Configurazione di SSO per SD-WAN con Microsoft Entra ID

Sommario

Introduzione

In questo documento viene descritto come configurare Single Sign-On (SSO) per le reti WAN (Wide Area Network) definite dal software Cisco Catalyst (SD-WAN) con Microsoft Entra ID.

Prerequisiti

Requisiti

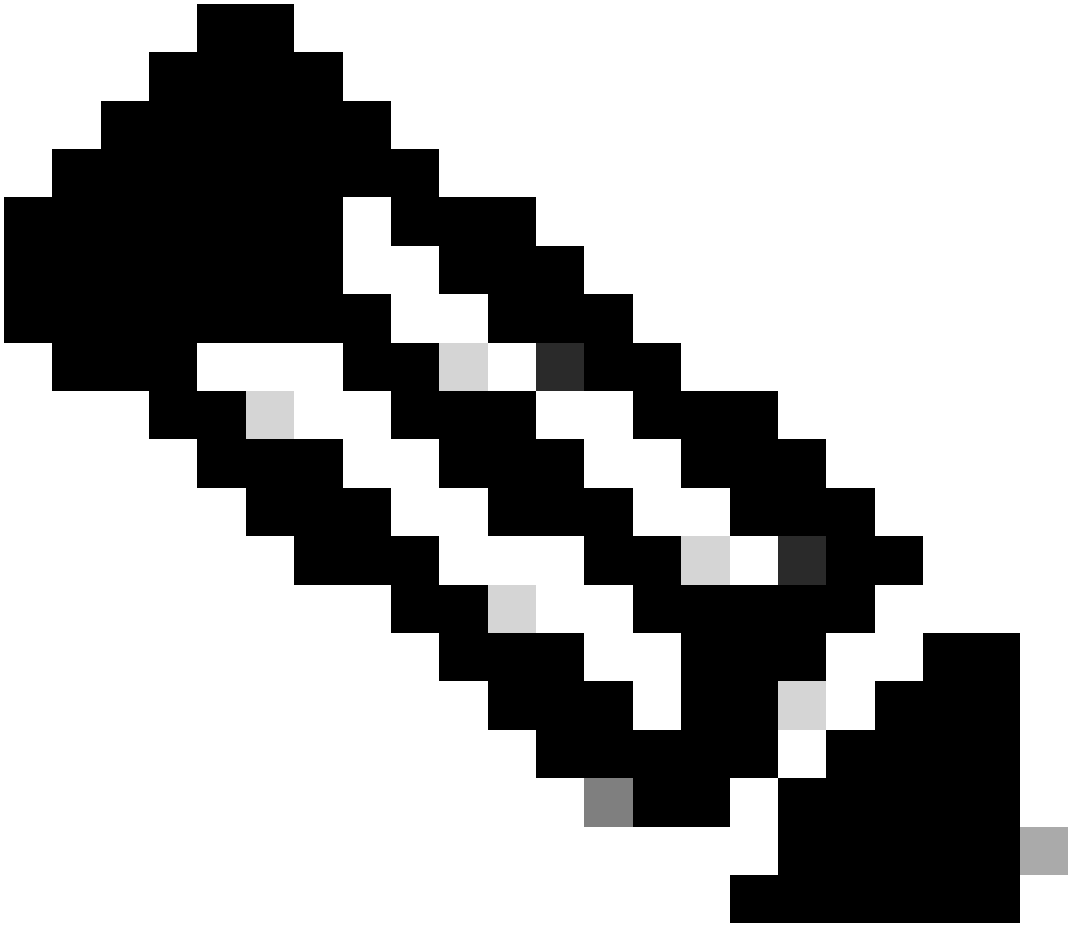
Cisco raccomanda la conoscenza generale dei seguenti argomenti:

- Single Sign-On
- Soluzione Cisco Catalyst SD-WAN

Componenti usati

Le informazioni fornite in questo documento si basano su:

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



Nota: La soluzione precedentemente nota come Azure Active Directory (Azure AD) è ora denominata Microsoft Entra ID.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Single Sign-On è un metodo di autenticazione che consente agli utenti di accedere in modo sicuro a più applicazioni o siti Web indipendenti utilizzando un unico insieme di credenziali. Con l'SSO, gli utenti non devono più accedere separatamente a ciascuna applicazione: una volta autenticati, possono accedere senza problemi a tutte le risorse consentite.

Un modo comune per implementare SSO è tramite la federazione, che stabilisce l'attendibilità tra un provider di identità (IdP) e un provider di servizi (SP) utilizzando protocolli quali SAML 2.0, WS-

Federation o OpenID Connect. La federazione migliora la sicurezza, l'affidabilità e l'esperienza utente centralizzando l'autenticazione.

Microsoft Entra ID è un provider di identità basato su cloud ampiamente utilizzato che supporta questi protocolli di federazione. In una configurazione SSO con Cisco Catalyst SD-WAN, Microsoft Entra ID agisce come IdP e Cisco SD-WAN Manager come provider di servizi.

L'integrazione funziona come segue:

1. Un amministratore di rete tenta di accedere a Cisco SD-WAN Manager.
2. Cisco SD-WAN Manager invia una richiesta di autenticazione a Microsoft Entra ID.
3. In Microsoft Entra ID viene richiesto all'amministratore di eseguire l'autenticazione con il proprio account Entra ID (Microsoft).
4. Una volta convalidate le credenziali, Microsoft Entra ID invia una risposta sicura al Cisco SD-WAN Manager per confermare l'autenticazione.
5. Cisco SD-WAN Manager concede l'accesso senza richiedere credenziali separate.

In questo modello:

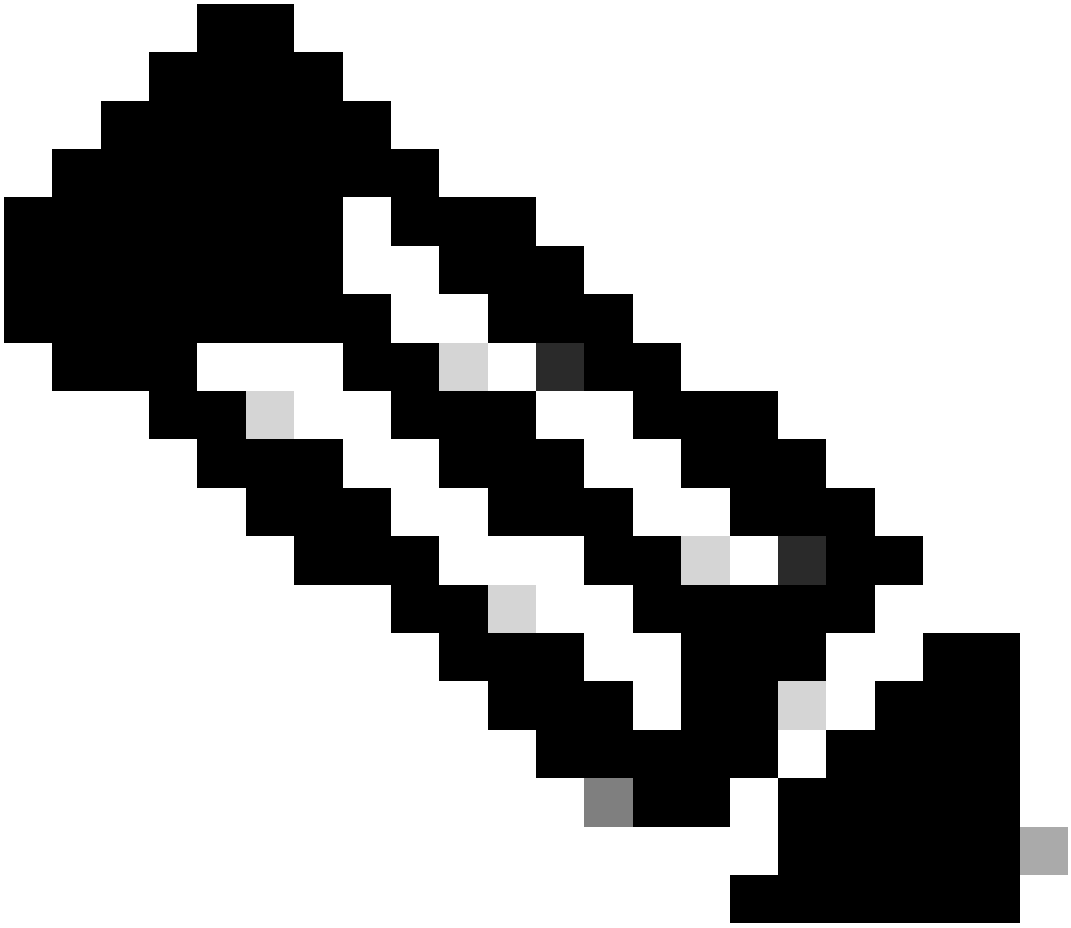
- Provider di identità (IdP): memorizza i dati utente e convalida le credenziali (ad esempio, Microsoft Entra ID, Okta, PingID, ADFS).
- Service Provider - Ospita l'applicazione a cui accedere (ad esempio, Cisco SD-WAN Manager).
- Utenti: hanno un account nella directory IdP e sono autorizzati ad accedere al provider di servizi.

Cisco Catalyst SD-WAN è compatibile con qualsiasi IdP conforme a SAML 2.0 se configurato secondo gli standard del settore.

Vantaggi dell'utilizzo di Single Sign-On

- Centralizza la gestione delle credenziali tramite il provider di identità.
- Maggiore sicurezza dell'autenticazione grazie all'eliminazione di più password vulnerabili.
- Accesso sicuro semplificato per gli amministratori.
- Consente di accedere con un solo clic a Cisco Catalyst SD-WAN Manager e ad altre applicazioni autorizzate.

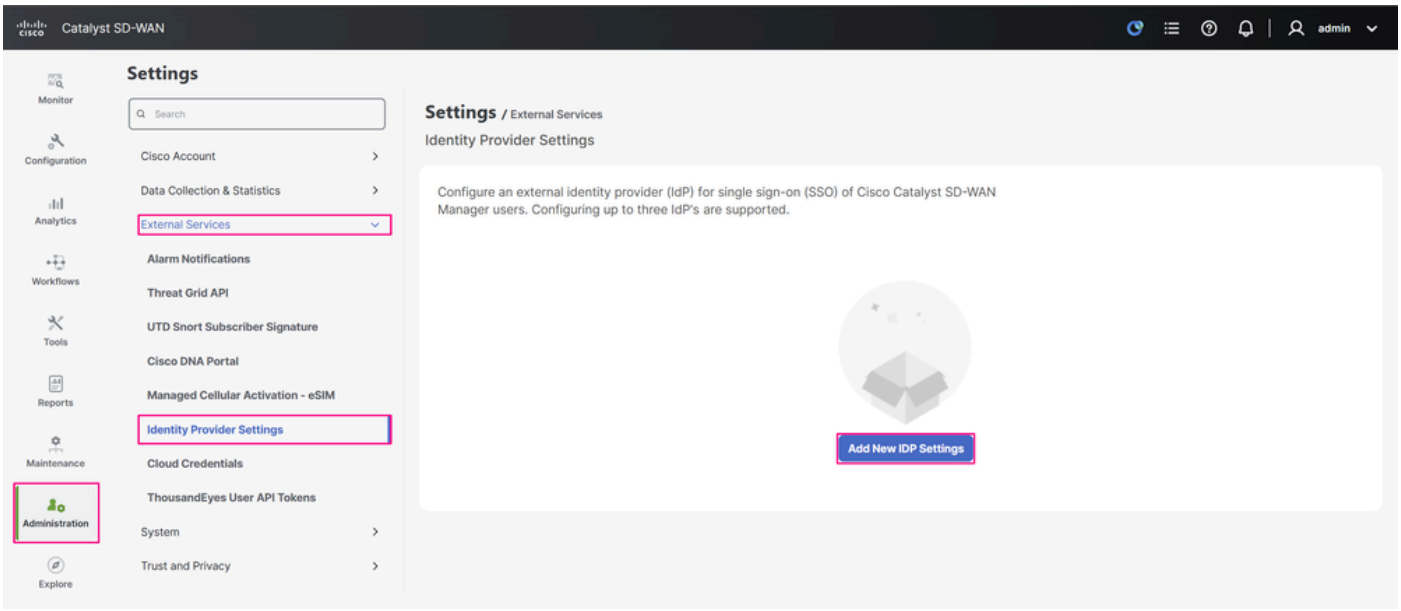
Configurazione



Nota: Versione minima supportata: Cisco Catalyst SD-WAN Manager release 20.8.1.

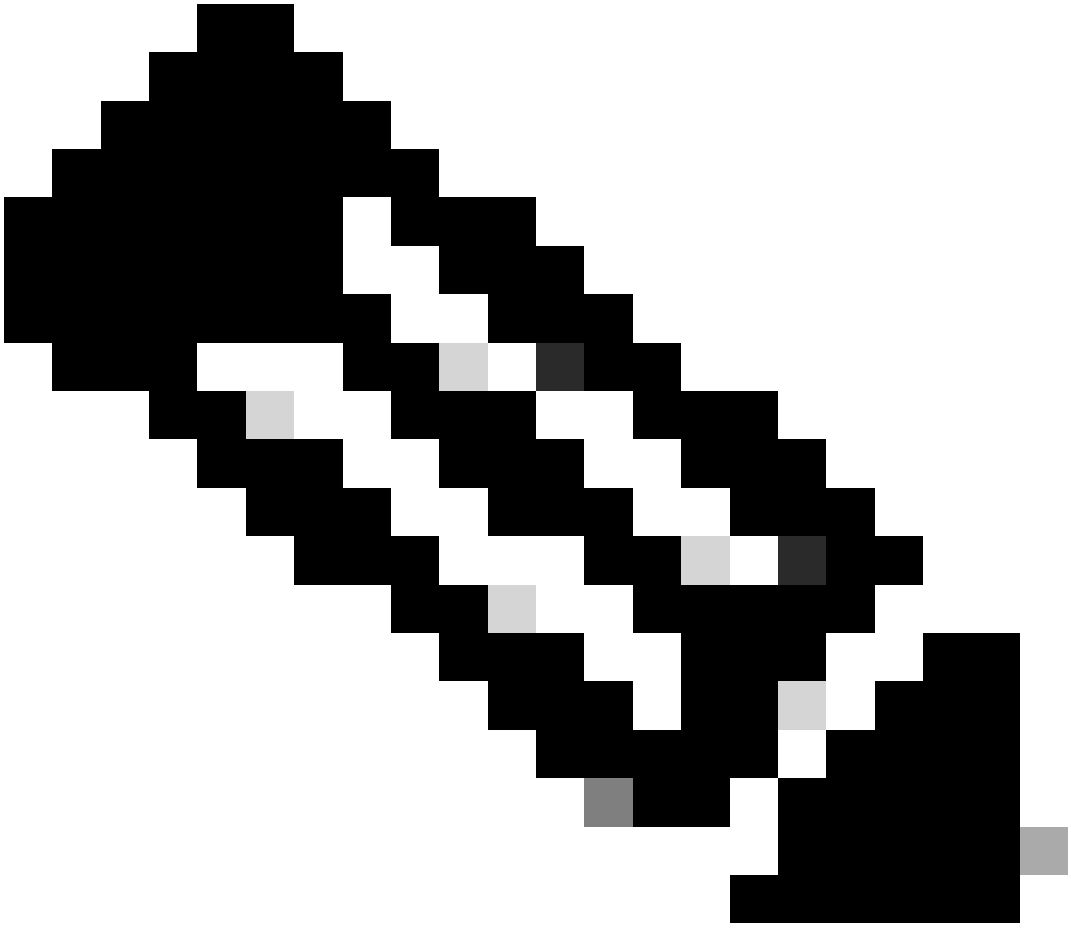
Passaggio 1. Ottenere i metadati SAML di Cisco SD-WAN Manager

- In Cisco SD-WAN Manager, selezionare Amministrazione > Impostazioni > Servizi esterni > Impostazioni provider di identità, quindi fare clic su Aggiungi nuove impostazioni IDP.



Interfaccia utente di Cisco SD-WAN Manager

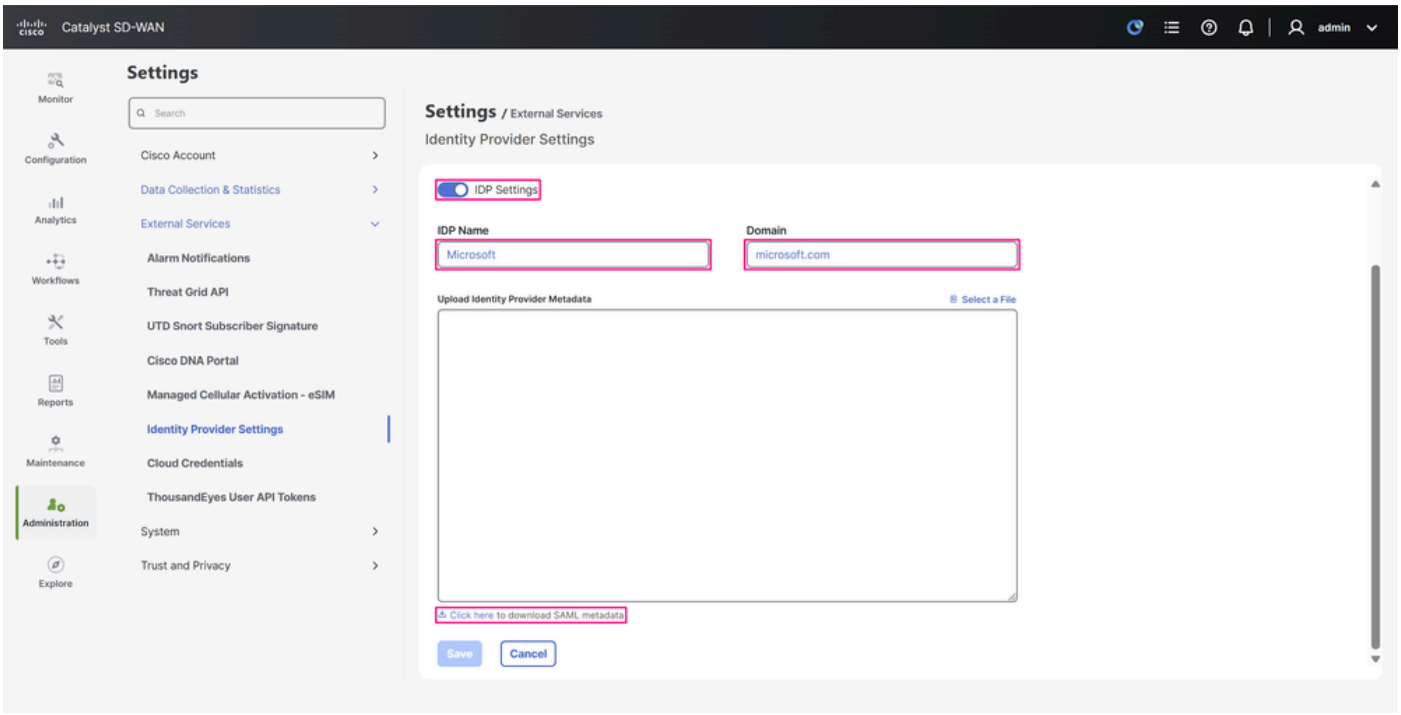
- Attiva/disattiva Impostazioni IDP per abilitare le impostazioni del provider di identità. Nel campo Nome IDP, immettere un nome che faccia riferimento all'IdP in uso e nel campo Dominio, immettere un dominio che corrisponda ai nomi di dominio utilizzati dagli utenti nell'applicazione enterprise dell'organizzazione. Fare clic su Fare clic qui per scaricare i metadati SAML e salvare il file XML dei metadati nel computer. Questo file viene utilizzato per configurare SSO in Microsoft Entra ID nel passaggio successivo.



