anwendung erforderlich:

- E-Mail-Adresse des Benutzers -user.mail
- User Principal Name (UPN) des Benutzers -user.userprincipalname

---

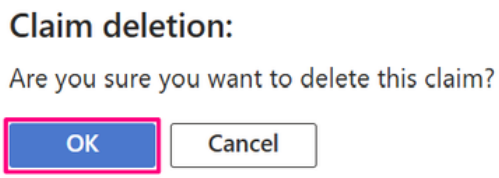


Anmerkung: Je nach den spezifischen Anforderungen Ihres Unternehmens können zusätzliche Anträge gestellt werden.



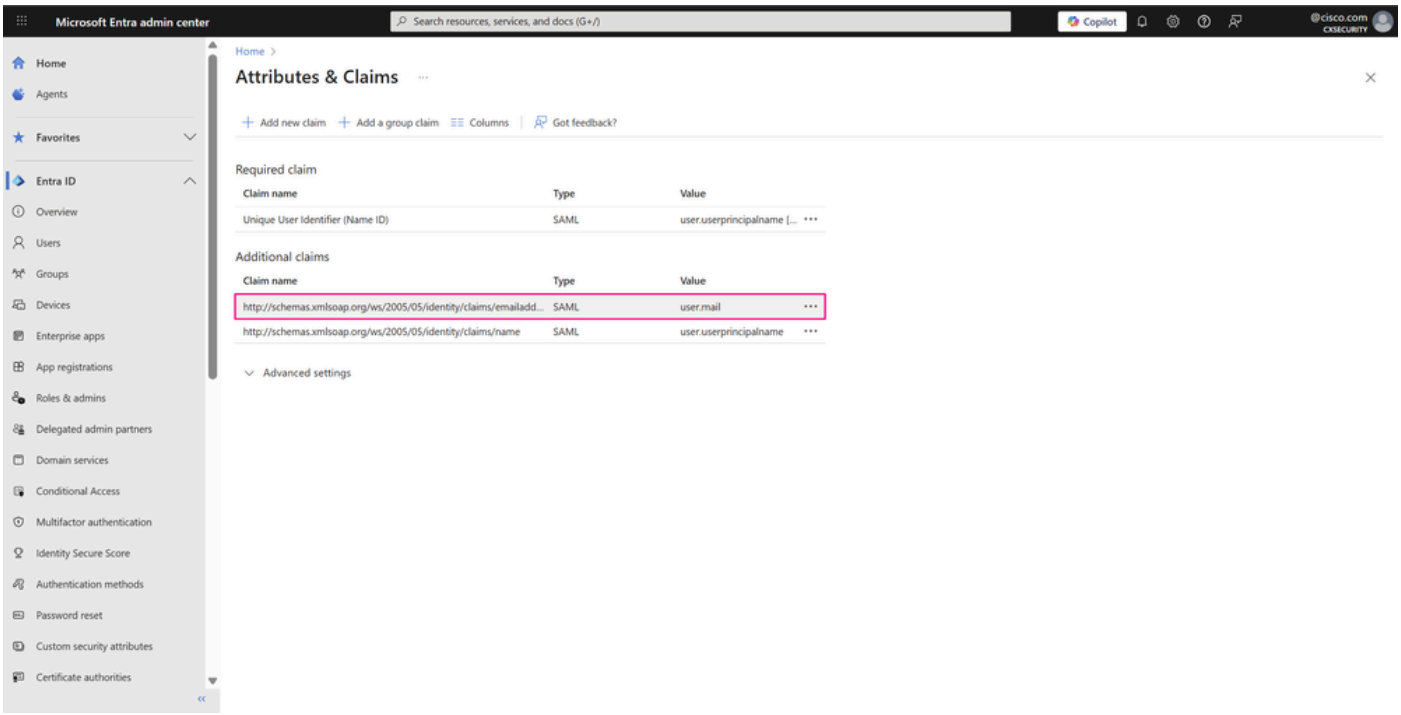
Seite "Attribute und Forderungen"

- Klicken Sie im Fenster zum Löschen von Ansprüchen auf OK, um den Anspruch zu löschen.



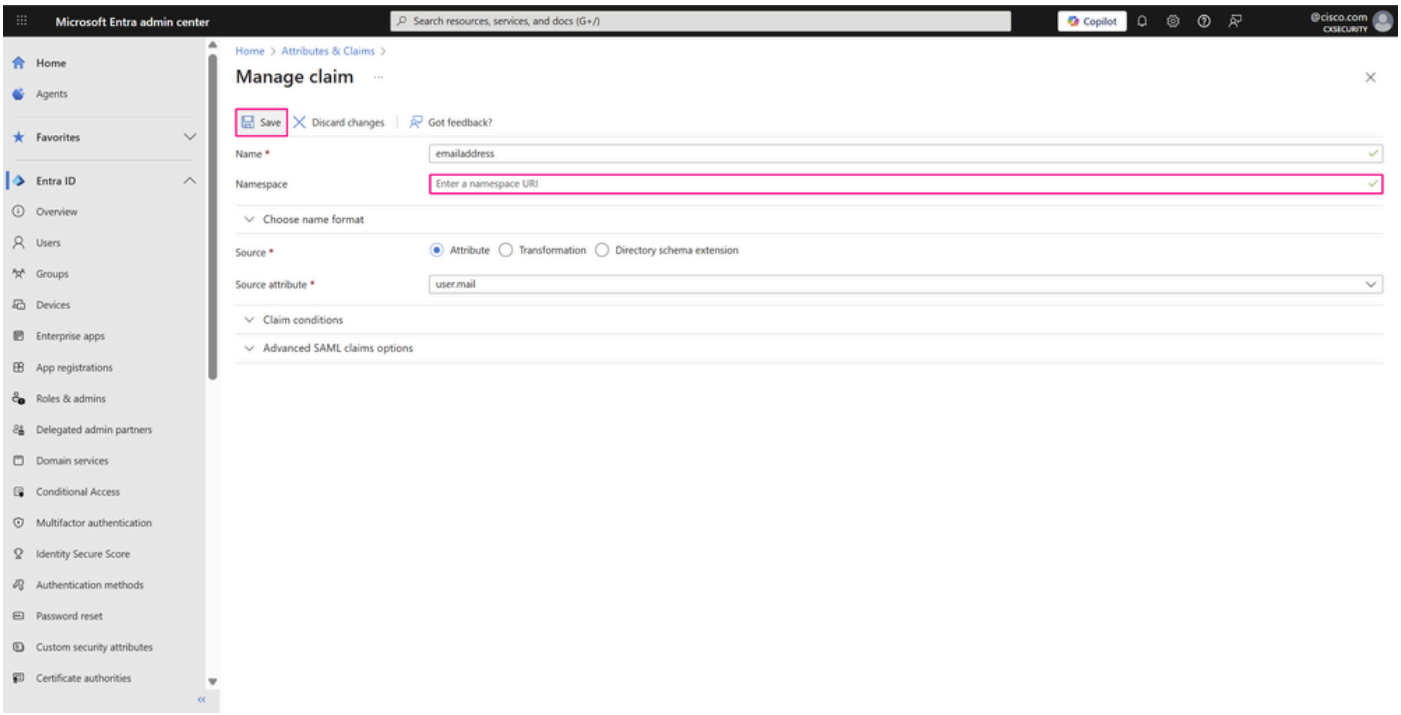
Fenster zum Löschen von Forderungen

- Entfernen Sie anschließend den Namespace aus dem Anspruchsnamen in den beiden verbleibenden Ansprüchen, da dieses Feld optional ist. Diese Änderung ermöglicht die Anzeige des tatsächlichen Namens der einzelnen Komponenten auf dieser Seite, um die Identifizierung zu erleichtern. Bewegen Sie den Mauszeiger über die einzelnen Ansprüche, und klicken Sie darauf, um auf die zugehörigen Einstellungen zuzugreifen.