Nota: In questo esempio, il file XML dei metadati punta direttamente all'indirizzo IP di Cisco SD-WAN Manager, ma in molti ambienti di produzione punta al relativo FQDN (Fully Qualified Domain Name). Per un Cisco SD-WAN Manager standalone, l'ID entità contenuto nei metadati corrisponde all'URL utilizzato per accedere a Cisco SD-WAN Manager al momento del download. Ciò significa che funziona sia con l'indirizzo IP che con il nome di dominio completo (FQDN), poiché è una configurazione a nodo singolo.

Per un cluster Cisco SD-WAN Manager, lo stesso principio si applica in quanto l'FQDN punta a uno dei nodi del cluster e i metadati includono questo dominio come ID entità. La differenza sta nel fatto che, sia che si utilizzino metadati con il nome di dominio completo del cluster o da un nodo specifico utilizzando il relativo indirizzo IP, una volta completata l'integrazione SSO con Microsoft Entra ID, anche gli altri nodi reindirizzano al prompt di accesso IdP.

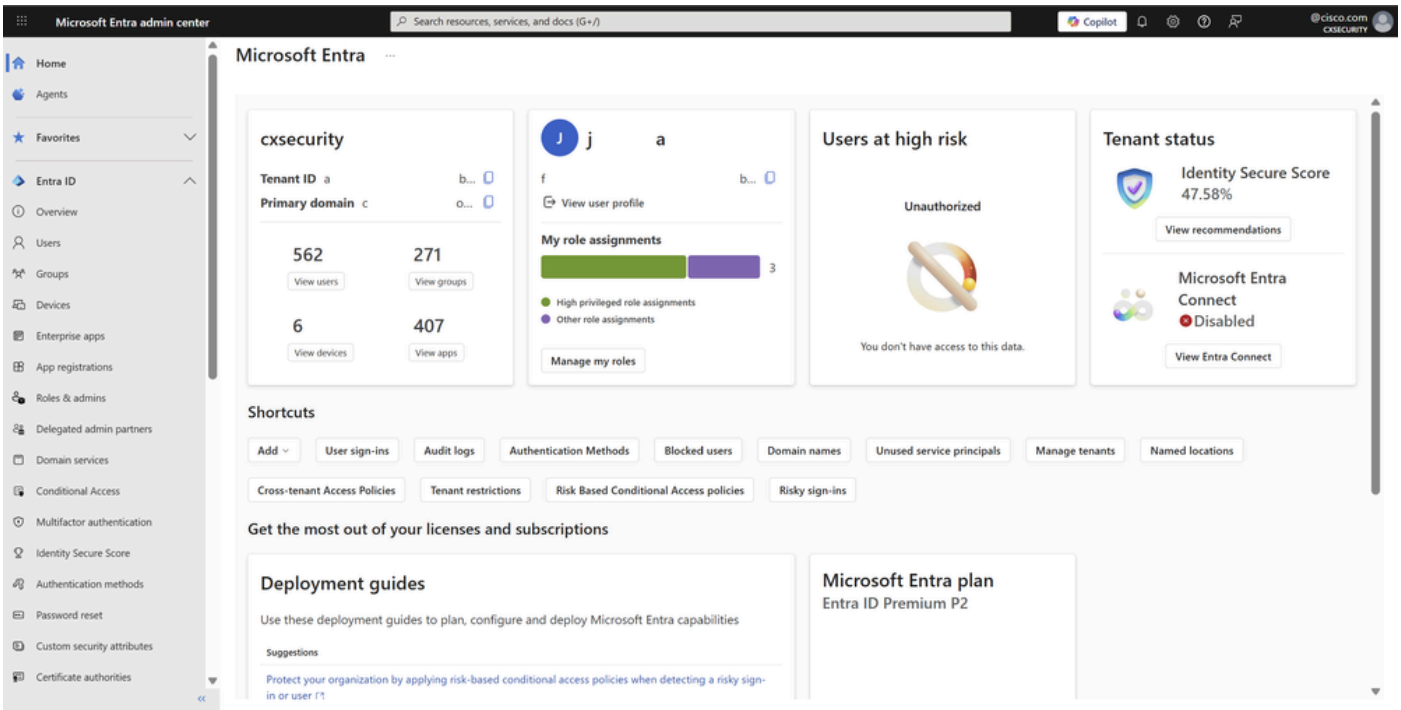
Il requisito principale in entrambi gli scenari è che l'ID entità utilizzato in Cisco SD-WAN Manager, sia che si tratti di un indirizzo IP o di un FQDN, corrisponda all'identificatore configurato sul lato IdP.



Pagina Configurazione impostazioni IdP

Passaggio 2. Configurare un'applicazione enterprise per SSO in Microsoft Entra ID

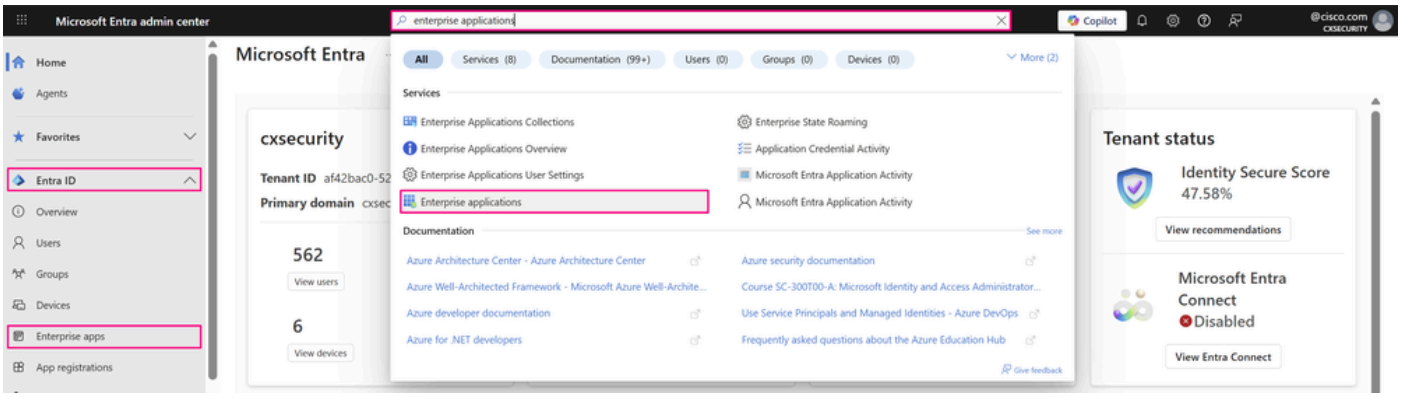
- Accedere al portale dell'interfaccia di amministrazione di Microsoft Entra con uno dei seguenti ruoli: Amministratore applicazione cloud, amministratore applicazione o proprietario dell'entità servizio.



Portale di Microsoft Entra Admin Center

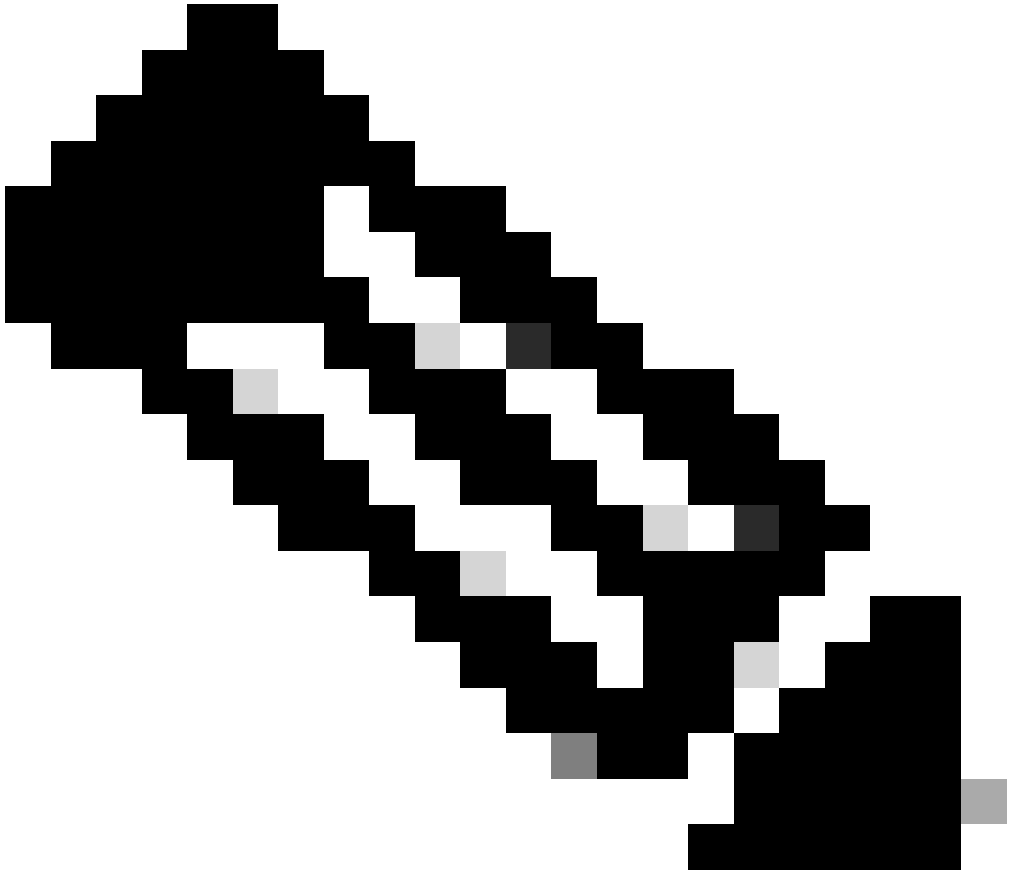
- Passare a Entra ID > App enterprise oppure accedere a questo servizio quando si immettono applicazioni enterprise nella barra di ricerca nella parte superiore del portale e

quindi si sceglie Applicazioni enterprise.



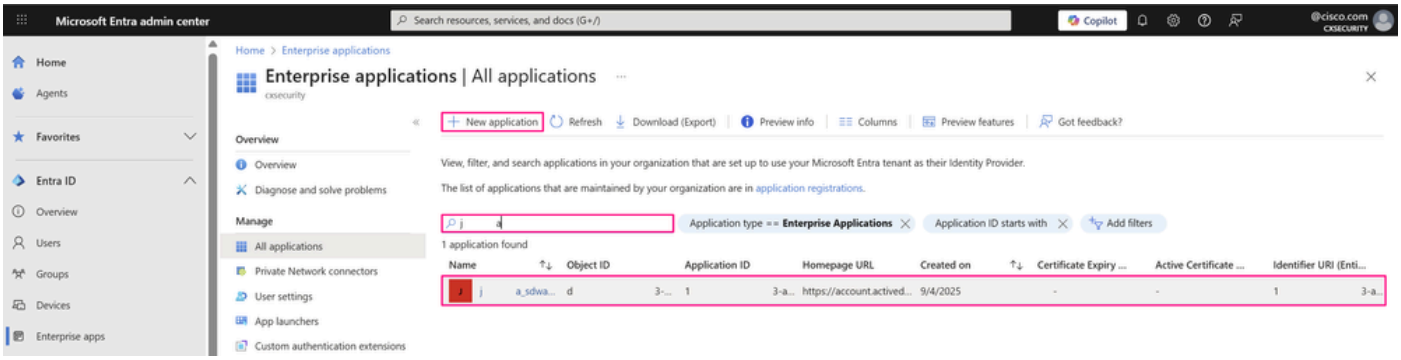
Portale di Microsoft Entra Admin Center

- Viene visualizzata la pagina Tutte le applicazioni. Immettere il nome dell'applicazione esistente nella casella di ricerca, quindi scegliere l'applicazione dai risultati della ricerca.



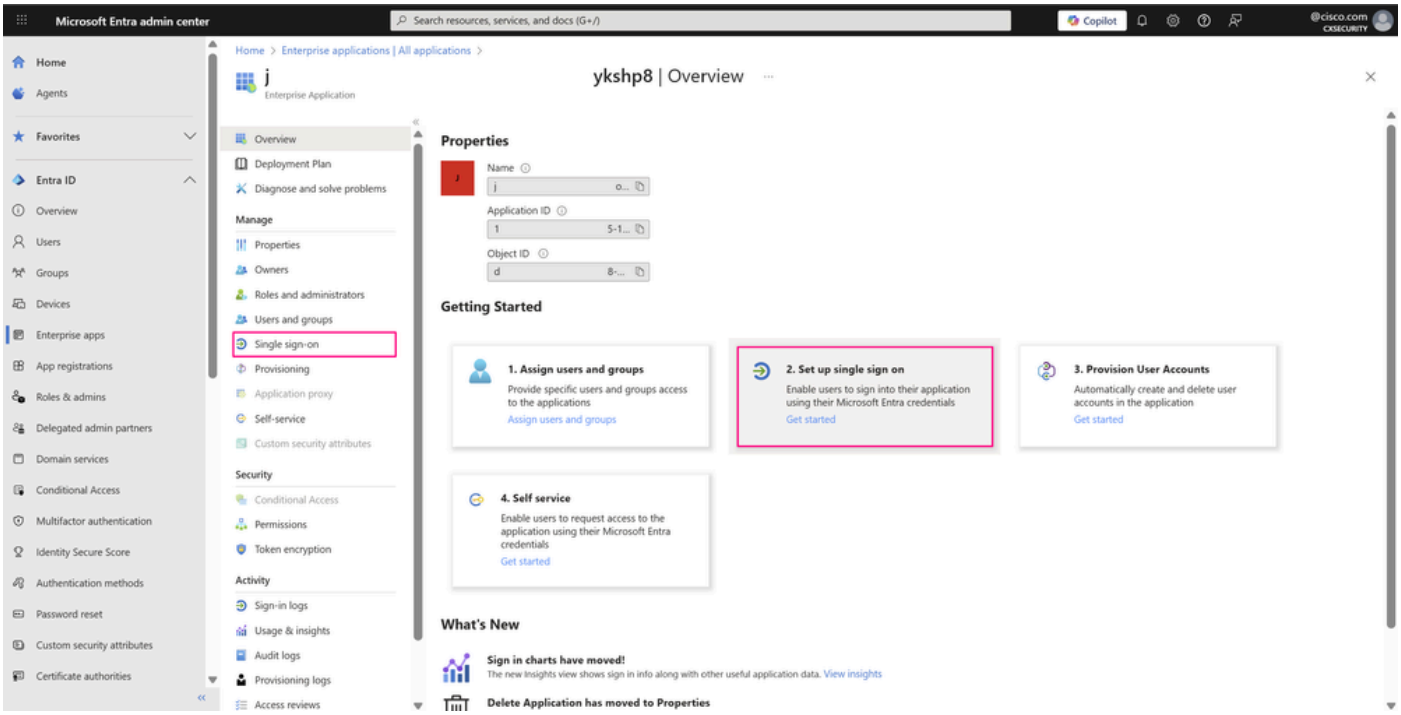
Nota: In questa pagina è possibile creare un'applicazione enterprise personalizzata in base ai requisiti dell'organizzazione e configurarla con l'autenticazione SSO, se

non è già disponibile, quando si fa clic su Nuova applicazione.



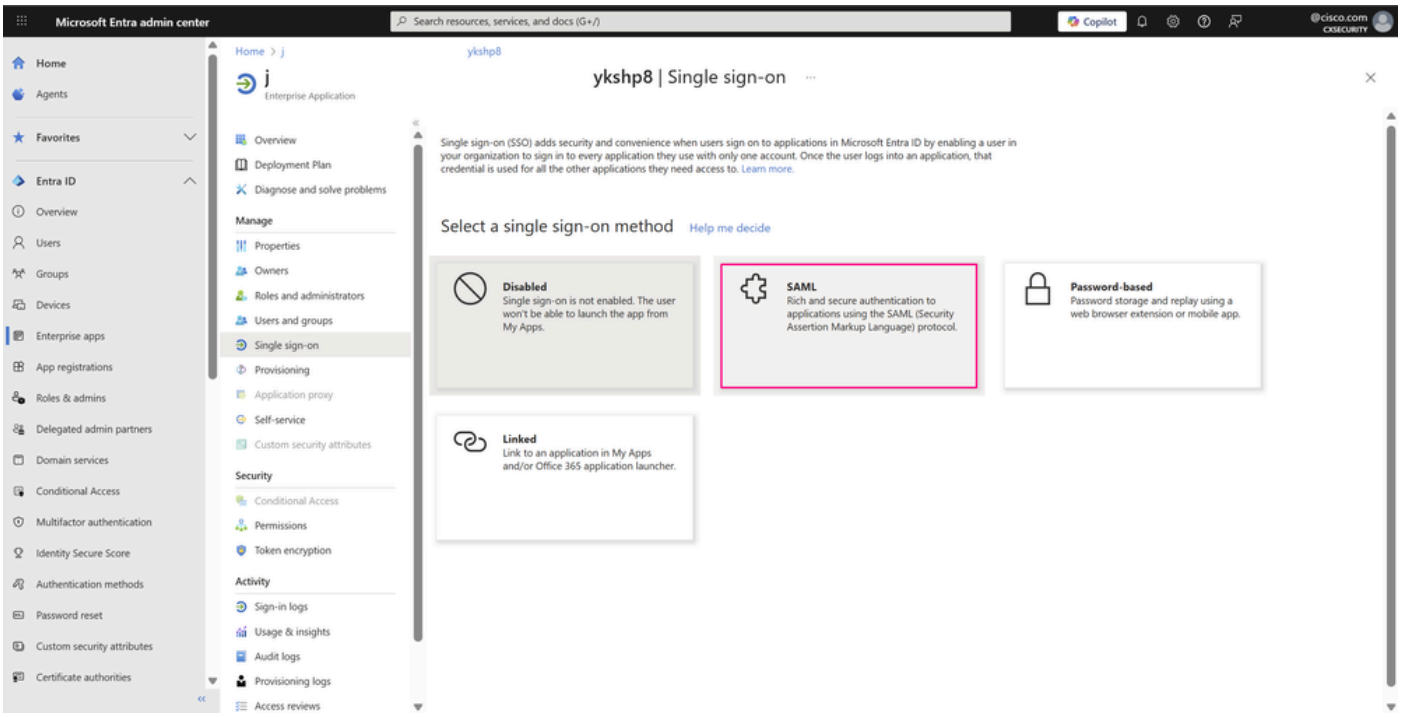
Dashboard applicazioni enterprise

- Nella sezione Gestisci del menu a sinistra fare clic su Single Sign-On oppure fare clic su 2. Impostare Single Sign-On per aprire il riquadro Getting Started nella sezione Overview.



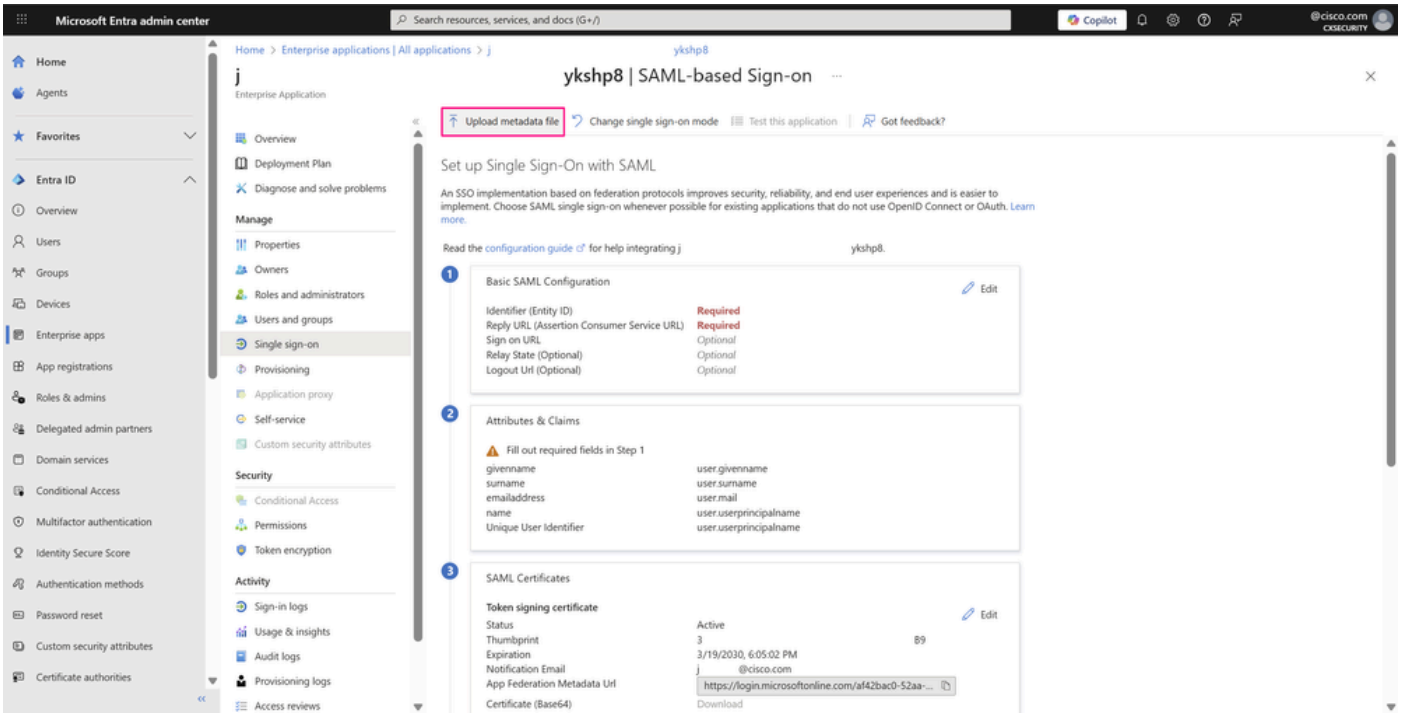
Panoramica delle applicazioni enterprise

- Selezionare SAML per aprire la pagina di configurazione SSO.



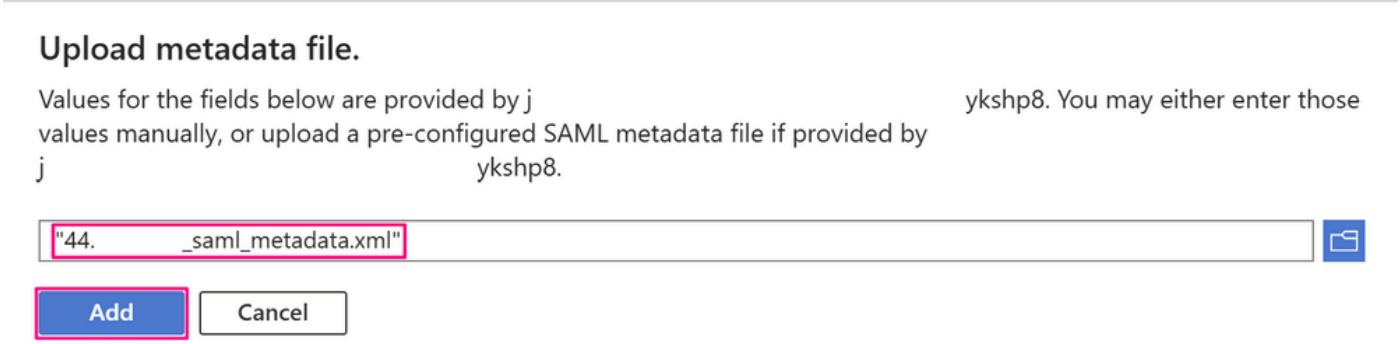
Riquadro Single Sign-On

- Nella pagina Configura Single Sign-On con SAML fare clic su Carica file metadati.



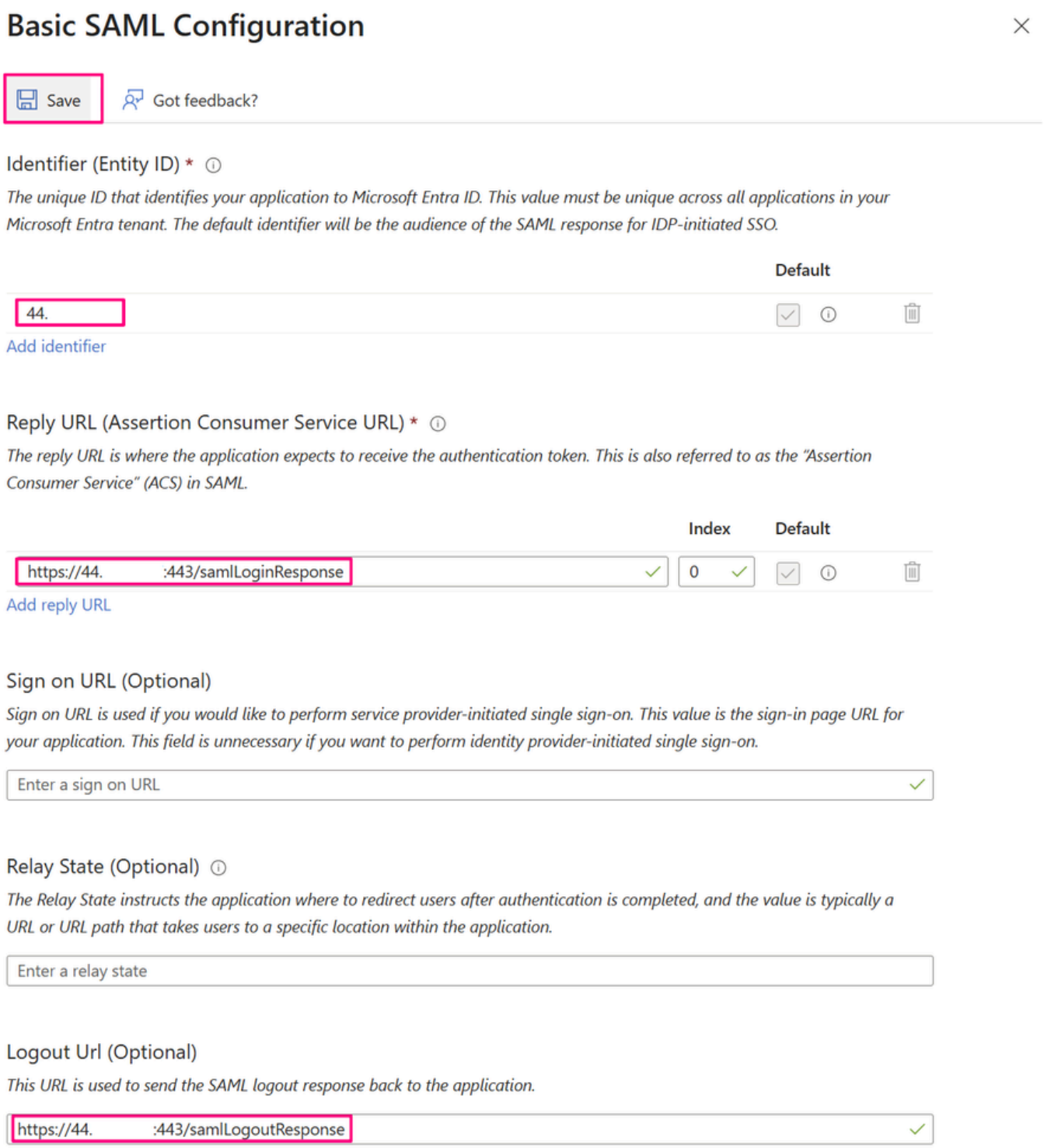
Pagina SSO con configurazione SAML

- Nella finestra Carica file di metadati, individuare e selezionare il file XML dei metadati scaricato in precedenza, quindi fare clic su Aggiungi.



Finestra Carica file di metadati

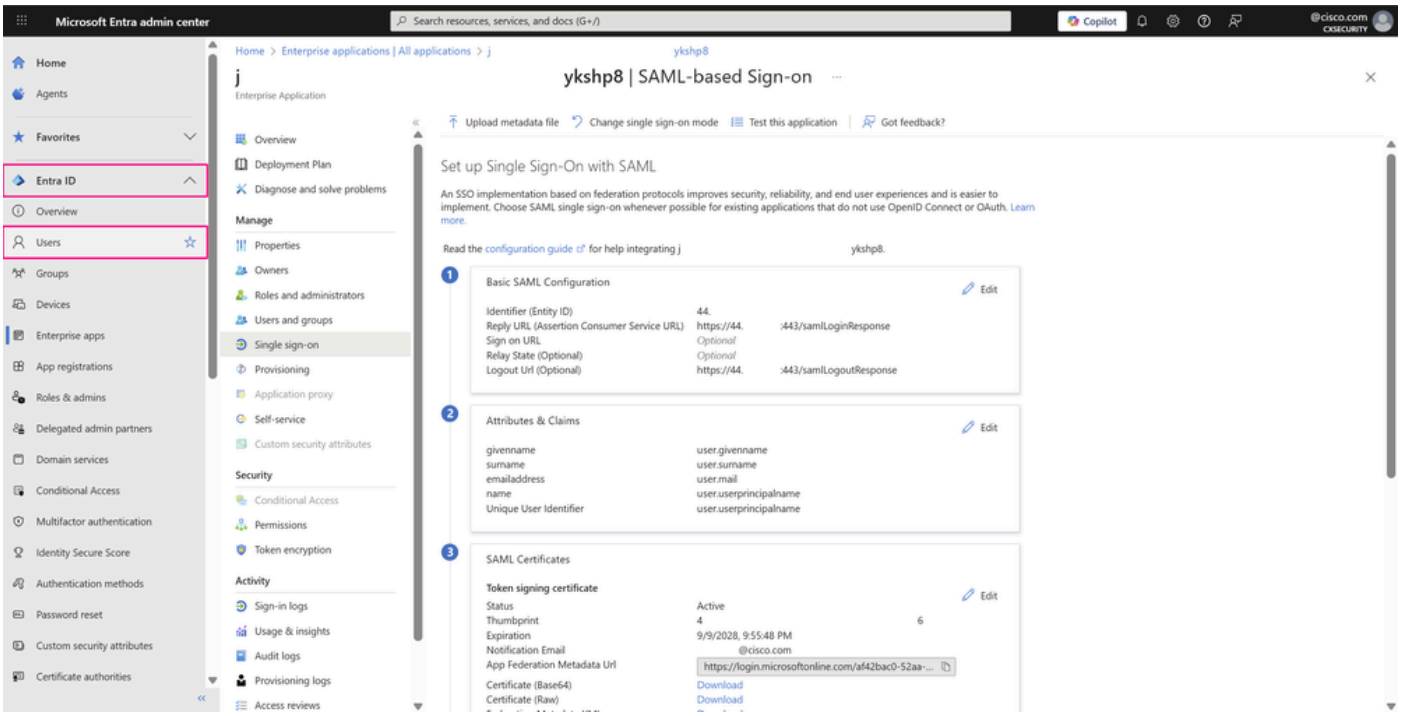
- Nella finestra Basic SAML Configuration (Configurazione SAML di base), l'identificatore (ID entità) è in genere l'URL specifico dell'applicazione (in questo caso, Cisco SD-WAN Manager) con cui si sta eseguendo l'integrazione (come spiegato nel passaggio precedente). I valori URL di risposta e URL di disconnessione vengono inseriti automaticamente una volta caricato correttamente il file. Per continuare, fare clic su Salva.



Finestra Configurazione SAML di base

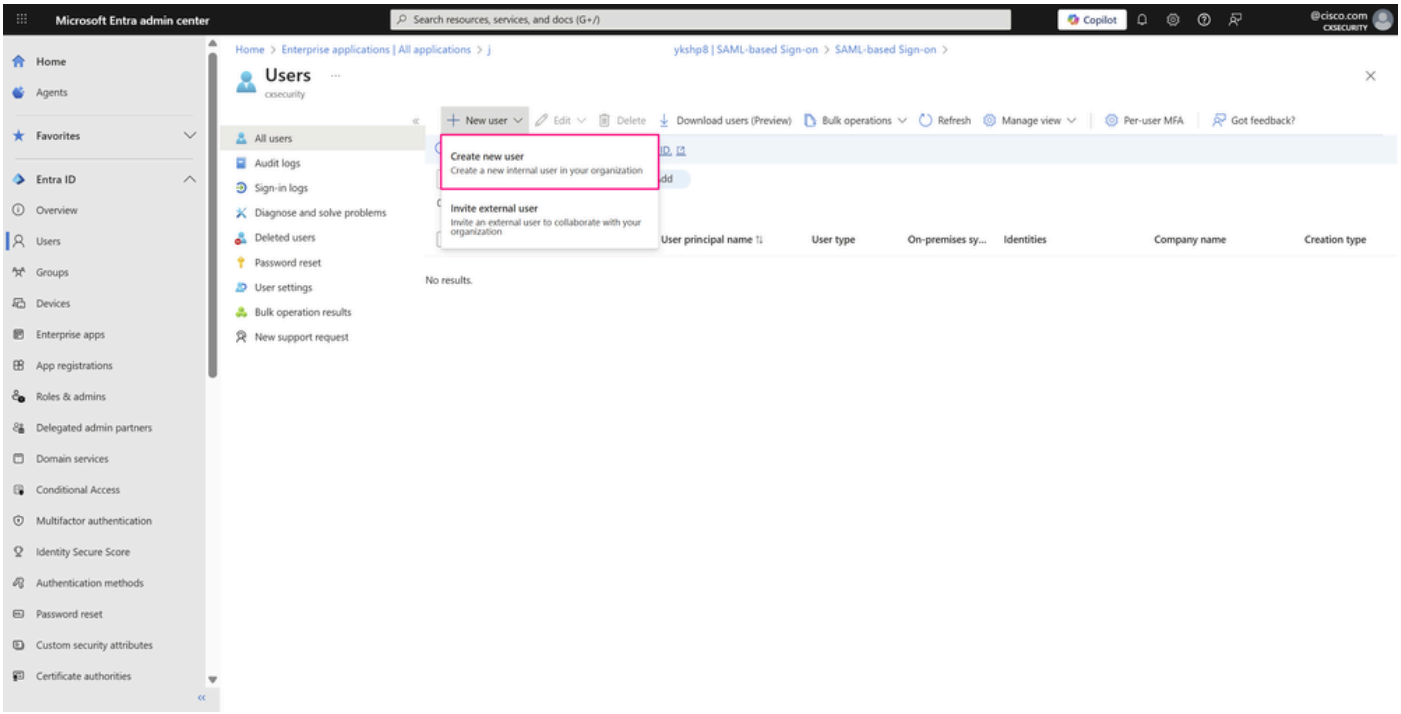
Passaggio 3. Aggiungere un account utente o di gruppo all'applicazione enterprise

- Dopo aver definito i parametri di configurazione SAML dell'applicazione, si procede con l'aggiunta degli utenti o dei gruppi dell'applicazione enterprise che accedono all'applicazione. A tale scopo, passare innanzitutto a Entra ID > Utenti oppure è possibile accedere a questo servizio quando si cerca il nome del servizio nella barra di ricerca nella parte superiore del portale, come illustrato in un passaggio precedente.



Pagina SSO con configurazione SAML

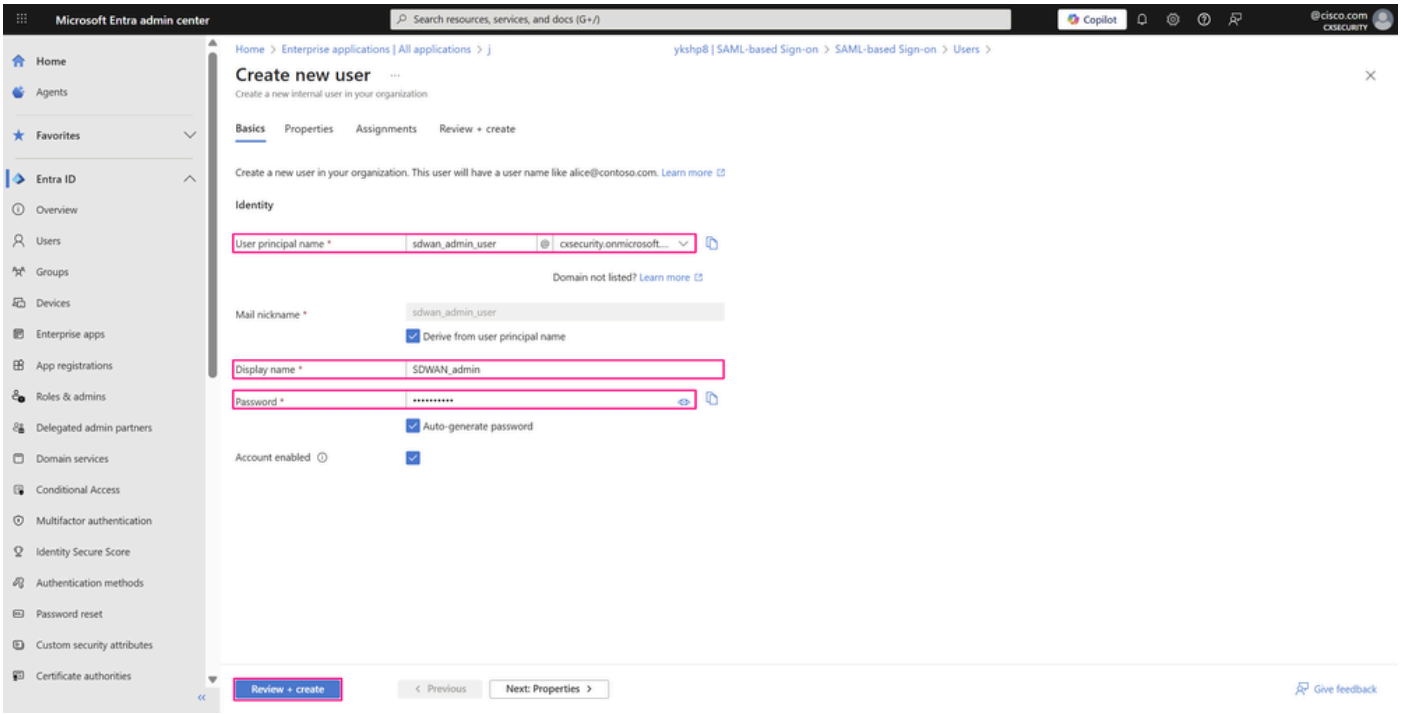
- Creare un utente da associare a un gruppo per illustrare l'autenticazione SSO con Cisco SD-WAN Manager e uno dei suoi gruppi di utenti, netadmin, il più comune negli ambienti di produzione. A tale scopo, passare a Entra ID > Utenti. Quindi, fare clic su Nuovo utente e scegliere Crea nuovo utente.