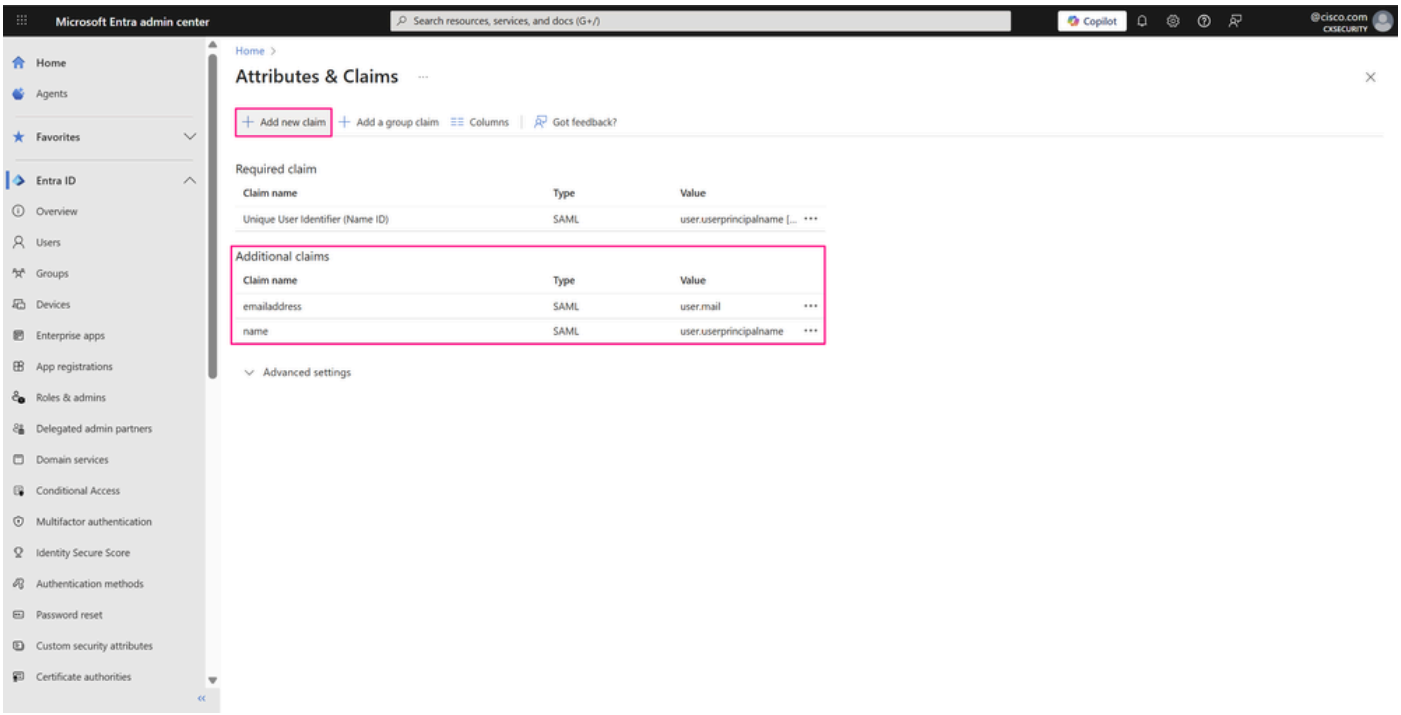
Seite "Attribute und Forderungen"

- Löschen Sie auf der Seite Ansprüche verwalten das Feld Namespace, und klicken Sie auf Speichern, um die Änderungen anzuwenden.



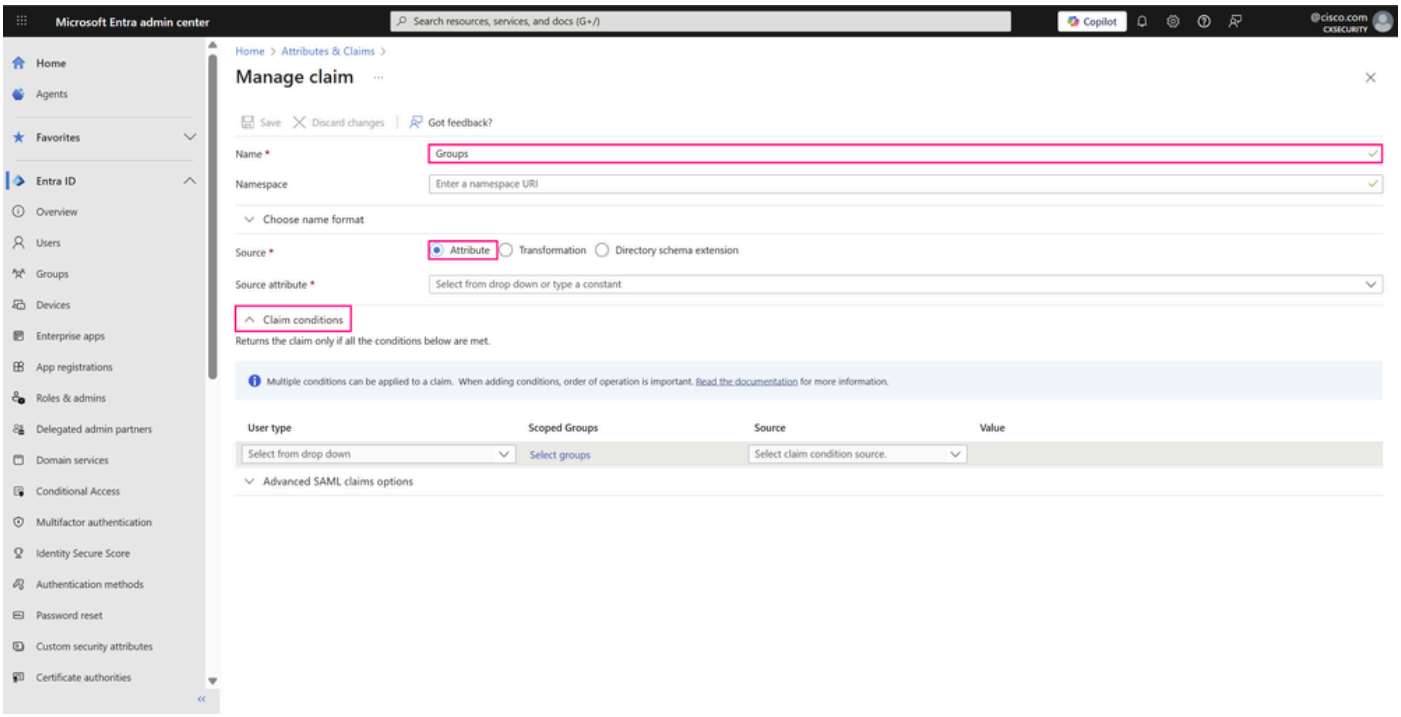
Seite "Forderungen verwalten"

- Die Namen der beiden erforderlichen Ansprüche sind nun sichtbar. Ein weiterer Anspruch ist jedoch erforderlich, um die Gruppen zu definieren, denen die Benutzer angehören und die zum Zugriff auf Anwendungsressourcen autorisiert sind. Klicken Sie dazu auf Neuen Anspruch hinzufügen.