Dashboard utenti

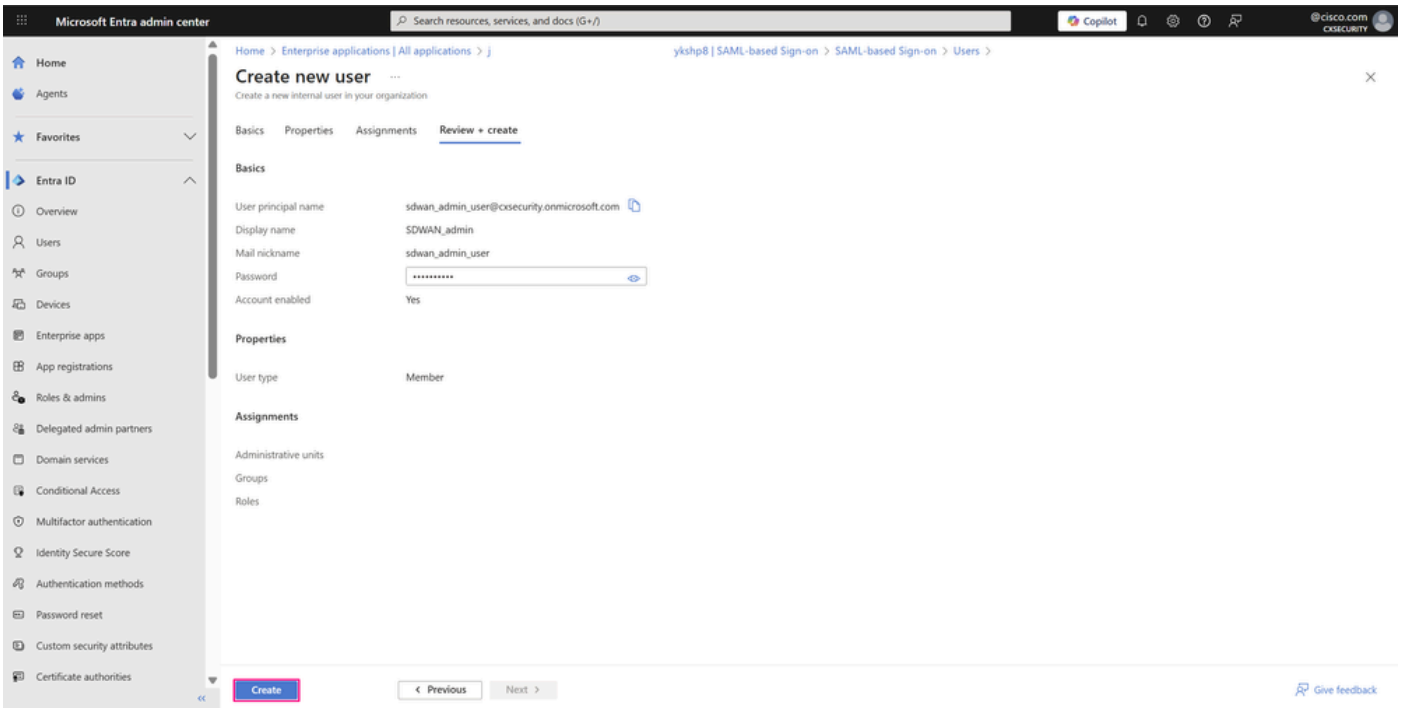
- La scheda Nozioni fondamentali contiene i campi fondamentali necessari per creare un nuovo utente.
  - Per il nome dell'entità utente, immettere un nome utente univoco e scegliere un dominio dall'elenco a discesa dei domini disponibili nell'organizzazione.

- Immettere un nome visualizzato per l'utente.
- Deselezionare Genera password automaticamente se si desidera immettere una password personalizzata o lasciare selezionata questa opzione per generarne una automaticamente.
- È possibile aggiungere l'utente a un gruppo nella scheda Assegnazioni, ma poiché l'appartenenza al gruppo non è stata ancora creata, fare clic su Rivedi + crea.



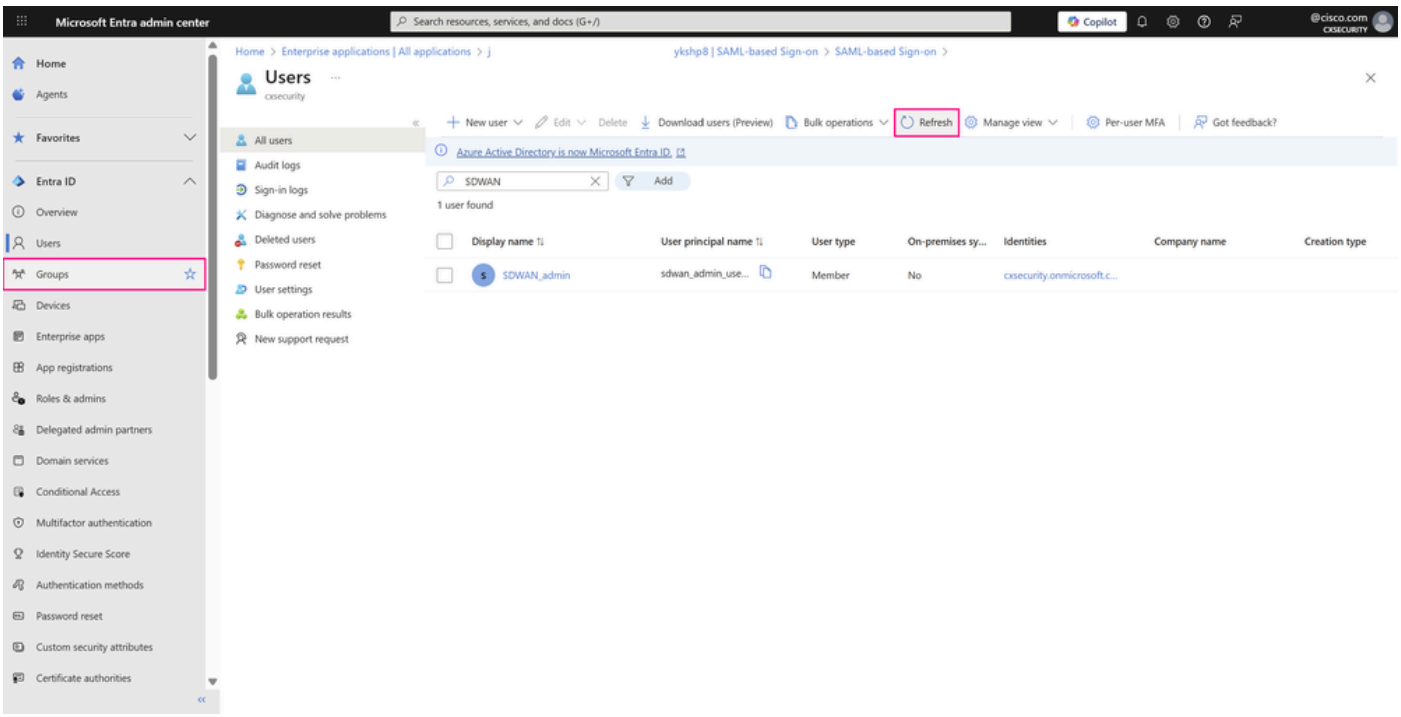
Pagina Creazione utente

- Nella scheda finale vengono visualizzati i dettagli principali del flusso di lavoro di creazione degli utenti. Esaminare i dettagli e fare clic su Crea per completare il processo.



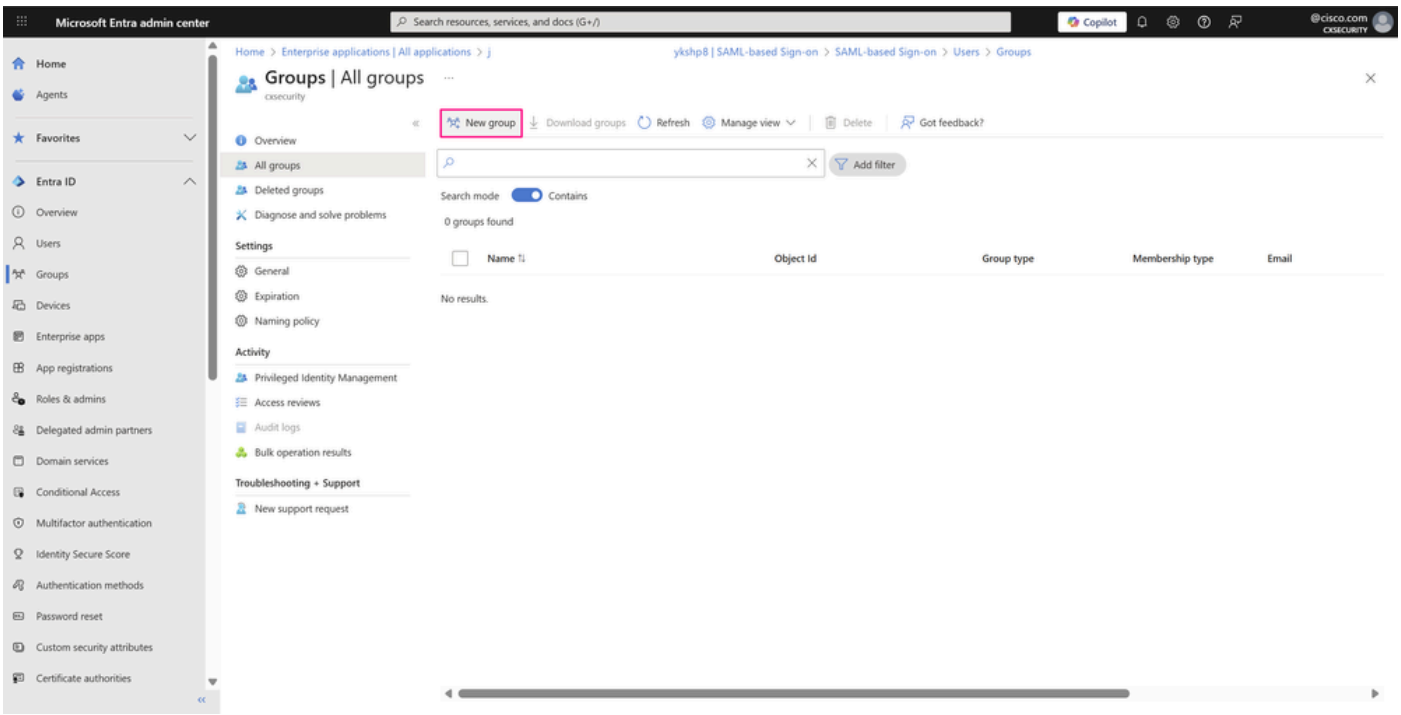
Pagina Creazione utente

- Il nuovo utente viene visualizzato poco dopo. In caso contrario, fare clic su Aggiorna e cercare l'utente utilizzando la barra di ricerca nel servizio. Quindi, passare a Entra ID > Gruppi > Tutti i gruppi per creare il nuovo gruppo.



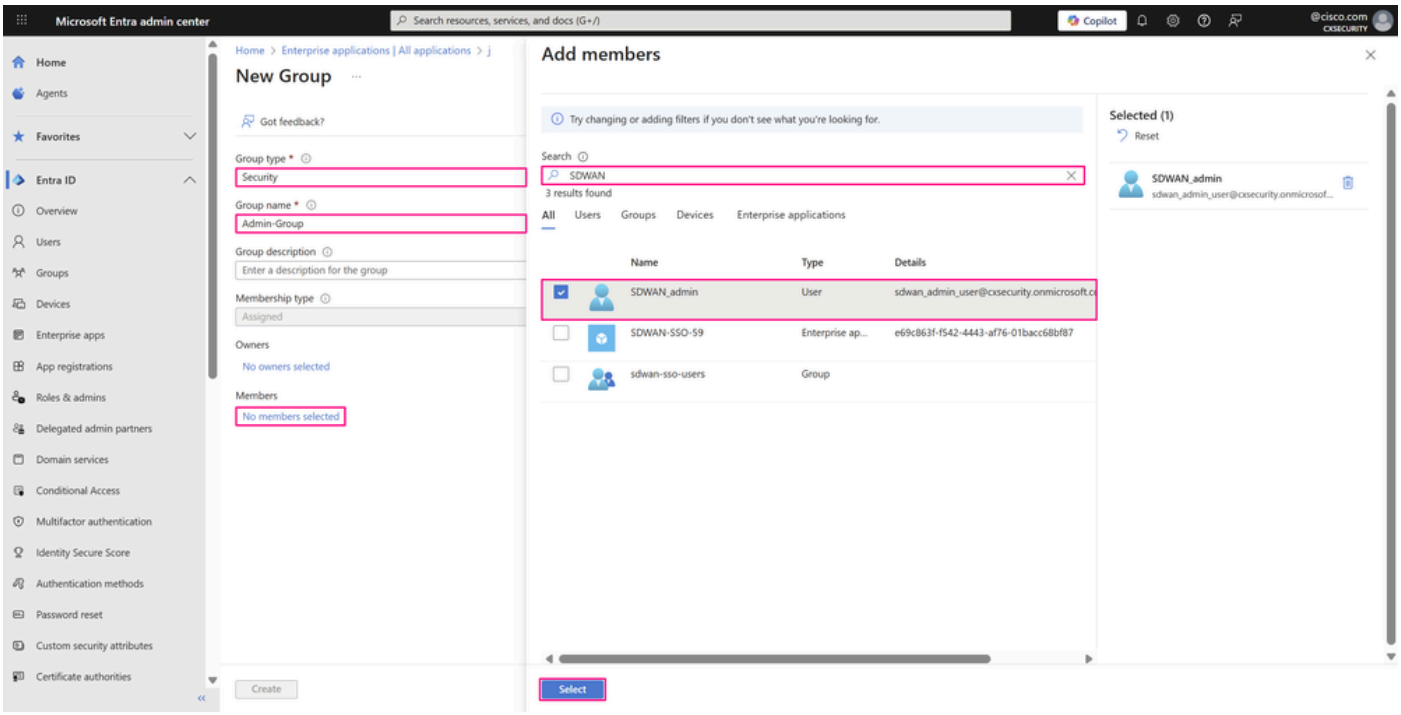
Dashboard utenti

- In questa pagina è possibile gestire i diversi gruppi e le relative autorizzazioni all'interno dell'organizzazione. Fare clic su Nuovo gruppo per creare il gruppo con privilegi di amministratore di rete.



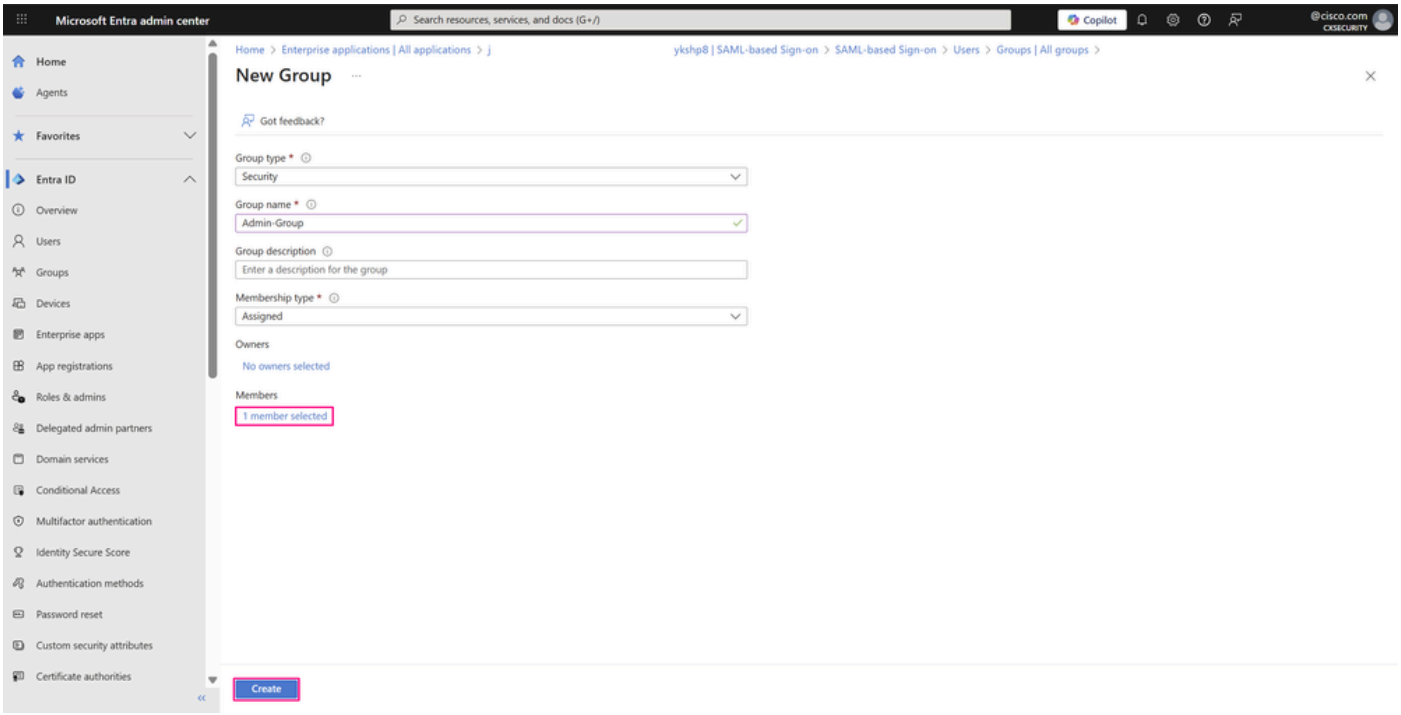
Pagina Tutti i gruppi

- Selezionare un tipo di gruppo dall'elenco a discesa, in questo caso Protezione, poiché è necessario solo l'accesso alle risorse condivise. Immettere il nome del gruppo desiderato che faccia riferimento al ruolo o alle autorizzazioni del gruppo. A questo punto, associare gli utenti al gruppo quando si fa clic sui membri selezionati nel campo Membri.
    - Nella finestra Aggiungi membri, individuare e scegliere gli utenti che si desidera aggiungere, nell'esempio l'utente appena creato, e quindi fare clic su Seleziona.



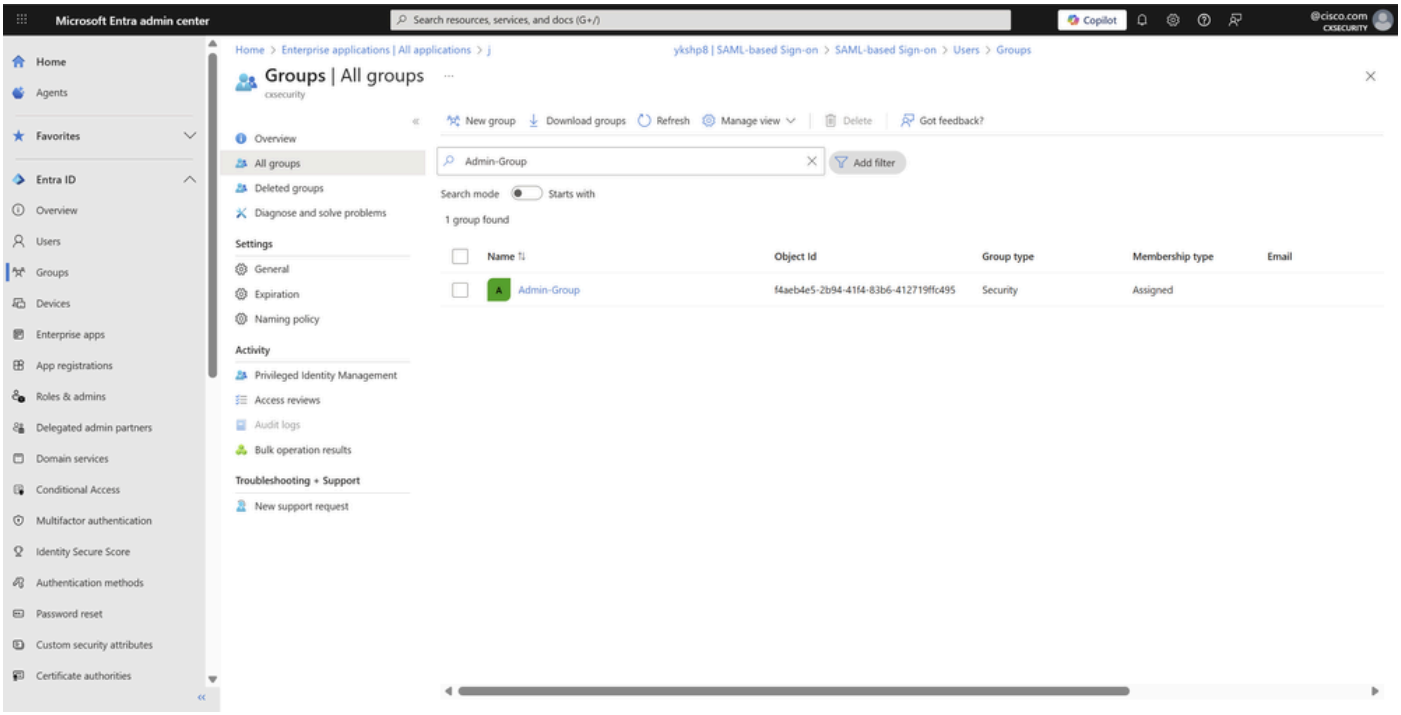
Pagina Creazione gruppo

- Fare clic su Crea per creare il gruppo.