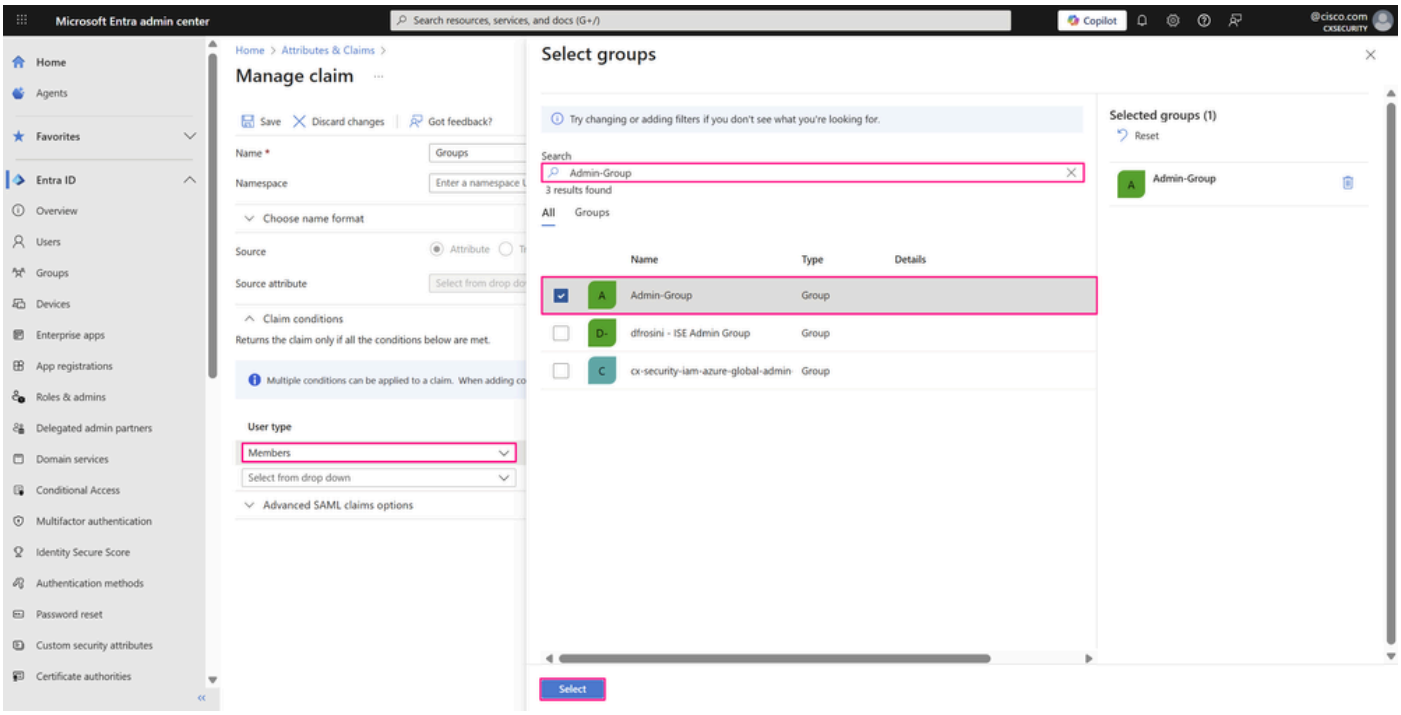
Seite "Attribute und Forderungen"

- Geben Sie einen Namen ein, um diesen Anspruch zu identifizieren. Wählen Sie neben Quelle die Option Attribut aus. Klicken Sie dann auf Anspruchsbedingungen, um die Optionen zu erweitern und mehrere Bedingungen zu konfigurieren.



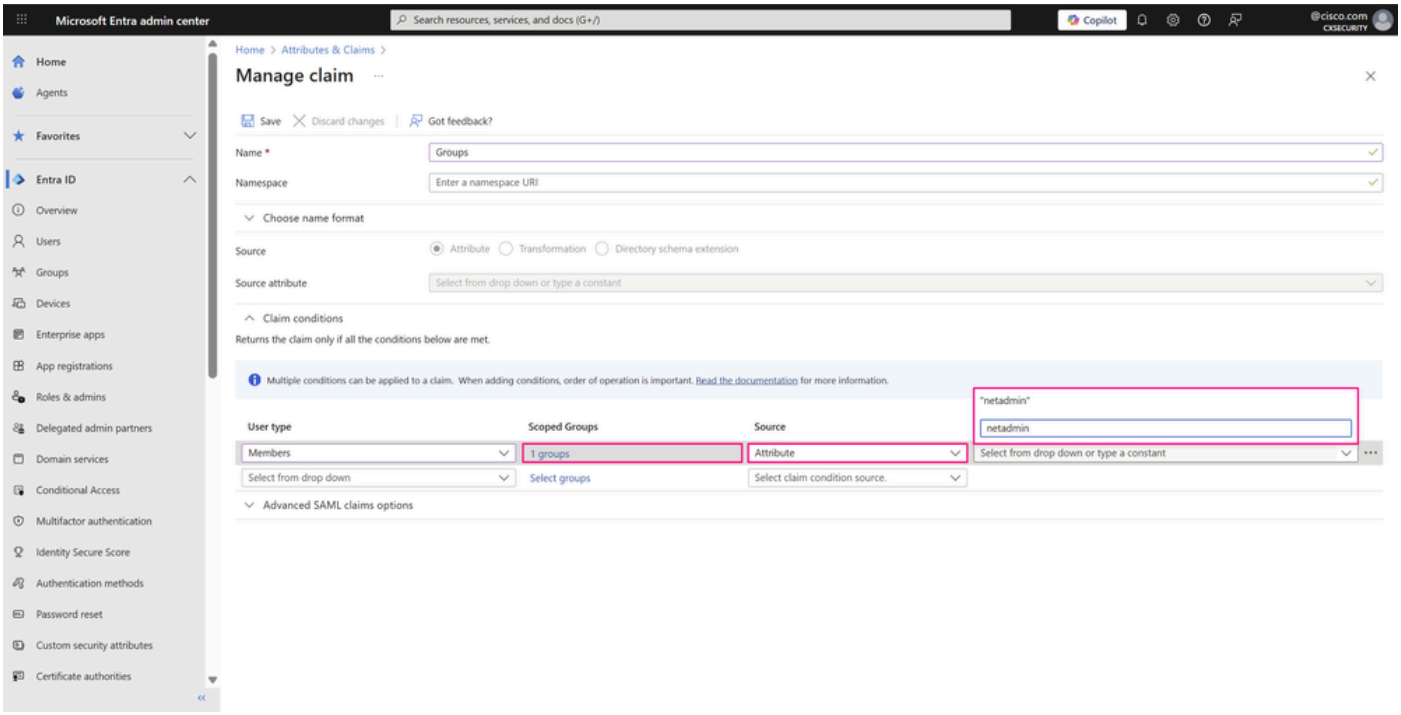
Seite "Forderungen verwalten"

- Wählen Sie in der Anspruchsbedingung Mitglieder aus der Dropdown-Liste Benutzertyp aus, und klicken Sie auf Gruppen auswählen, um die Gruppe(n) auszuwählen, der der Benutzer angehören muss, und klicken Sie dann auf Auswählen.



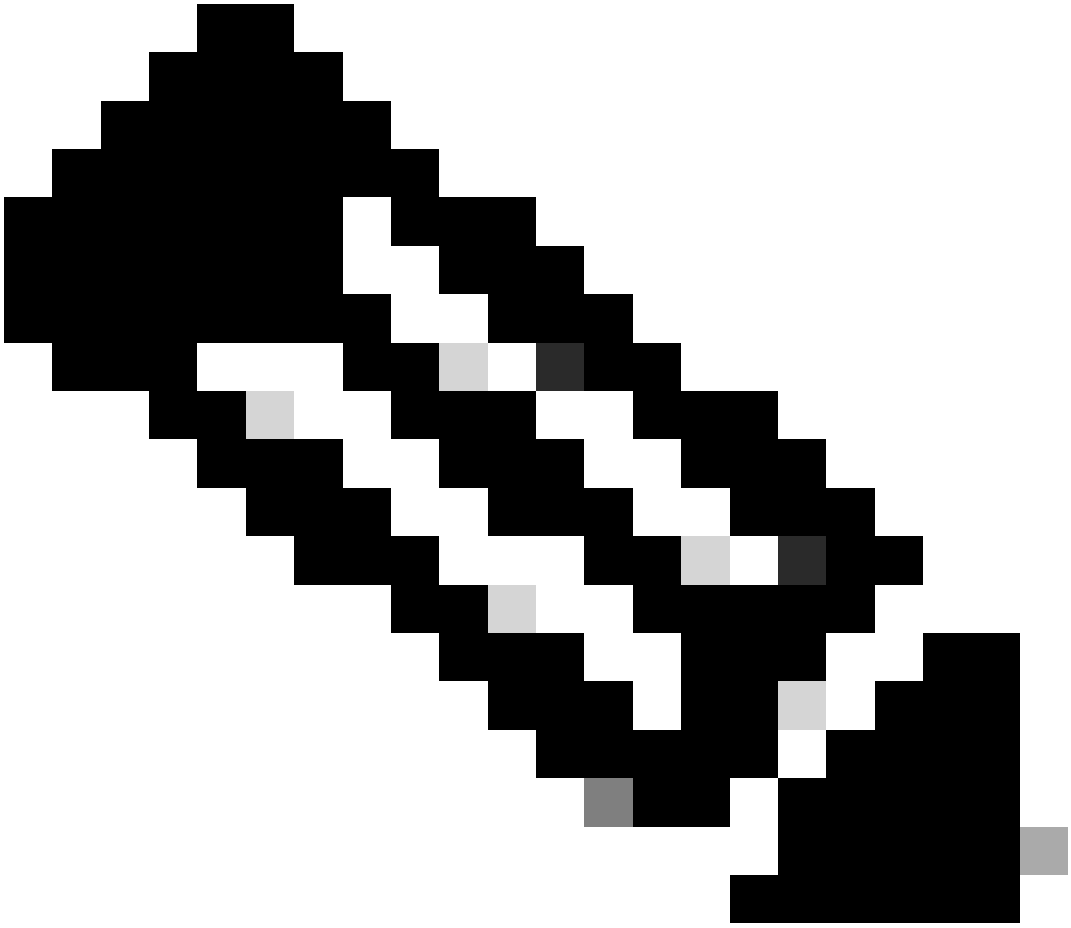
Seite "Forderungen verwalten"

- Wählen Sie Attribute aus der Dropdown-Liste Quelle aus, in der der Anspruch seinen Wert abruft. Geben Sie im Feld Wert das benutzerdefinierte Attribut des Benutzers ein, der auf die in der Anwendung definierte Benutzergruppe verweist. In diesem Beispiel ist netadmin eine der Standard-Benutzergruppen im Cisco SD-WAN Manager. Geben Sie den Attributwert ohne Anführungszeichen ein, und drücken Sie die Eingabetaste.

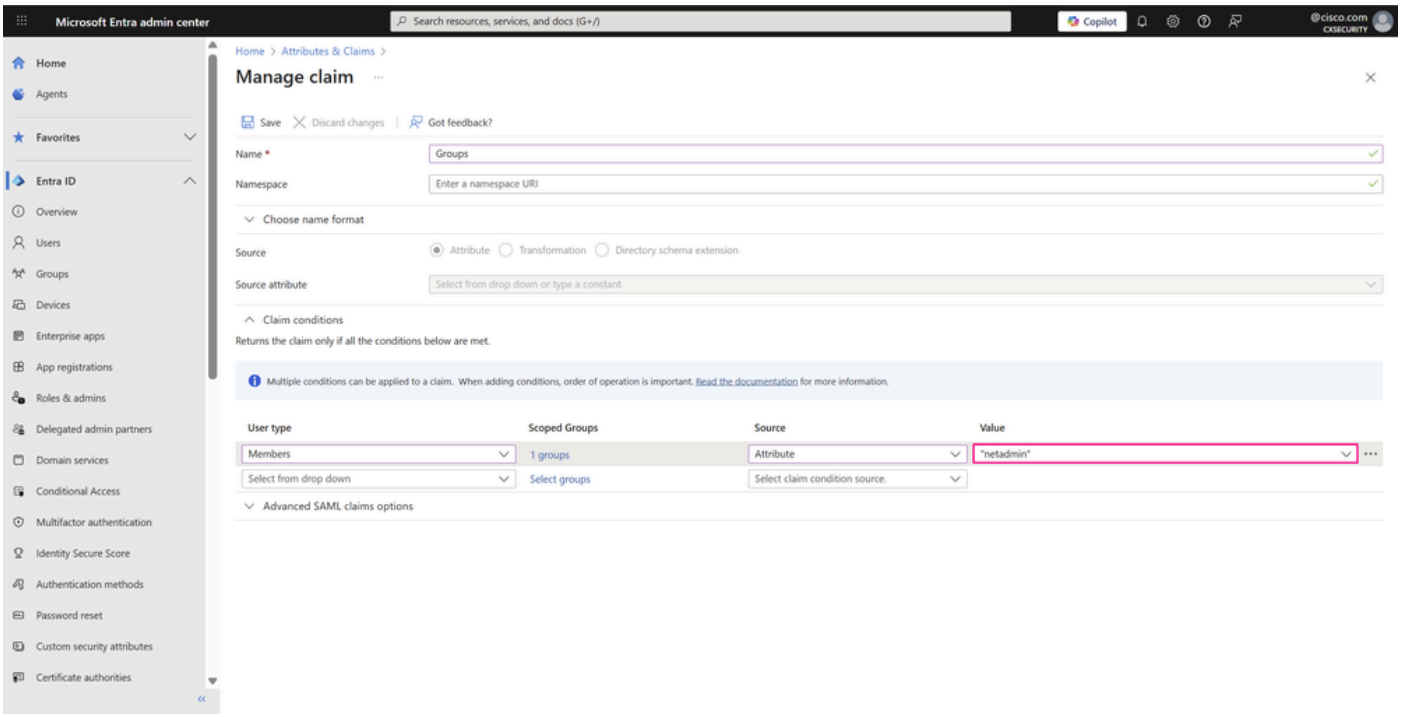


Seite "Forderungen verwalten"

- Unmittelbar danach wird der Attributwert mit Anführungszeichen angezeigt, da dieser Wert von Microsoft Entra ID als Zeichenfolge behandelt wird.

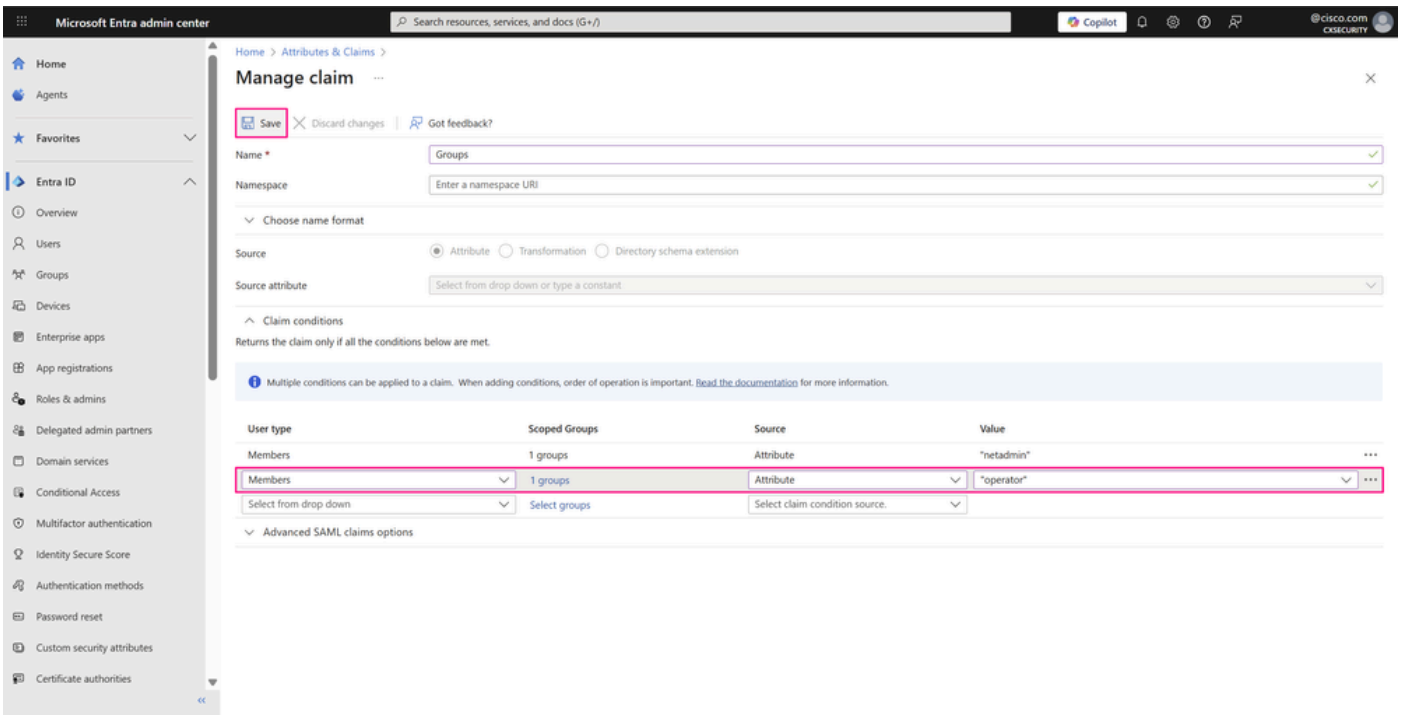


Anmerkung: Diese Parameter innerhalb der Anspruchsbedingungen sind in der SSO SAML-Konfiguration der Unternehmensanwendung sehr relevant, da diese benutzerdefinierten Attribute immer mit den im Cisco SD-WAN Manager definierten Benutzergruppen übereinstimmen müssen. Diese Übereinstimmung bestimmt die Berechtigungen oder Berechtigungen, die Benutzern basierend auf der Gruppe gewährt werden, zu der sie in Microsoft Entra ID gehören.