Pagina Creazione gruppo

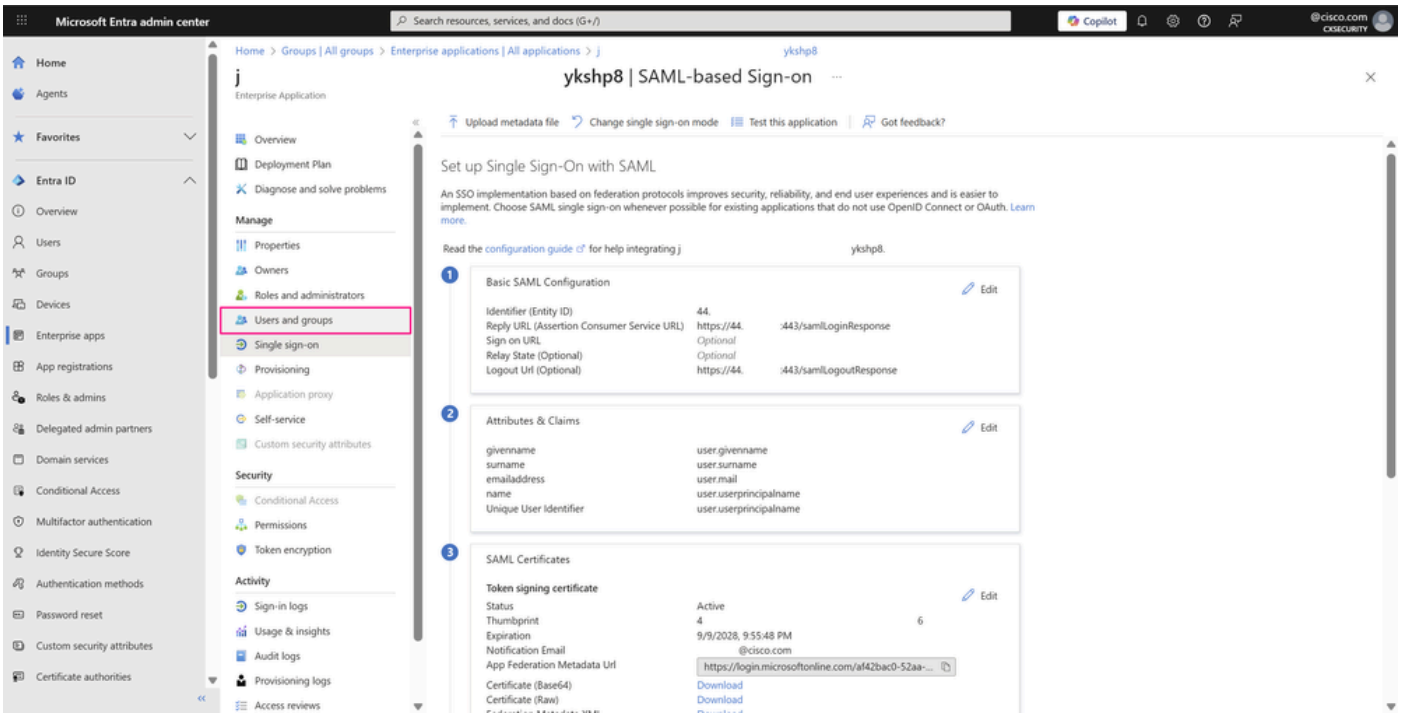
- Il nuovo gruppo viene visualizzato poco dopo. In caso contrario, fare clic su Aggiorna e cercare il nome del gruppo con la barra di ricerca all'interno del servizio. Ripetere i passaggi precedenti per creare un altro utente e aggiungerlo a un altro gruppo di appartenenza per convalidare l'accesso SSO con l'applicazione e uno degli altri gruppi di utenti, ad esempio l'operatore.



Pagina Tutti i gruppi

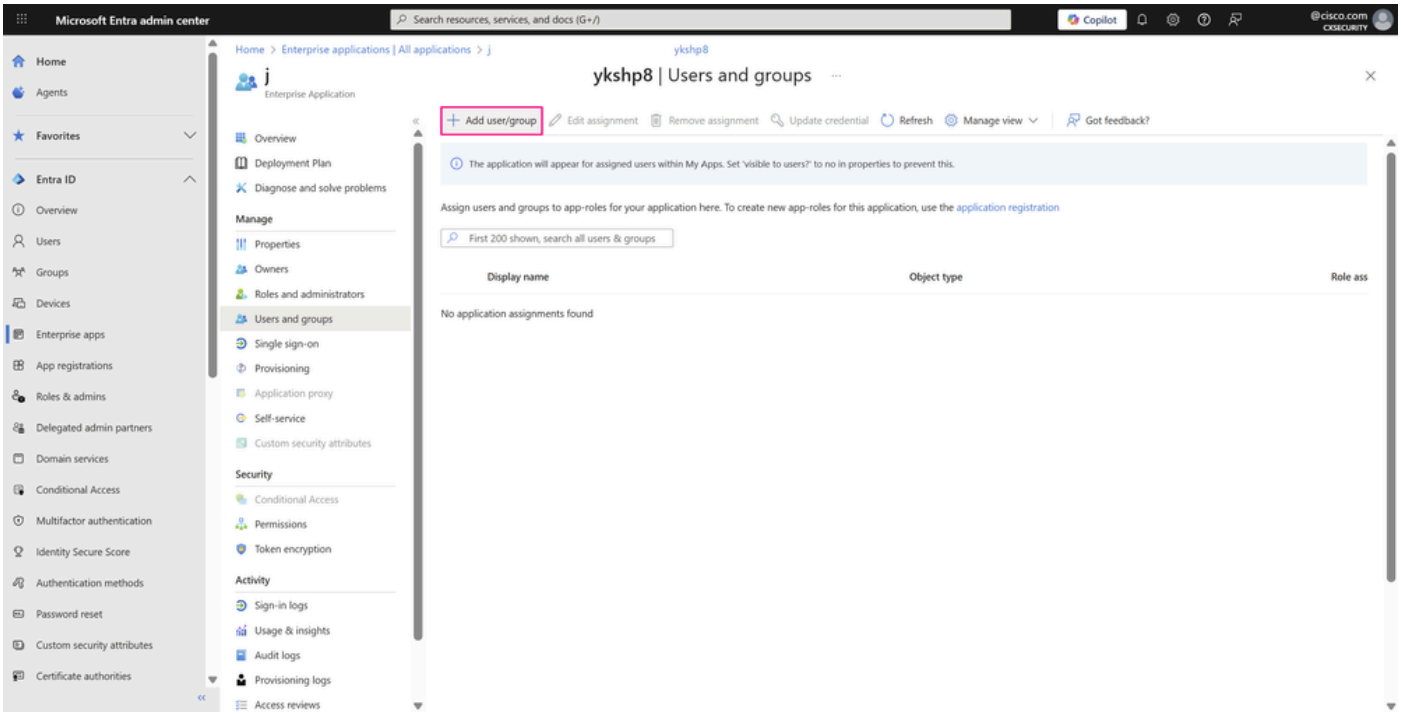
Passaggio 4. Configurare il provisioning del gruppo SAML per l'ID Entra Microsoft

- Per effettuare il provisioning dei gruppi o degli utenti a essi associati nella configurazione SAML, è necessario assegnarli all'applicazione enterprise in modo che dispongano delle autorizzazioni di accesso per l'applicazione, ad esempio Cisco SD-WAN Manager. Tornare a Entra ID > App Enterprise e aprire l'applicazione enterprise. Nella sezione Gestisci del menu a sinistra, fare clic su Utenti e gruppi.



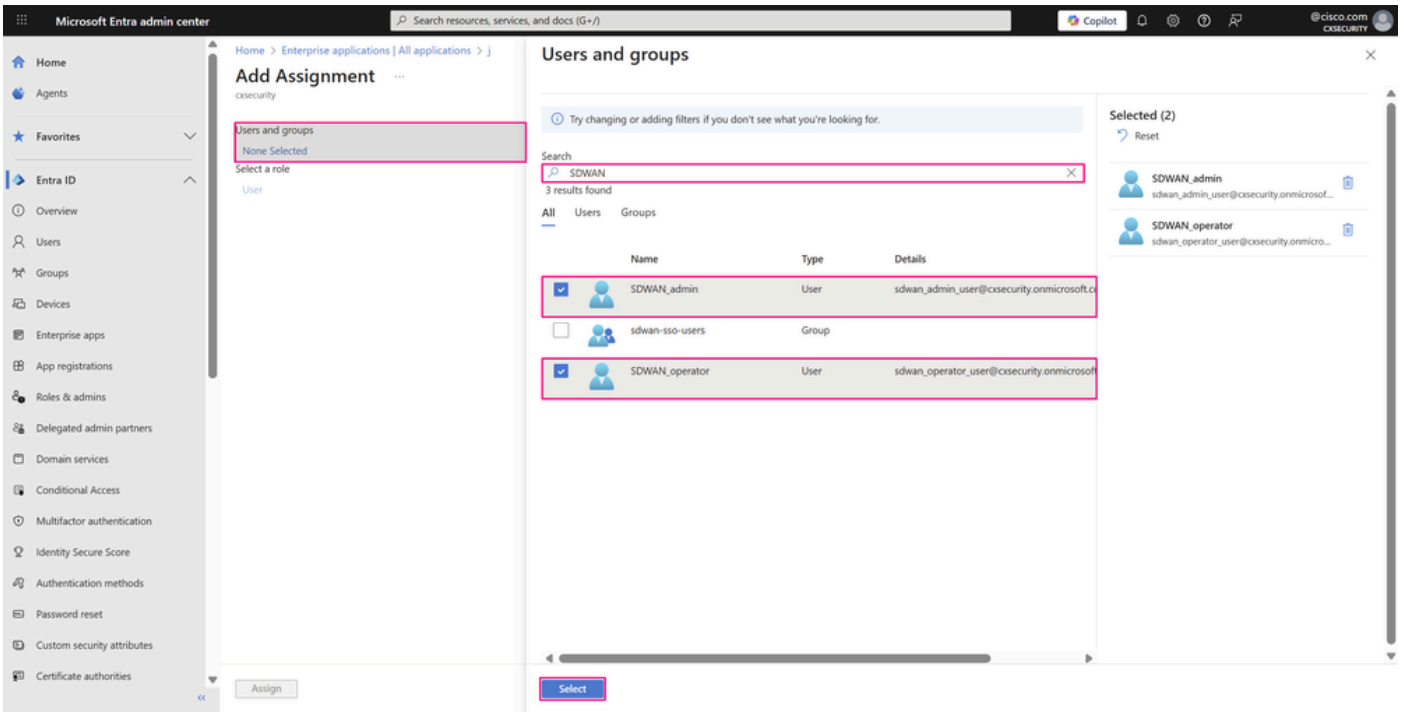
Pagina SSO con configurazione SAML

- Fare quindi clic su Add user/group (Aggiungi utente/gruppo).



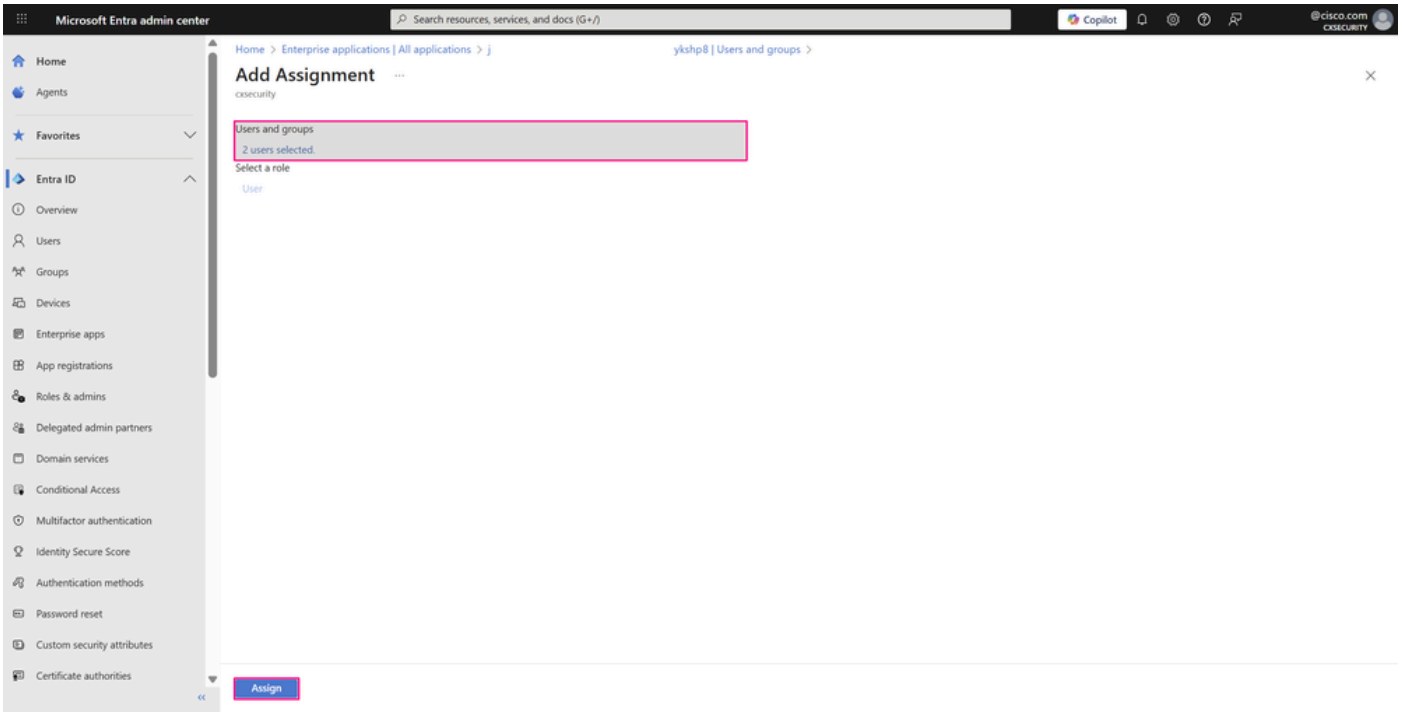
Pagina Utenti e gruppi

- Nel riquadro Aggiungi assegnazione fare clic su Nessuna selezione in campo Utenti e gruppi. Cercare e scegliere l'utente o il gruppo che si desidera assegnare all'applicazione, nell'esempio riportato i due utenti creati nei passaggi precedenti , e quindi fare clic su Seleziona.



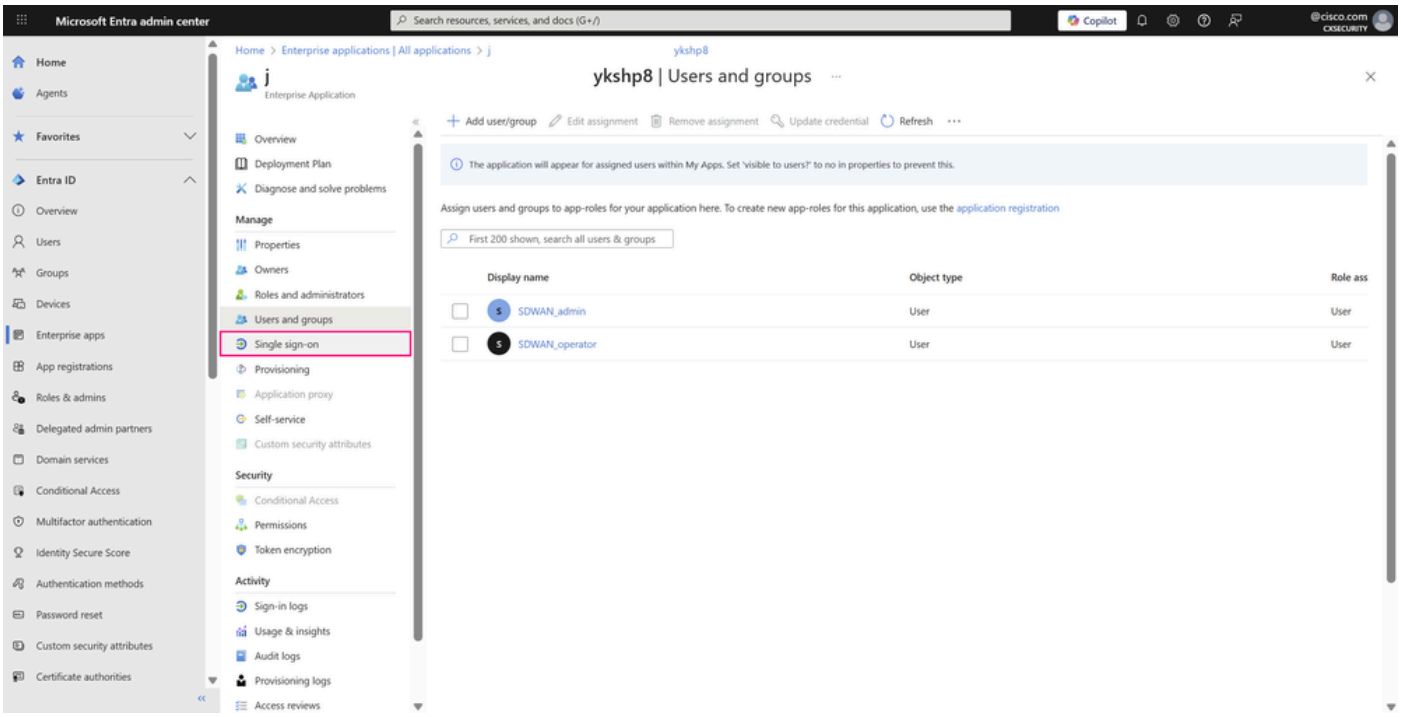
Riquadro assegnazione utenti/gruppi

- Fare clic su Assegna per assegnare l'utente o il gruppo all'applicazione.