Seite "Forderungen verwalten"

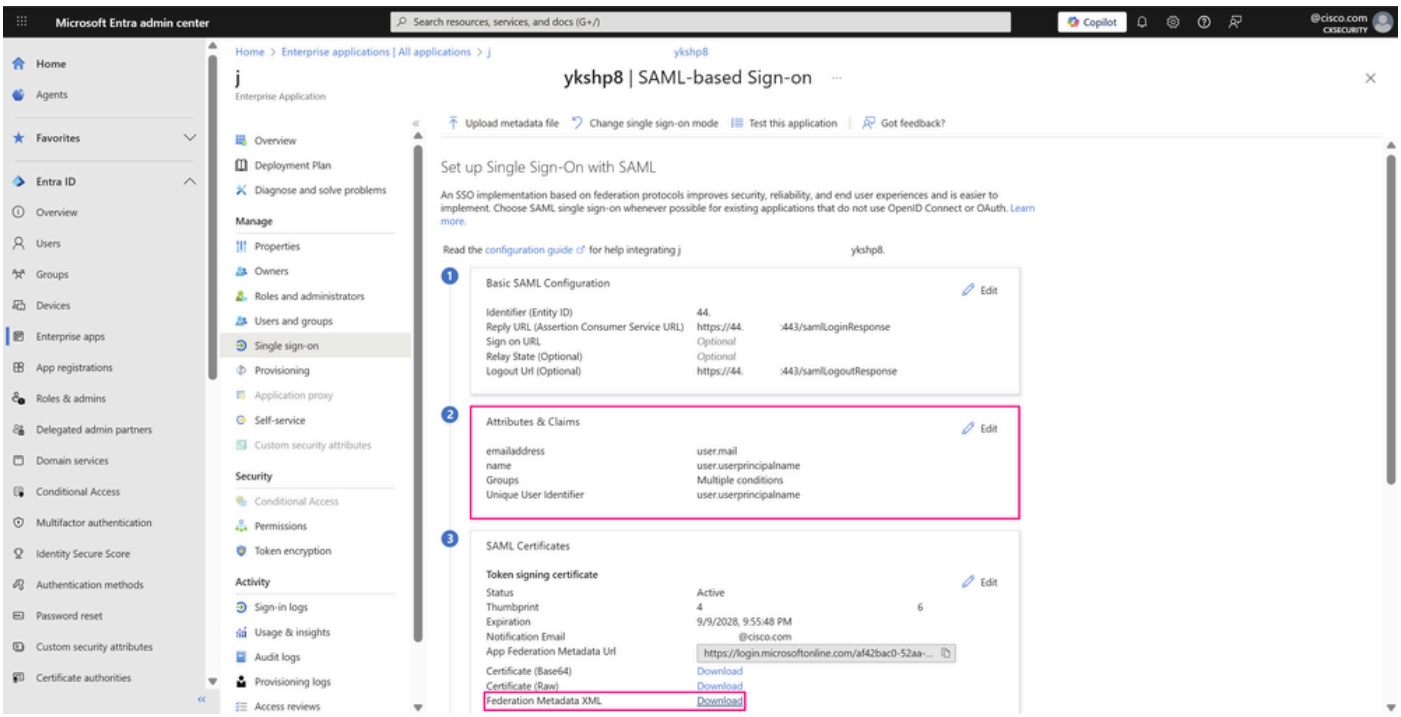
- Wiederholen Sie die gleichen Schritte für eine zweite Anspruchsbedingung für die zweite erstellte Gruppe, die der Operator-Benutzergruppe im Cisco SD-WAN Manager zugeordnet ist. Dieser Prozess ist für jede Gruppe mit spezifischen Berechtigungen erforderlich, die Sie bei der Anwendung anmelden möchten. Sie können auch mehrere Gruppen innerhalb einer Bedingung hinzufügen. Klicken Sie auf Speichern, um die Änderungen zu speichern.



Seite "Forderungen verwalten"

- Auf der Seite Einmalige Anmeldung mit SAML einrichten werden im Abschnitt Attribute und Ansprüche die vorgenommenen Änderungen angezeigt. Um die Konfiguration in der

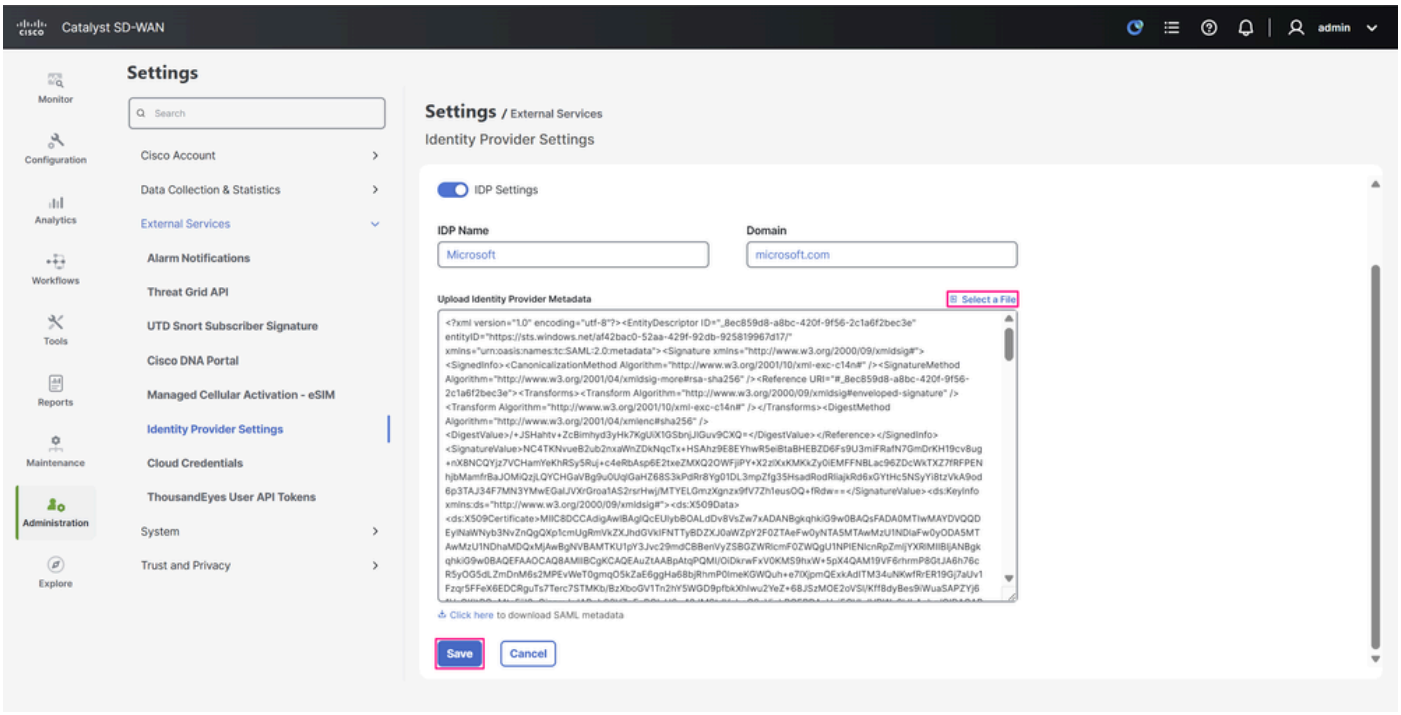
Microsoft Entra-ID abzuschließen, klicken Sie unter SAML-Zertifikate auf Herunterladen neben Verbundmetadaten-XML, um die XML-Datei herunterzuladen, die Identitätsdienste für die Anwendung bereitstellt.



SSO mit SAML-Konfigurationsseite

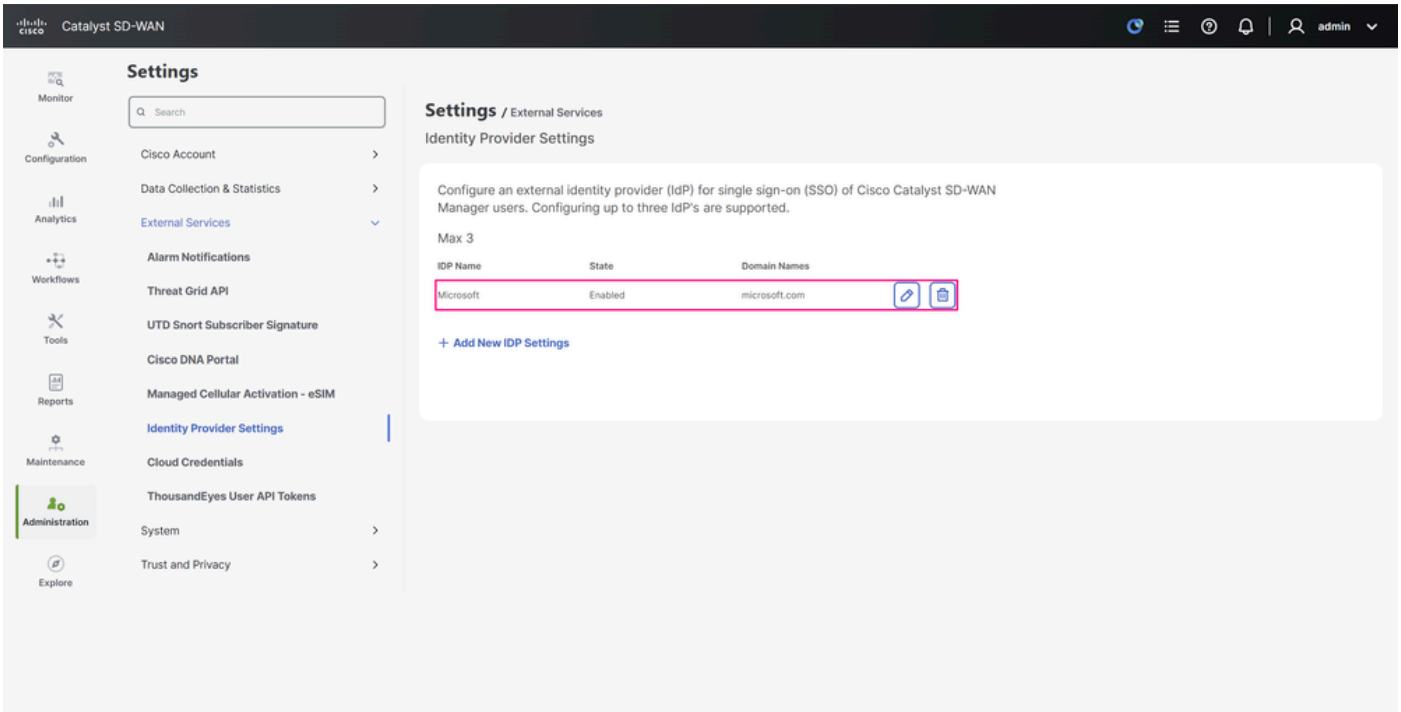
Schritt 5: Importieren der Microsoft Entra ID SAML-Metadatendatei in den Cisco SD-WAN Manager

- Um die Verbundmetadaten in den Cisco SD-WAN Manager hochzuladen, navigieren Sie zu Administration > Settings > External Services > Identity Provider Settings, und klicken Sie auf Select a file. Wählen Sie die Datei aus, die Sie gerade von Microsoft Entra ID heruntergeladen haben, und klicken Sie dann auf Speichern.



Seite "IDp Settings Configuration"

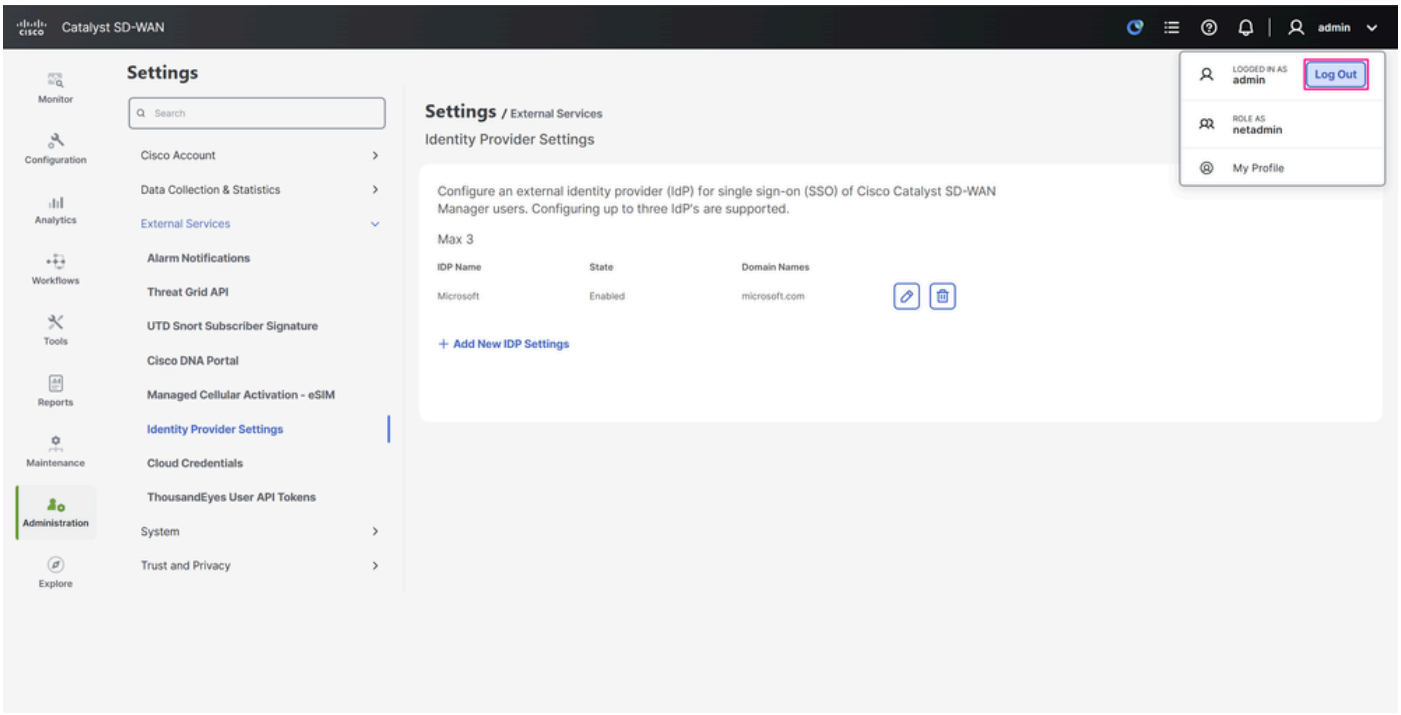
- Die IdP-Einstellungen und Metadaten werden jetzt gespeichert.



Seite "IDp Settings Configuration"