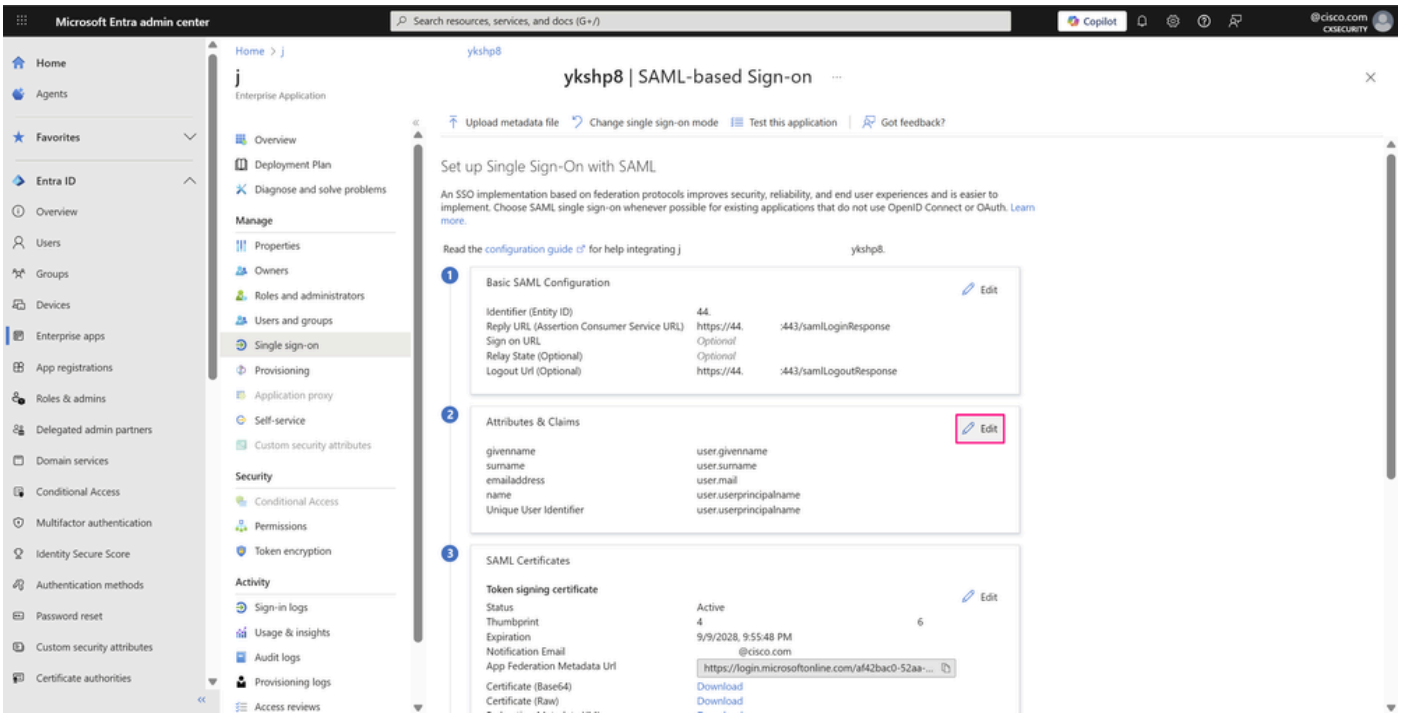
Riquadro assegnazione utenti/gruppi

- Gli utenti assegnati all'applicazione enterprise vengono elencati subito dopo l'assegnazione. Fare clic su Single Sign-on nella sezione Gestisci del menu a sinistra per accedere alla configurazione SAML SSO dell'applicazione e completare la configurazione richiesta rimanente.



Pagina Utenti e gruppi

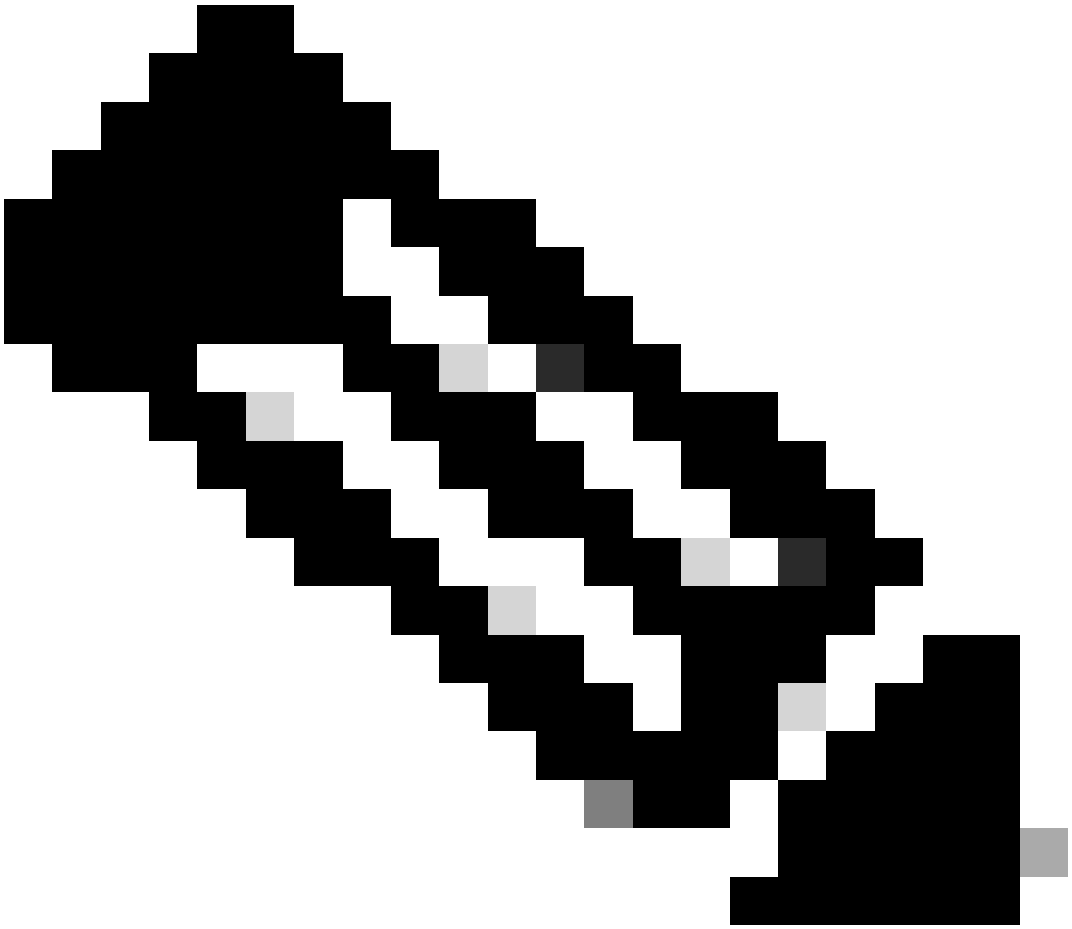
- Nella pagina Imposta Single Sign-On con SAML, in Attributi e attestazioni, fare clic su Modifica.



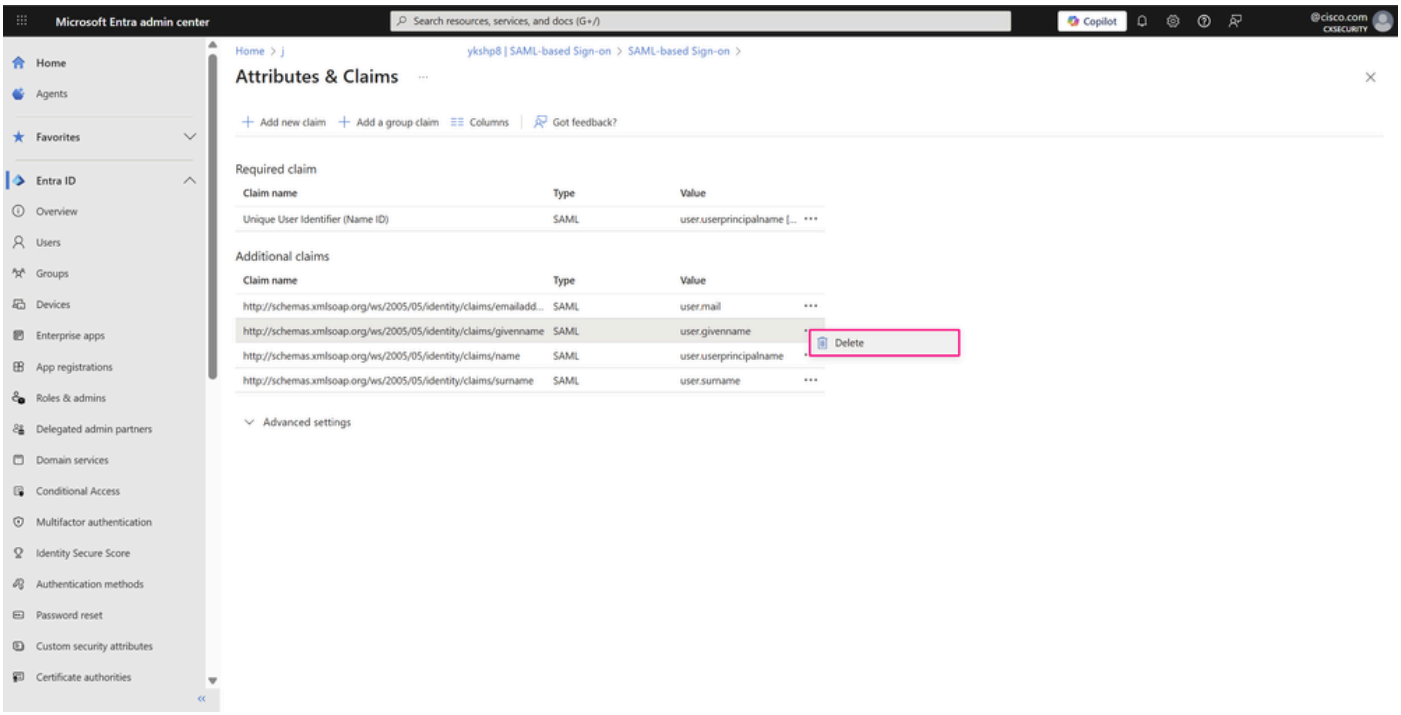
Pagina SSO con configurazione SAML

- Nella pagina Attributi e attestazioni fare clic sull'icona a tre punti e quindi su Elimina per rimuovere l'attestazione con il valore user.givenname e l'attestazione con il valore user.surname, poiché non sono necessarie per questo esempio.Per l'autenticazione SSO di base con l'applicazione sono necessarie solo le attestazioni successive:
    - Indirizzo di posta elettronica dell'utente -user.mail

- Nome dell'entità utente (UPN) dell'utente -user.userprincipalname

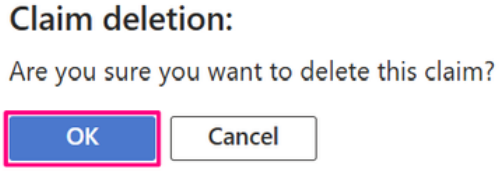


Nota: L'organizzazione può richiedere ulteriori richieste di rimborso in base alle proprie esigenze specifiche.



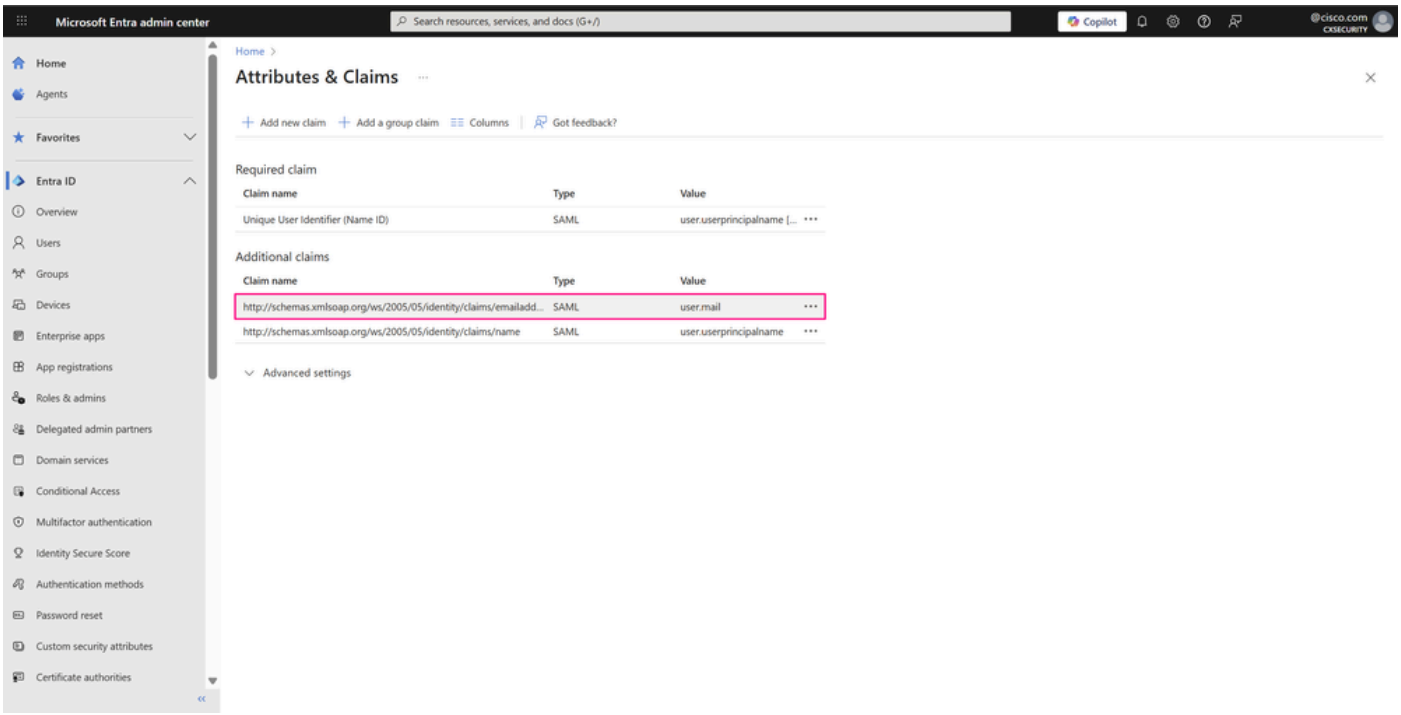
Pagina Attributi e attestazioni

- Nella finestra Eliminazione richiesta di rimborso, fare clic su OK per eliminare la richiesta di rimborso.



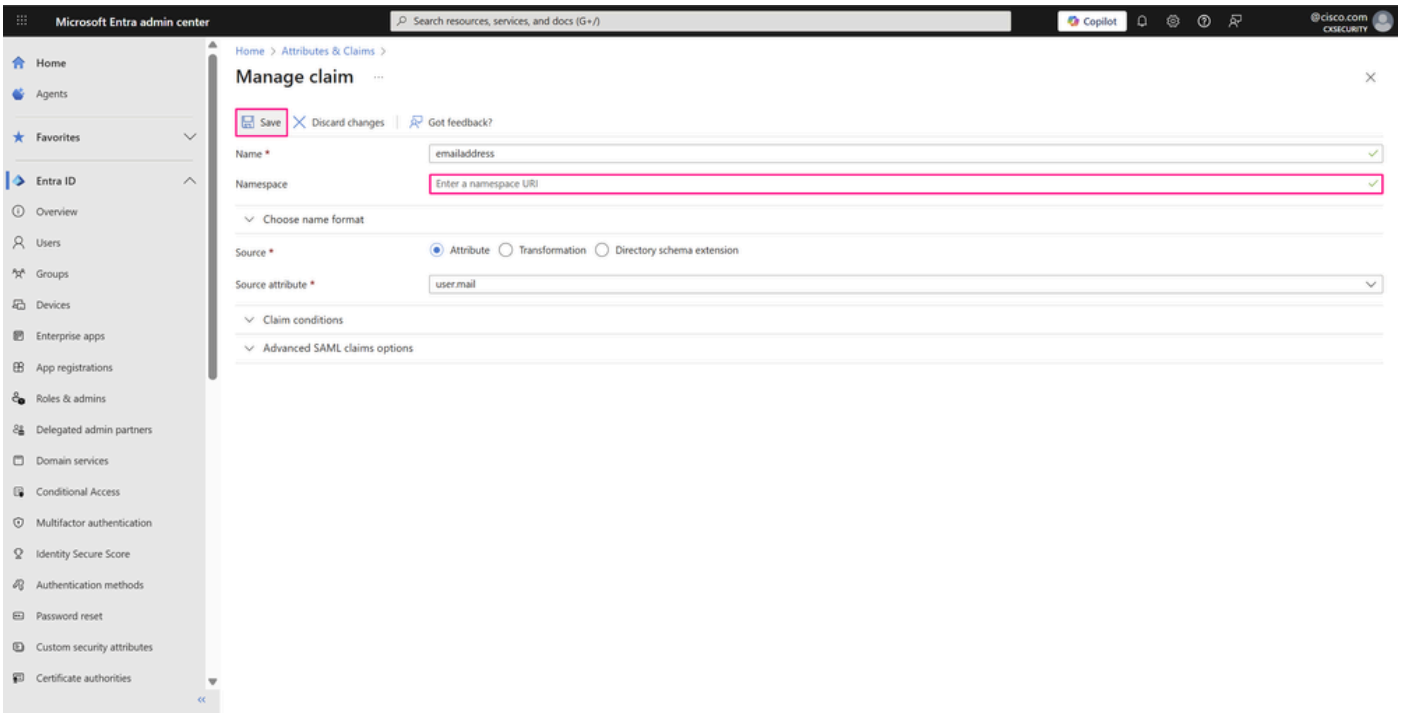
Finestra Eliminazione richiesta di rimborso

- Rimuovere quindi lo spazio dei nomi dal nome dell'attestazione nelle due attestazioni rimanenti, poiché questo campo è facoltativo. Questa modifica consente di visualizzare in questa pagina il nome effettivo di ciascuno di essi per facilitarne l'identificazione. Passare il mouse su ogni attestazione e fare clic su di essa per accedere alle relative impostazioni.



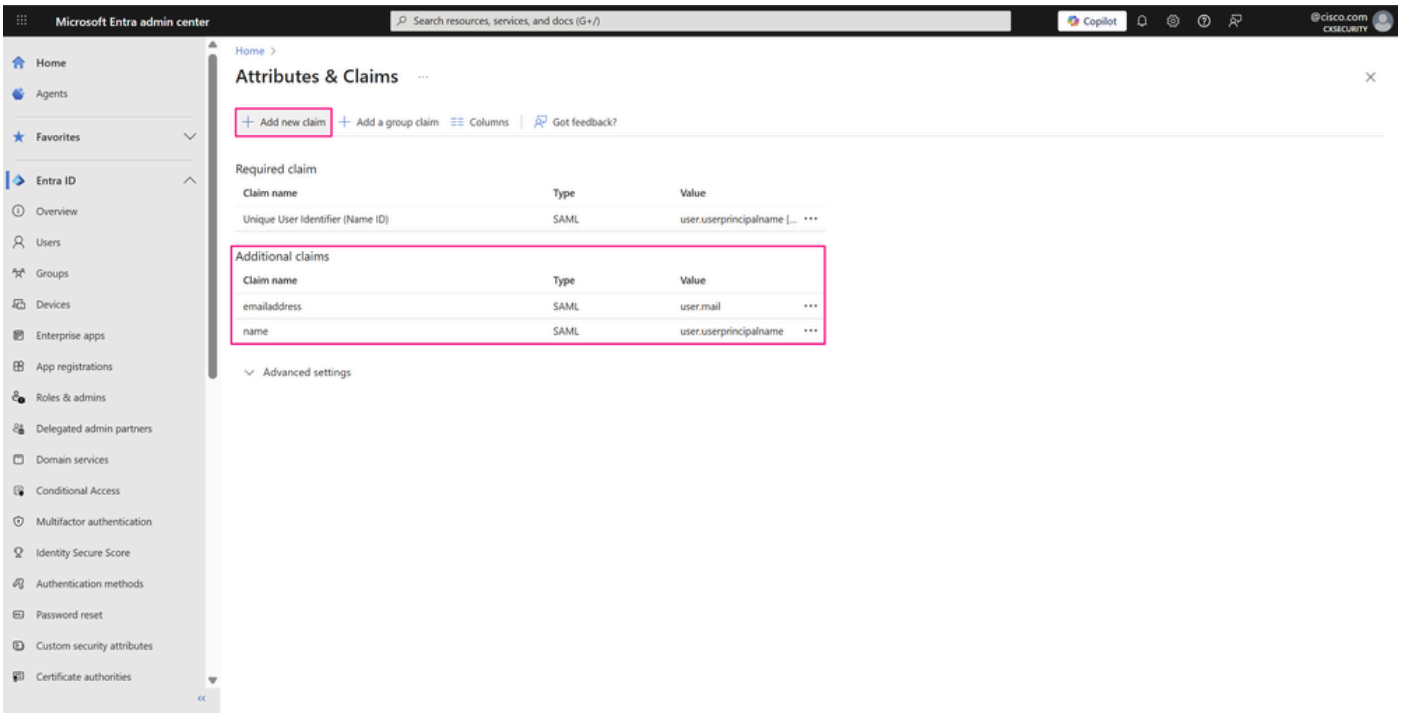
Pagina Attributi e attestazioni

- Nella pagina Gestisci attestazione eliminare il campo Spazio dei nomi e fare clic su Salva per applicare le modifiche.