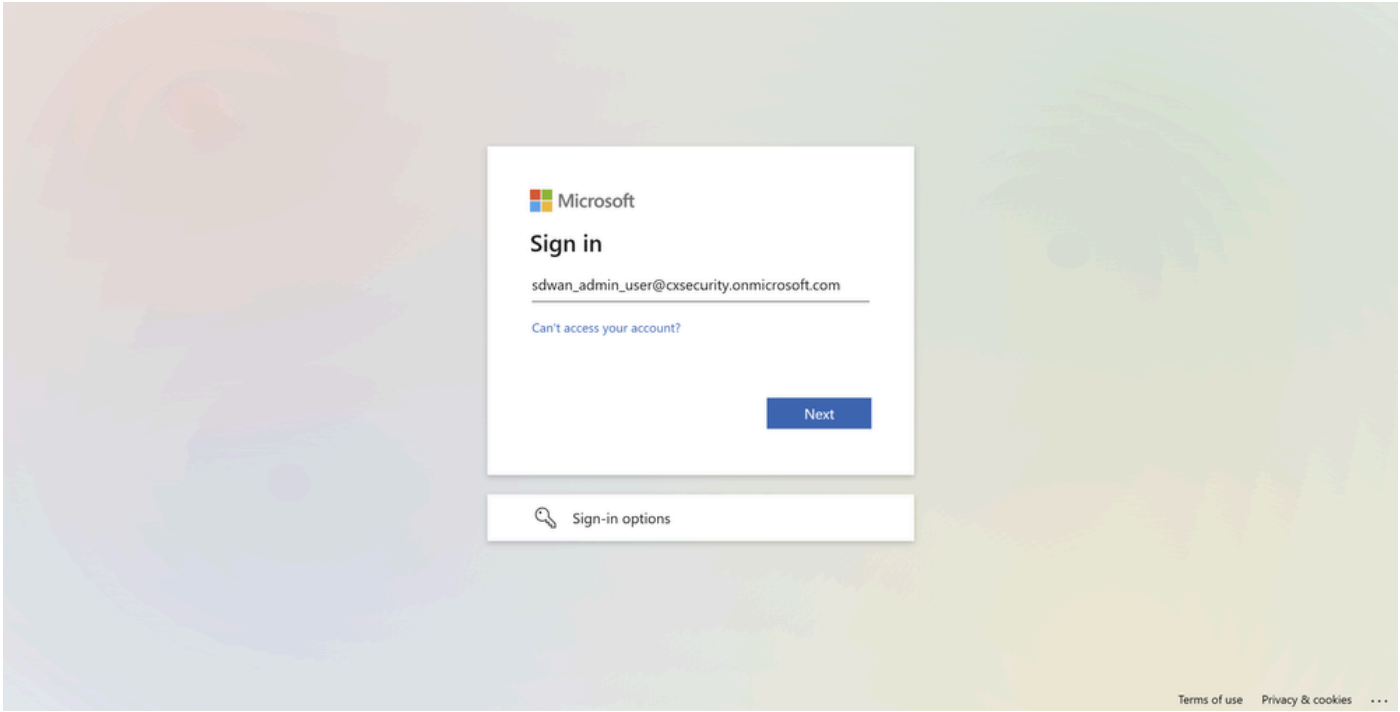
Überprüfung

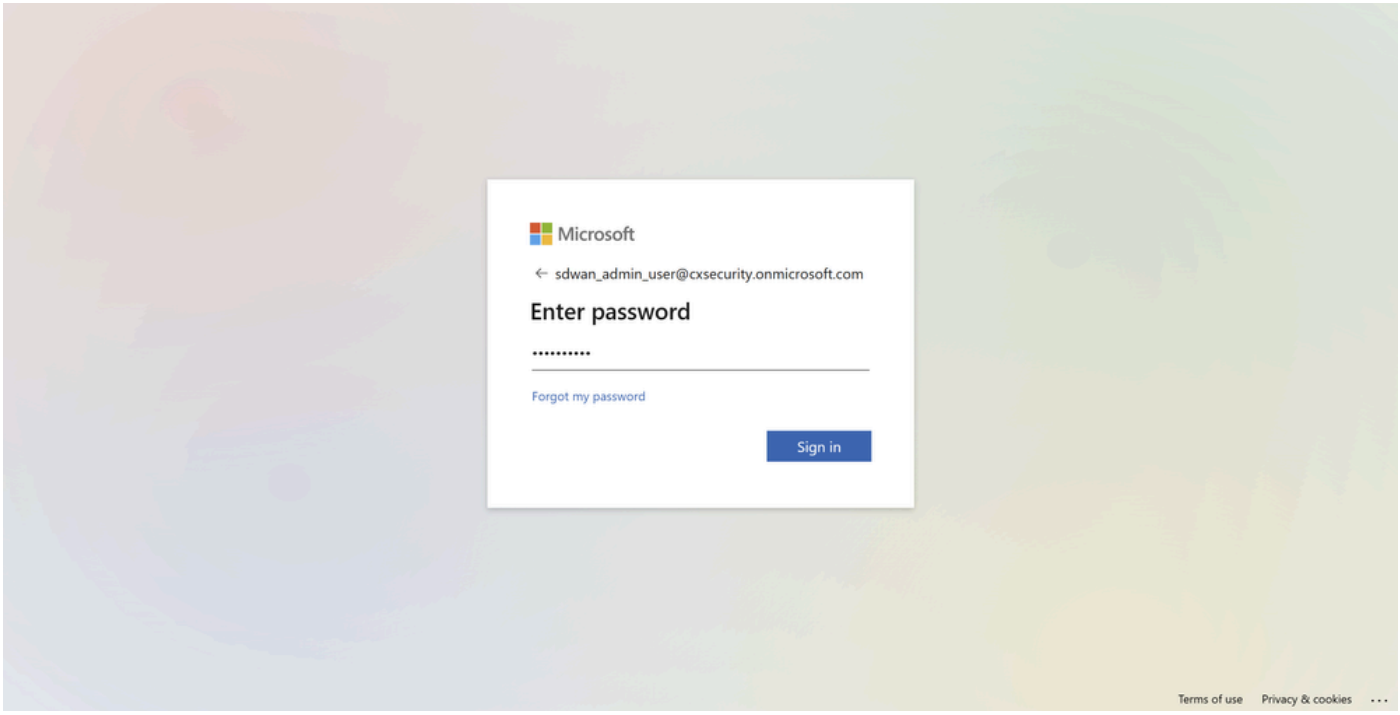
- Klicken Sie auf Ihren Profilnamen in der oberen rechten Ecke der Benutzeroberfläche, um die Optionen zu erweitern, und klicken Sie dann auf Abmelden, um sich vom Portal abzumelden.



Profilmenü

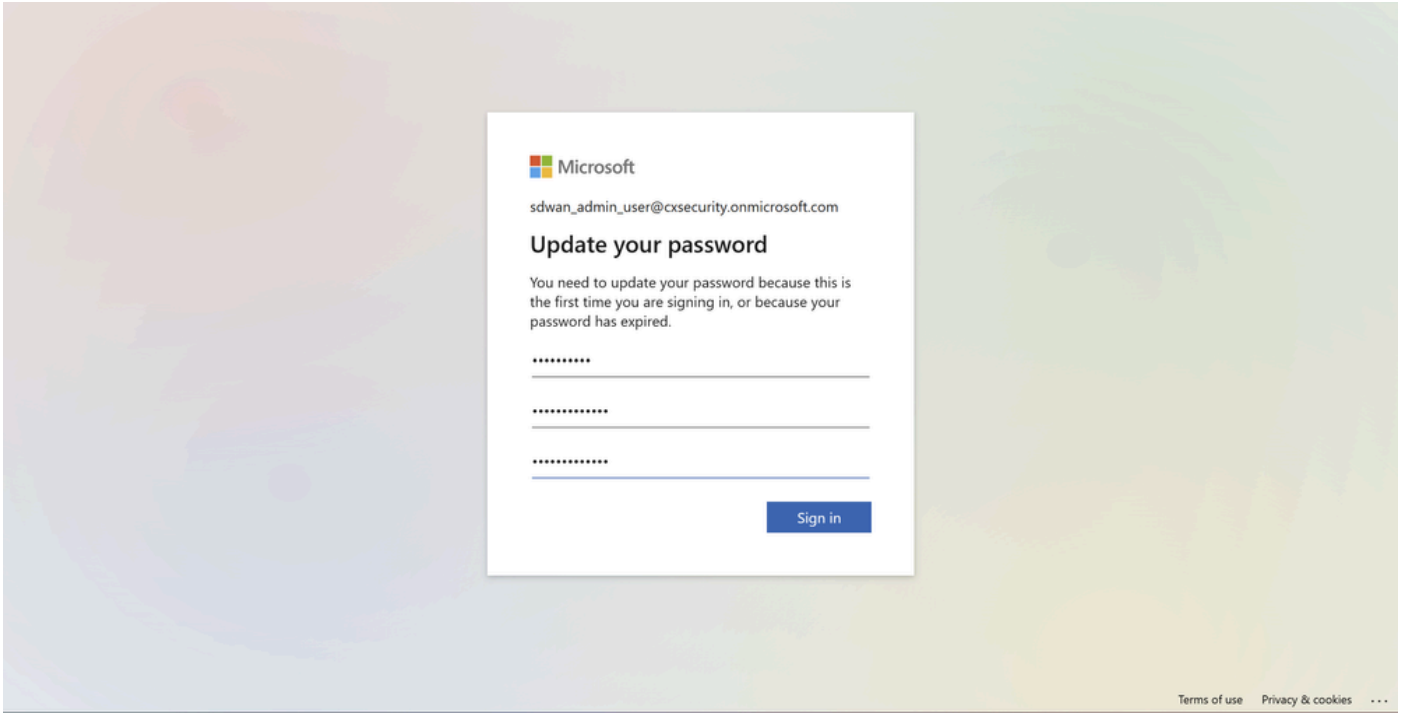
- Sie werden sofort zum Microsoft-Authentifizierungsbildschirm weitergeleitet, auf dem Sie sich mit den Anmeldeinformationen der Microsoft Entra ID SSO-Benutzer anmelden.