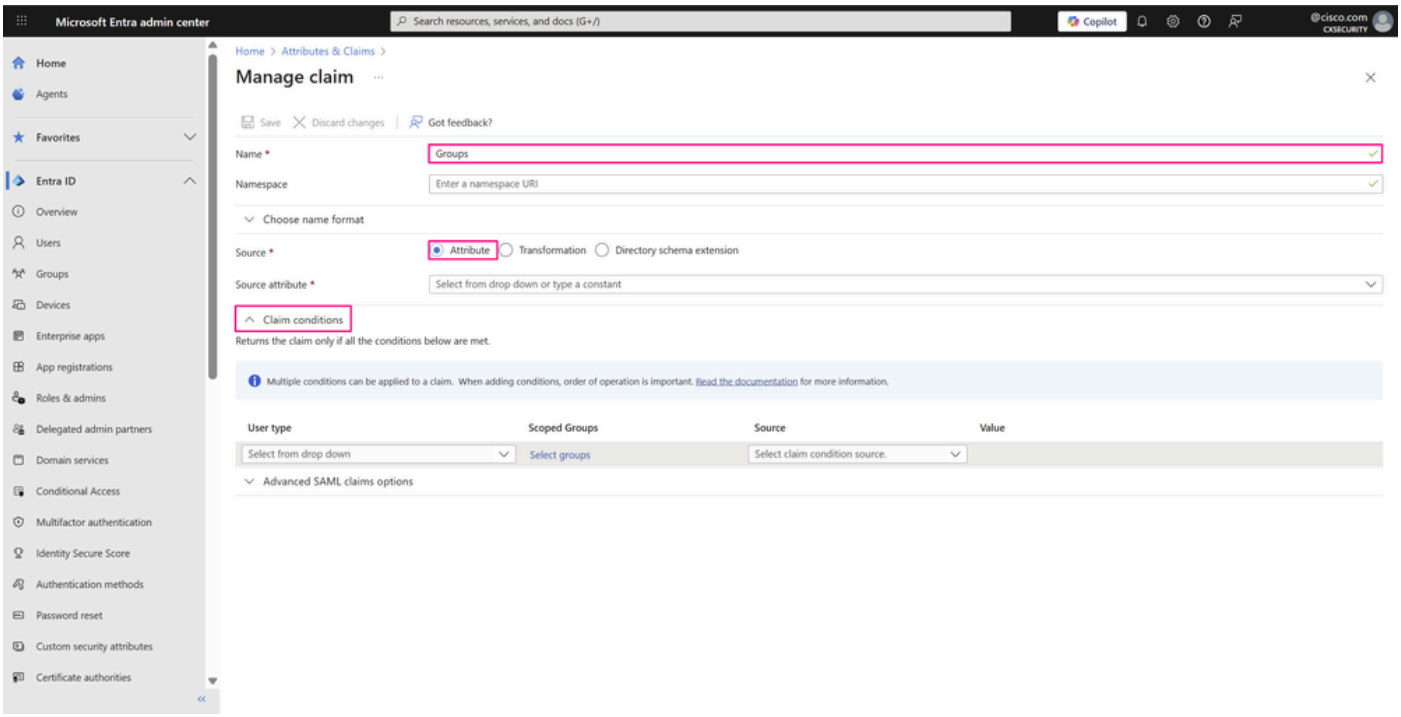
Pagina Gestisci risarcimento

- È ora possibile visualizzare i nomi delle due attestazioni richieste. È tuttavia ancora necessaria un'attestazione aggiuntiva per definire i gruppi a cui appartengono gli utenti e che sono autorizzati ad accedere alle risorse dell'applicazione. A tale scopo, fare clic su Aggiungi nuova attestazione.



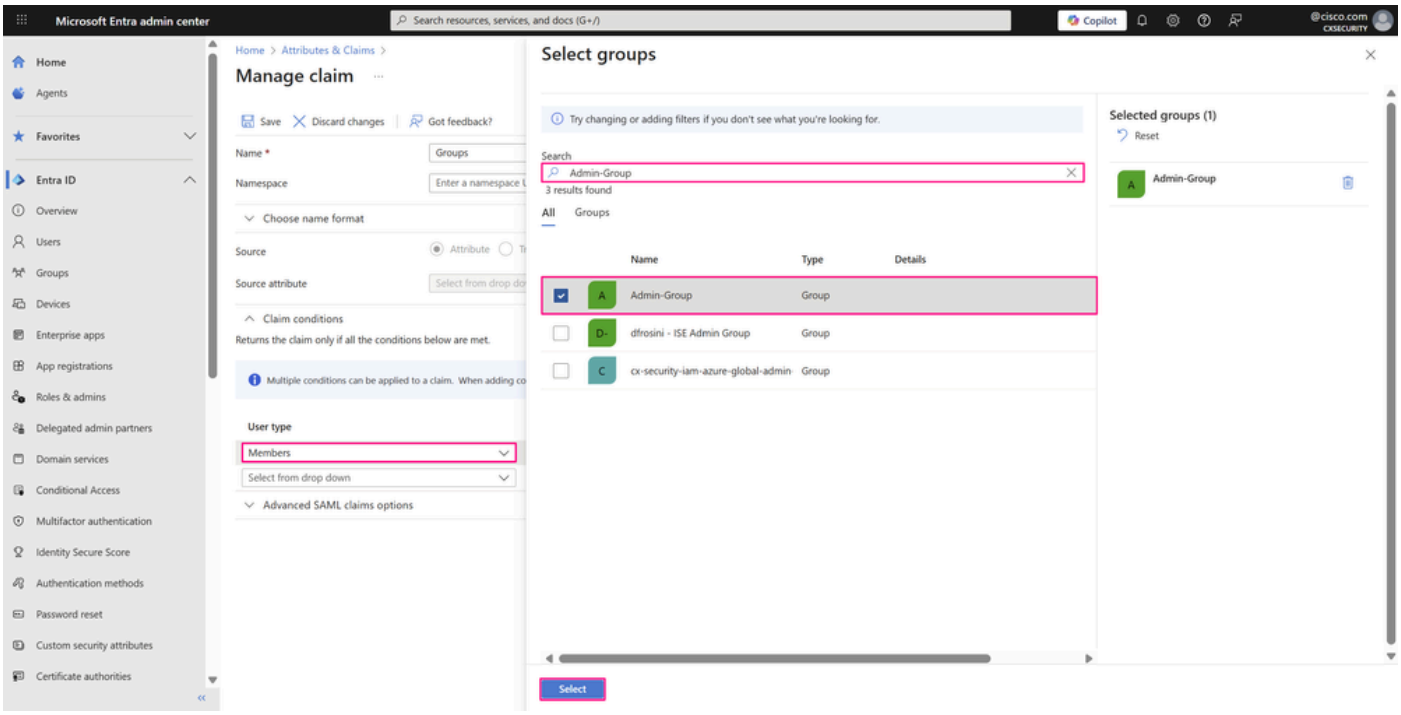
Pagina Attributi e attestazioni

- Immettere un nome per identificare l'attestazione. Accanto a Origine, selezionare Attributo. Quindi fare clic su Condizioni attestazione per espandere le opzioni e configurare più condizioni.



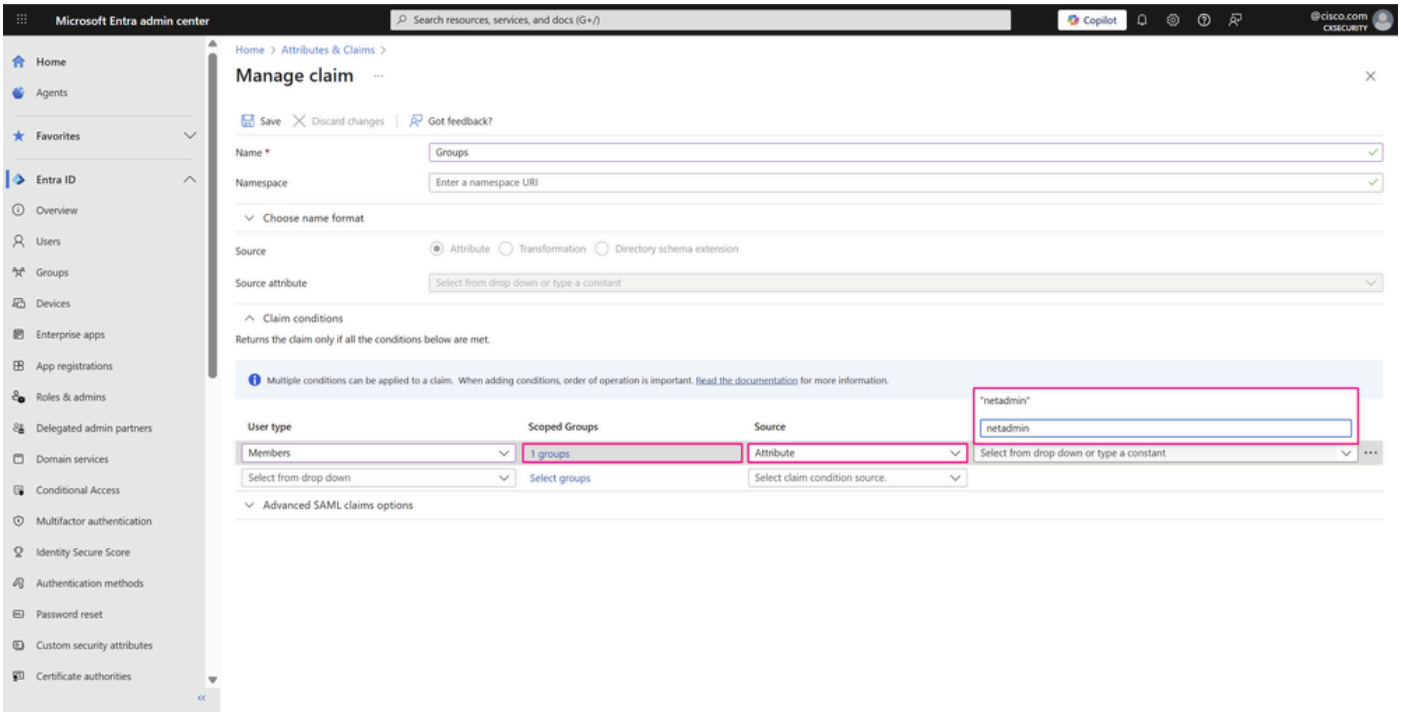
Pagina Gestisci risarcimento

- Nella condizione dell'attestazione, scegliere Membri dall'elenco a discesa Tipo utente e fare clic su Seleziona gruppi per scegliere i gruppi a cui l'utente deve appartenere, quindi fare clic su Seleziona.



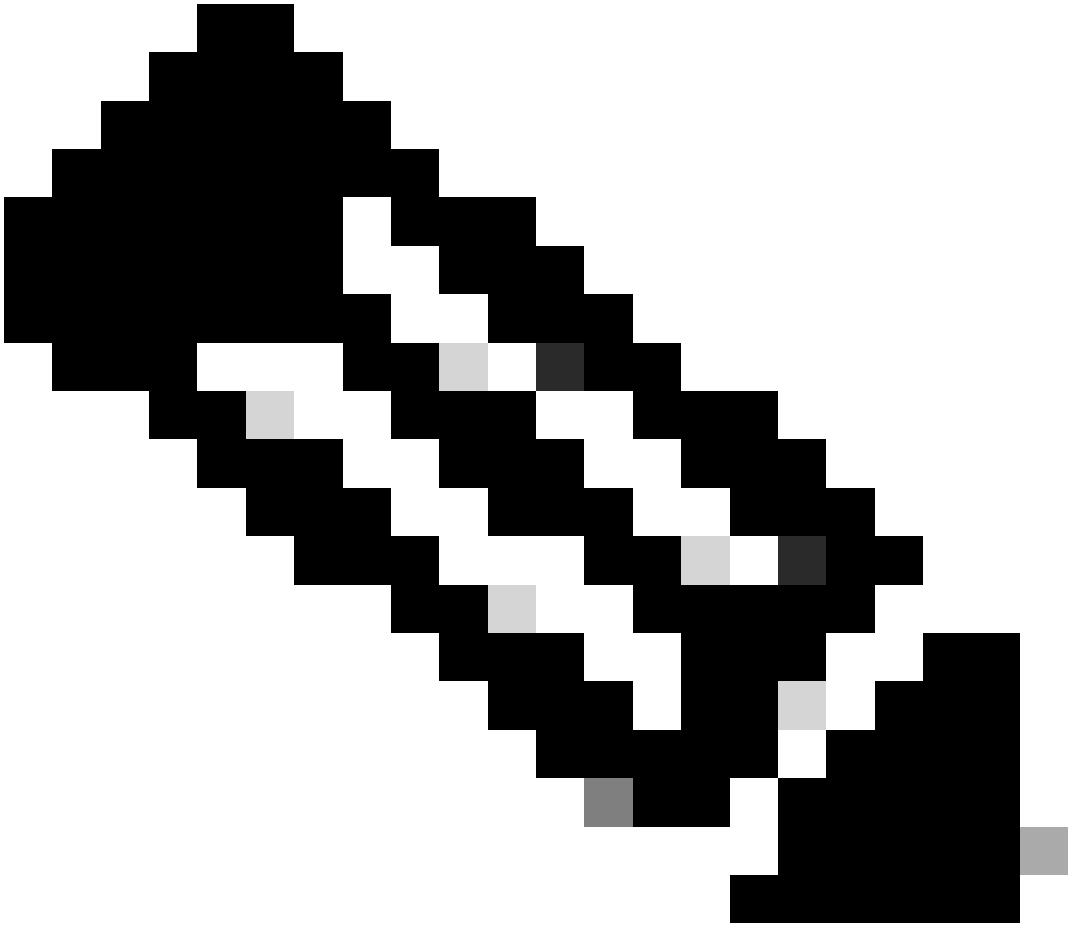
Pagina Gestisci risarcimento

- Scegliere Attributo dall'elenco a discesa Origine in cui l'attestazione recupera il relativo valore. Nel campo Valore, immettere l'attributo personalizzato dell'utente che fa riferimento al gruppo di utenti definito nell'applicazione. In questo esempio, netadmin è uno dei gruppi di utenti standard in Cisco SD-WAN Manager. Immettere il valore dell'attributo senza virgolette e premere Invio.

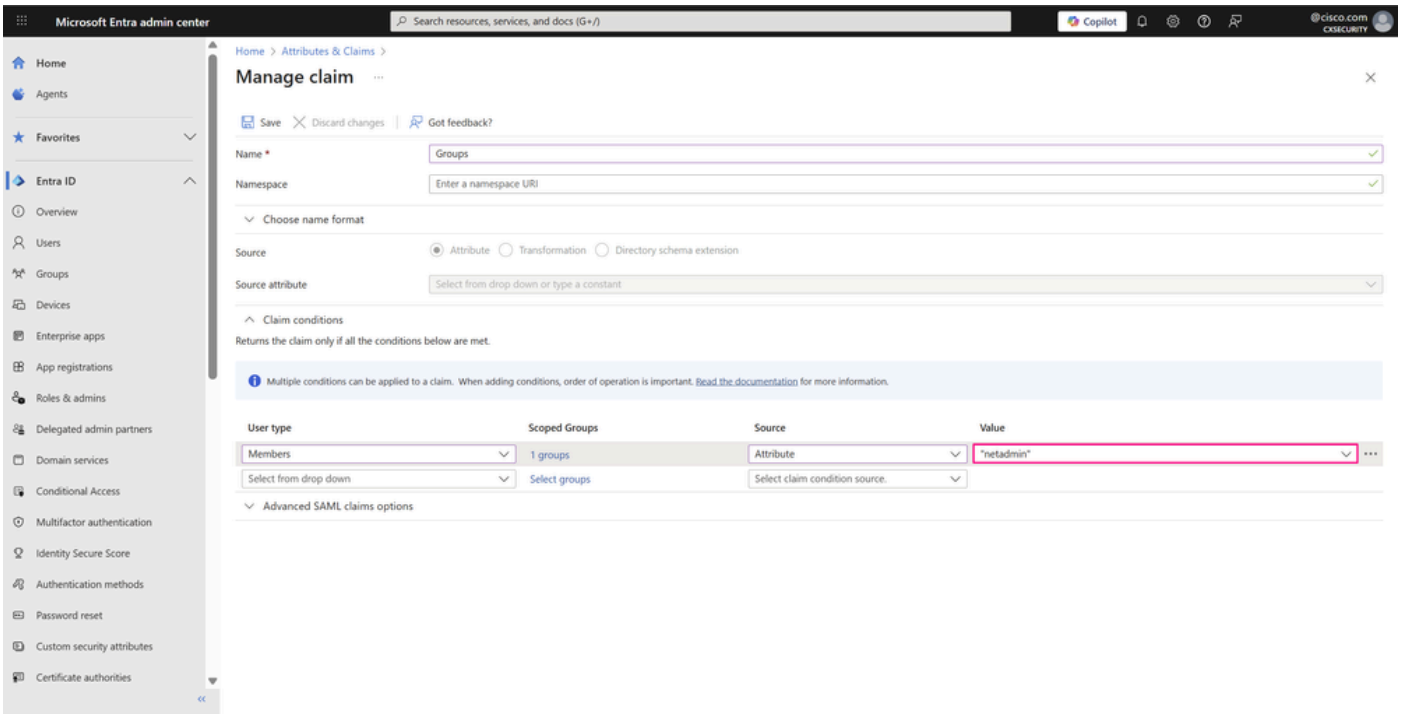


Pagina Gestisci risarcimento

- Immediatamente dopo, il valore dell'attributo viene visualizzato tra virgolette perché Microsoft Entra ID gestisce questo valore come stringa.