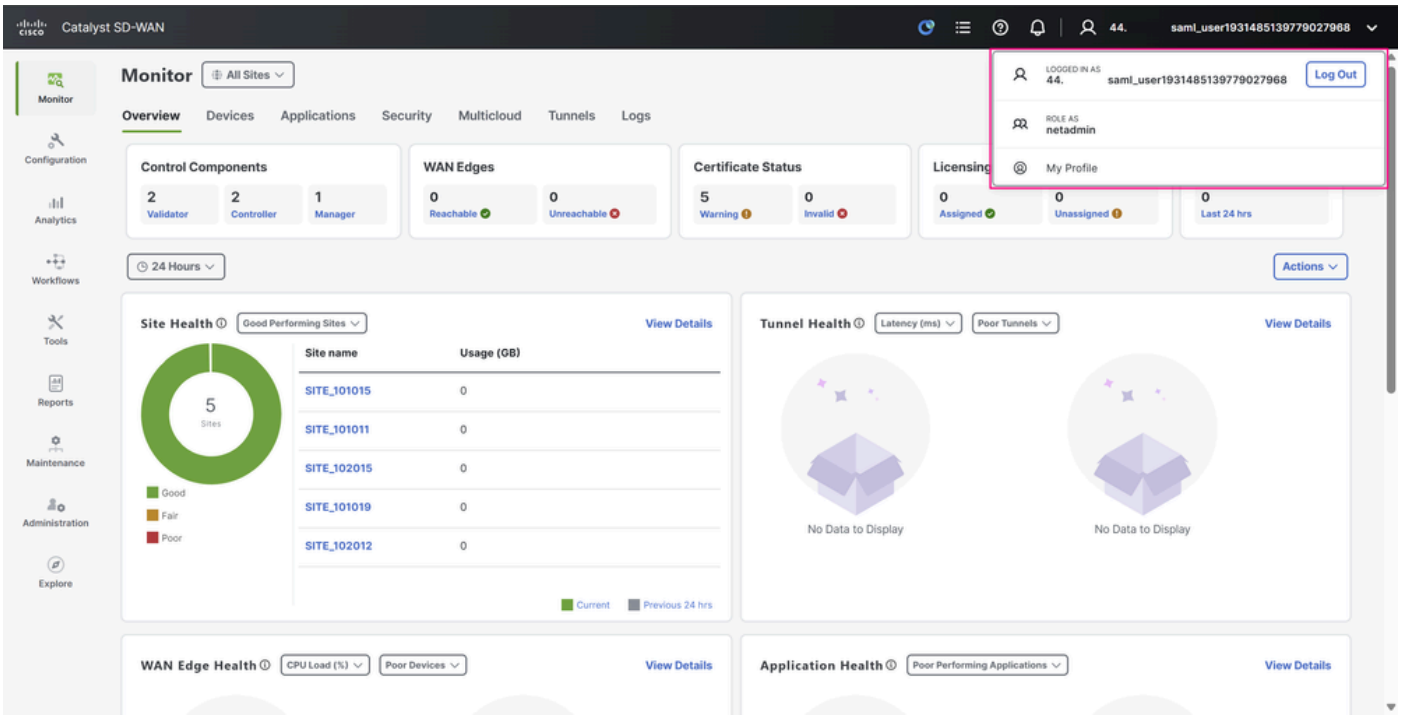
Microsoft-Anmeldebildschirm

- Da sich der SSO-Benutzer zum ersten Mal anmeldet, wird eine Kennwortänderung angefordert.



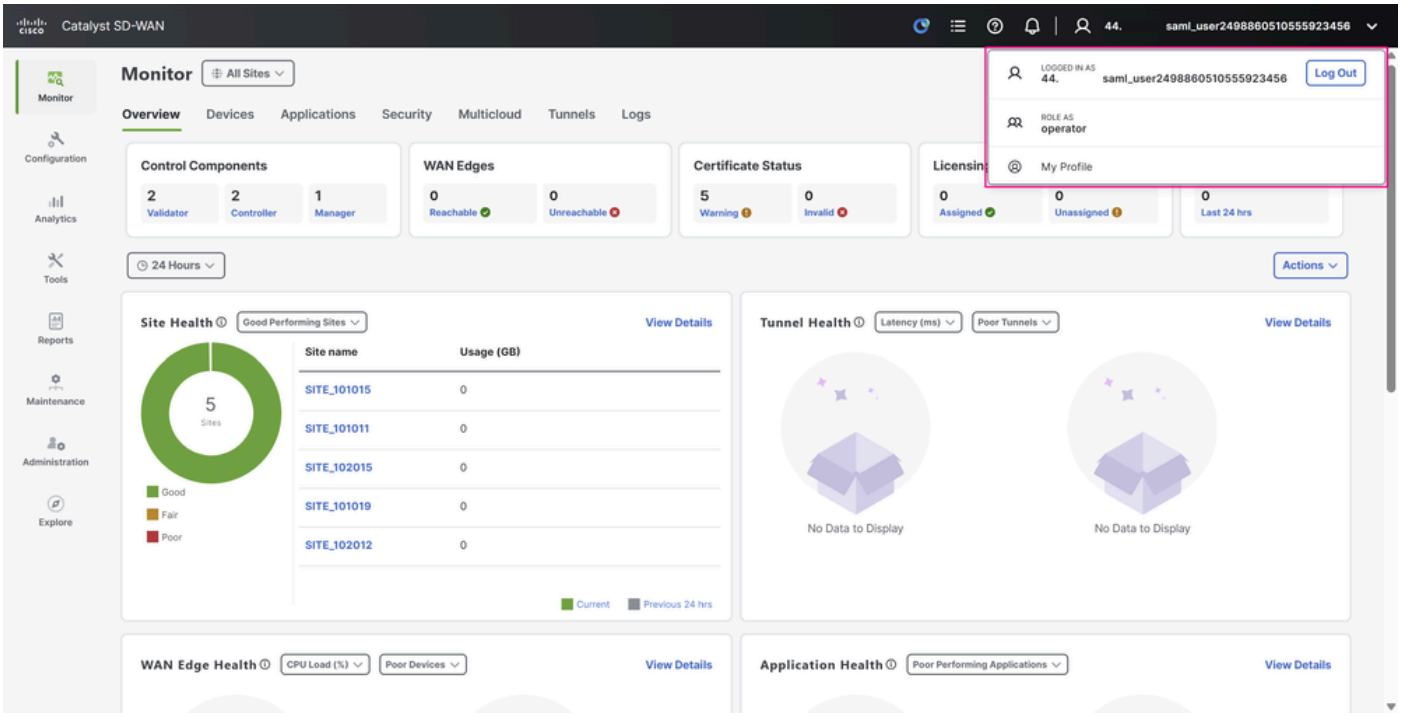
Microsoft-Anmeldebildschirm

- Erweitern Sie nach einer erfolgreichen Anmeldung die Details Ihres Profils erneut in der oberen rechten Ecke des Dashboards, und Sie können bestätigen, dass der Benutzer mit einer netadmin-Rolle erkannt wird, genau wie in Microsoft Entra ID konfiguriert.



Benutzeroberfläche des Cisco SD-WAN-Managers

- Führen Sie abschließend den gleichen Anmeldetest mit dem anderen Benutzer durch. Sie sehen dasselbe Verhalten - der Benutzer ist nun mit der Operator-Rolle identifiziert.



Benutzeroberfläche des Cisco SD-WAN-Managers

Zugehörige Informationen

- [Konfigurieren der einmaligen Anmeldung auf dem Cisco IOS XE Catalyst SD-WAN]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.