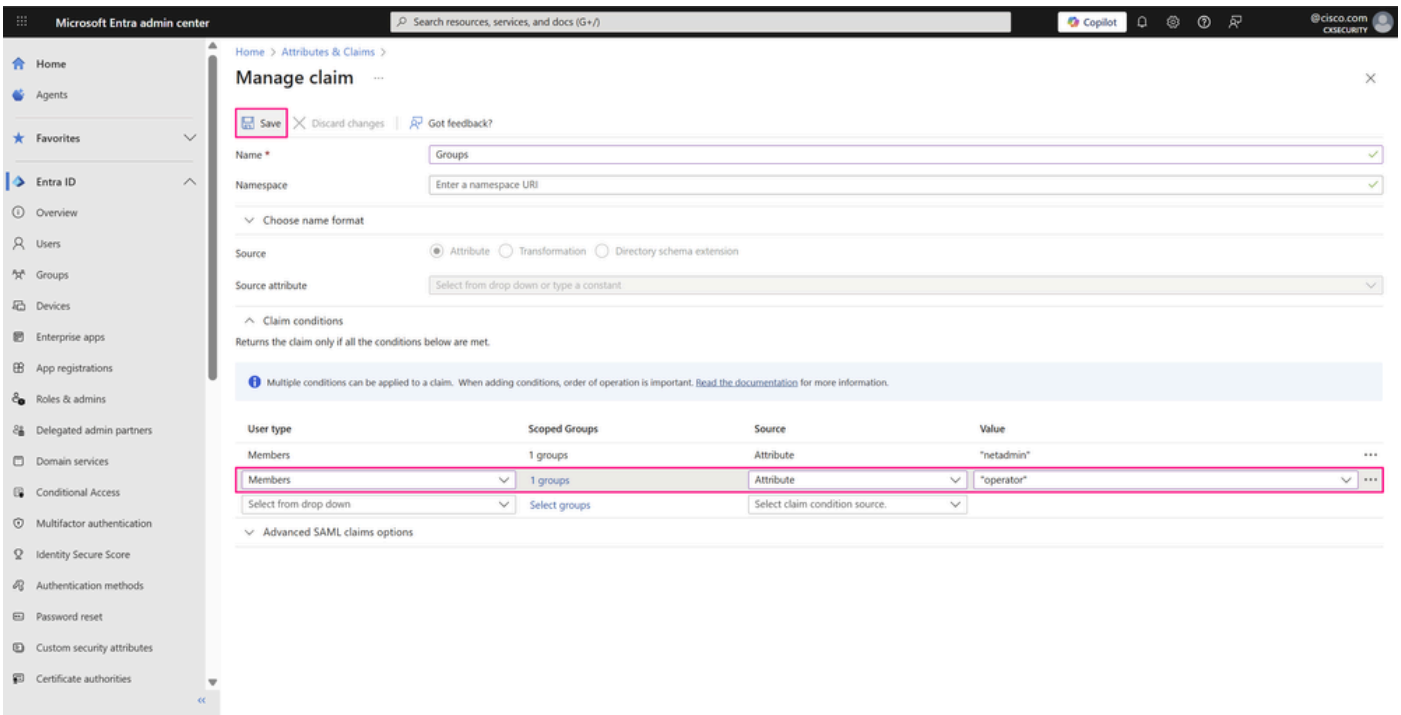


Nota: Questi parametri all'interno delle condizioni attestazione sono molto rilevanti nella configurazione SAML SSO dell'applicazione enterprise, poiché questi attributi personalizzati devono sempre corrispondere ai gruppi di utenti definiti in Cisco SD-WAN Manager. Questa corrispondenza determina i privilegi o le autorizzazioni concesse agli utenti in base al gruppo a cui appartengono in Microsoft Entra ID.



Pagina Gestisci risarcimento

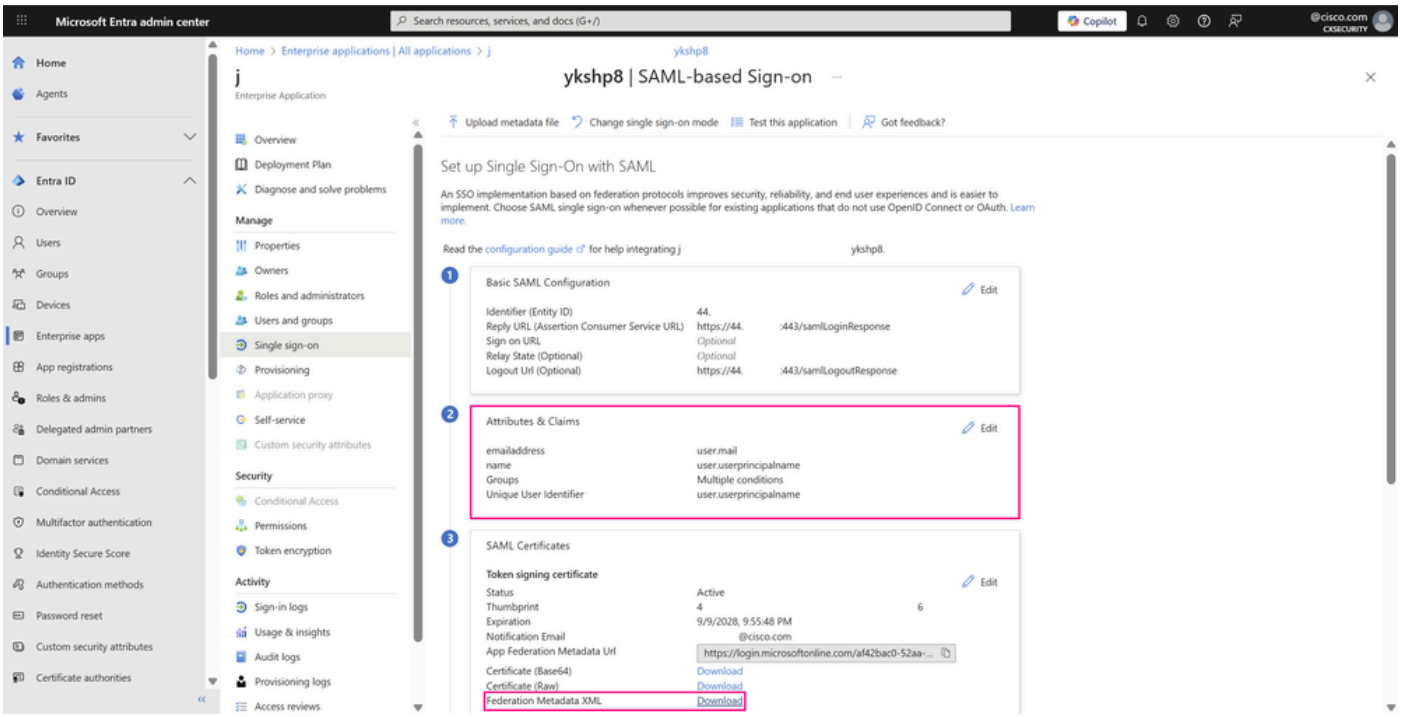
- Ripetere gli stessi passaggi per una seconda condizione di attestazione per il secondo gruppo creato, che esegue il mapping al gruppo di utenti operatore in Cisco SD-WAN Manager. Questo processo è necessario per ogni gruppo con autorizzazioni specifiche che si desidera accedere all'applicazione. È inoltre possibile aggiungere più gruppi all'interno di una singola condizione. Fare clic su Salva per salvare le modifiche.



Pagina Gestisci risarcimento

- Nella pagina Imposta servizio Single Sign-on con SAML, la sezione Attributi e attestazioni mostra le nuove modifiche apportate. Per completare la configurazione nell'ID dei metadati

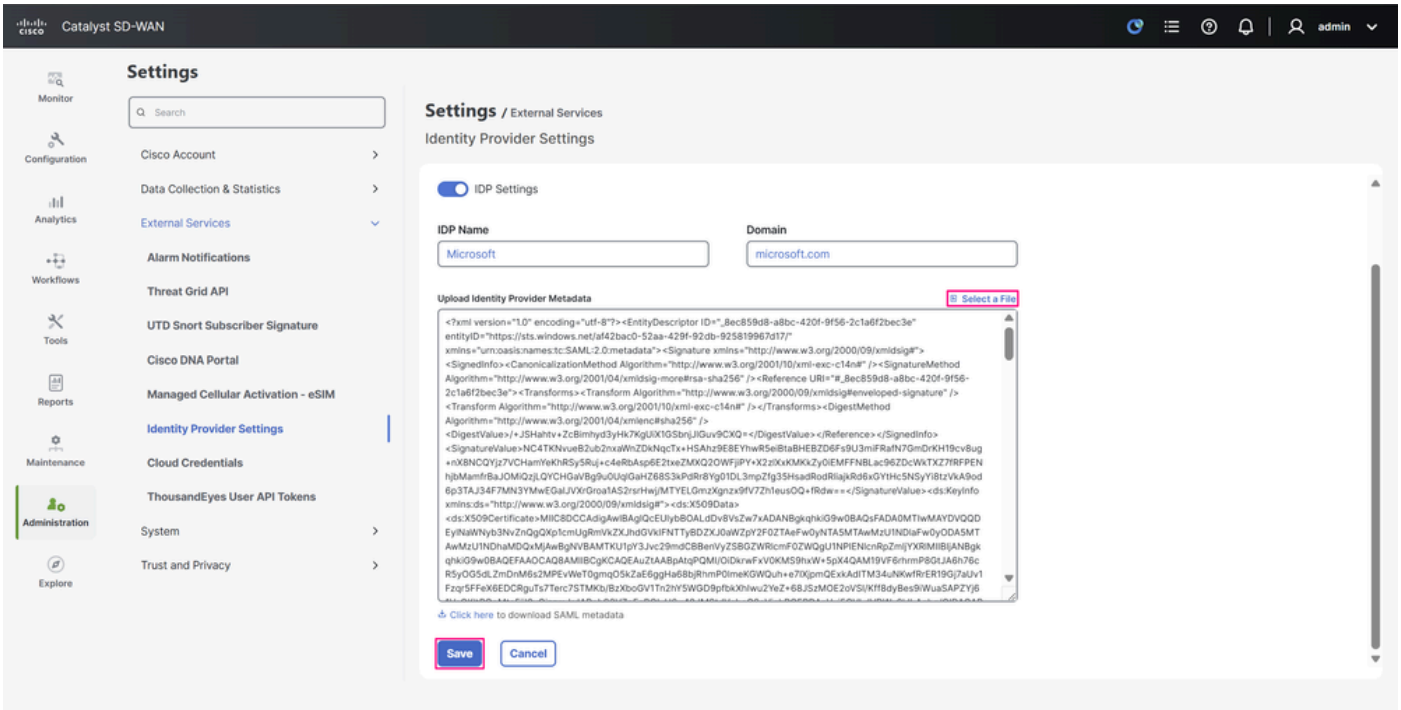
Microsoft, in Certificati SAML fare clic su Scarica accanto a XML metadati federativi per scaricare il file XML che fornisce i servizi di identità all'applicazione.



Pagina SSO con configurazione SAML

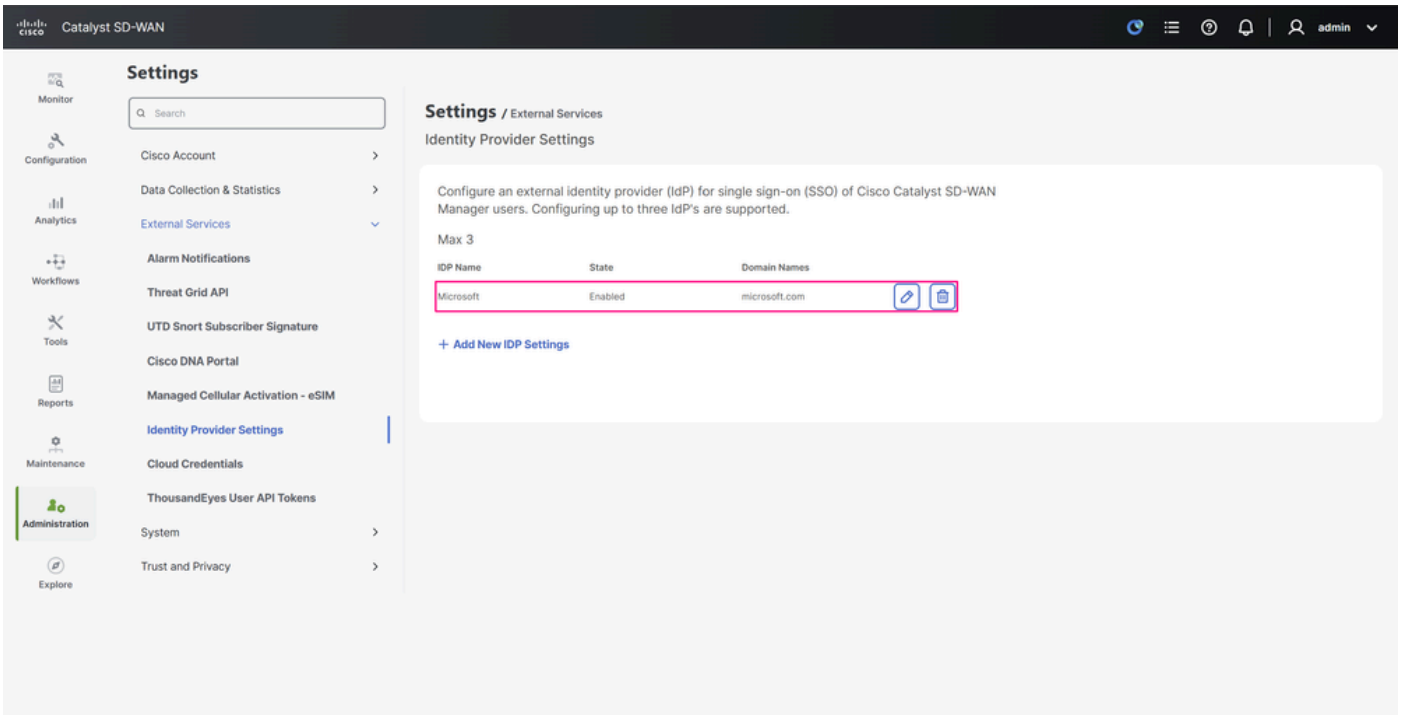
Passaggio 5. Importazione del file di metadati SAML di Microsoft Entra ID in Cisco SD-WAN Manager

- Per caricare i metadati federativi in Cisco SD-WAN Manager, selezionare Amministrazione > Impostazioni > Servizi esterni > Impostazioni provider di identità e fare clic su Seleziona file. Scegliere il file appena scaricato da Microsoft Entra ID, quindi fare clic su Salva.



Pagina Configurazione impostazioni IdP

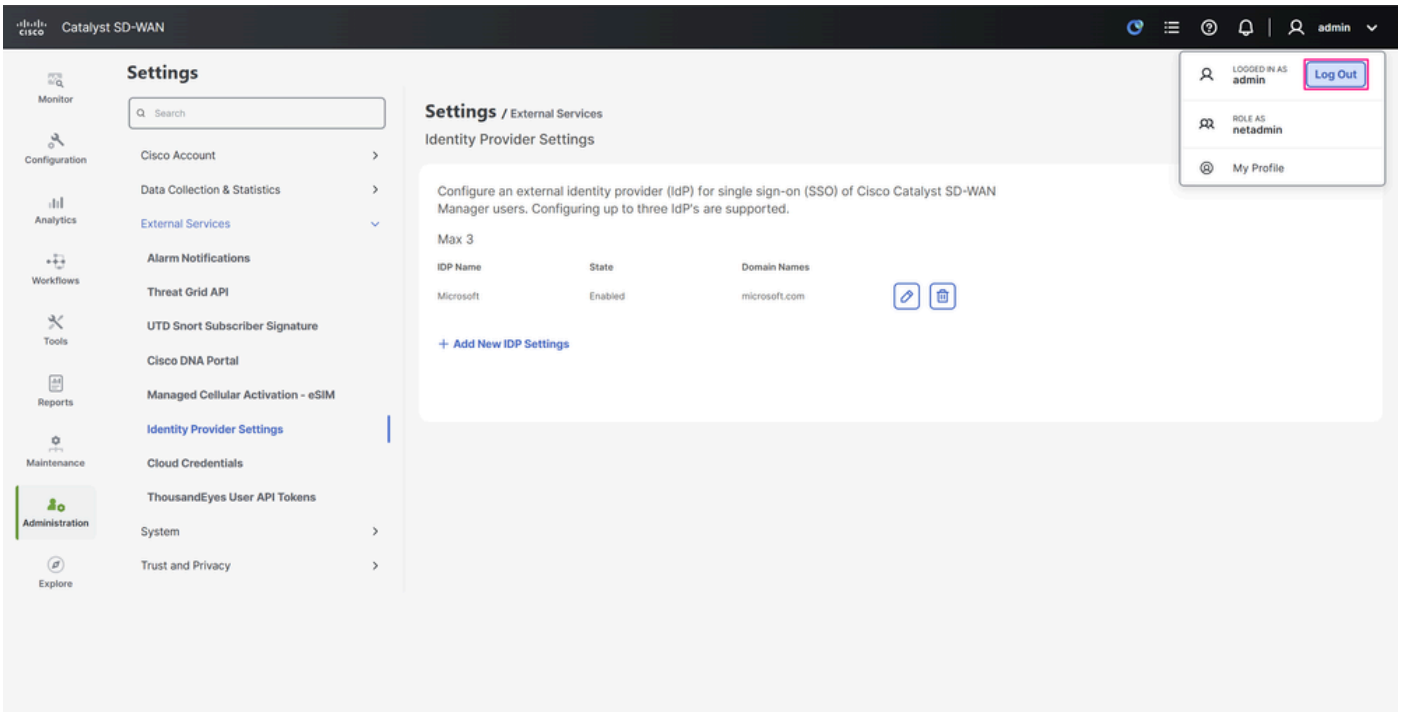
- Le impostazioni e i metadati del provider di identità sono stati salvati.



Pagina Configurazione impostazioni IdP

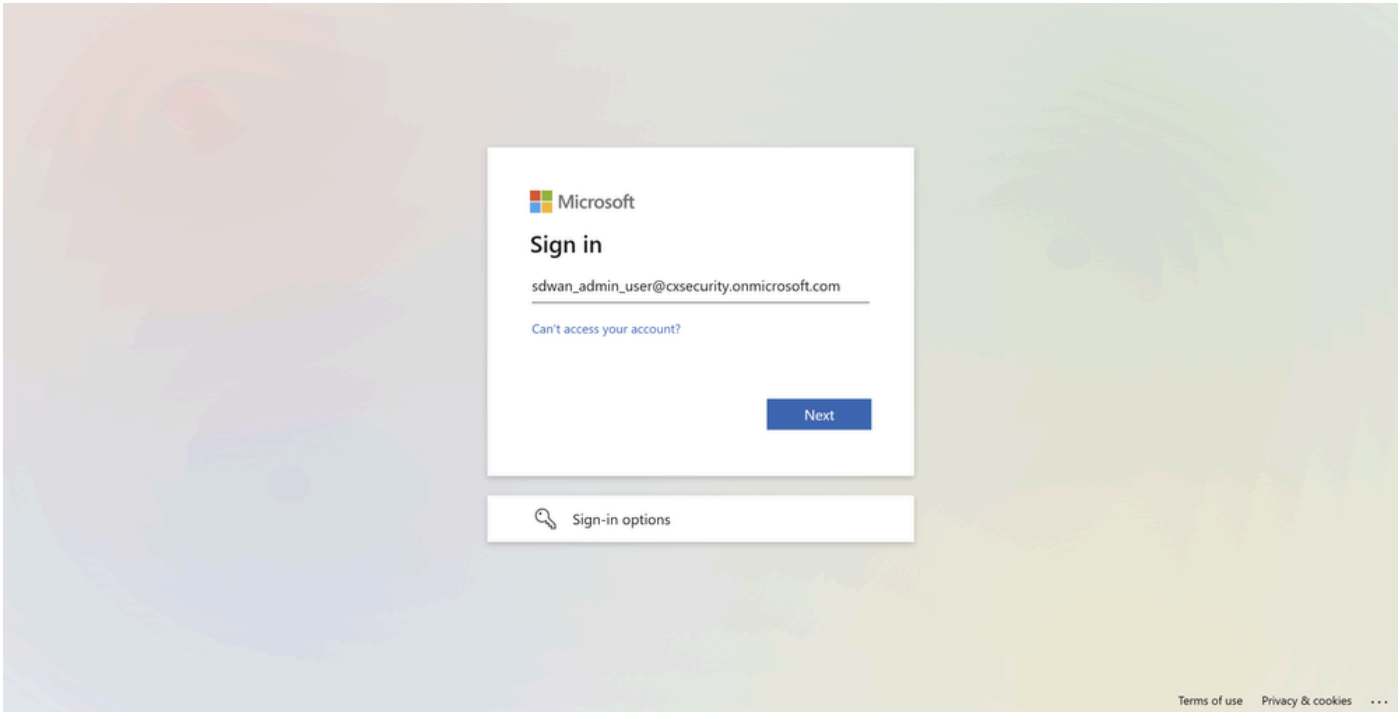
Verifica

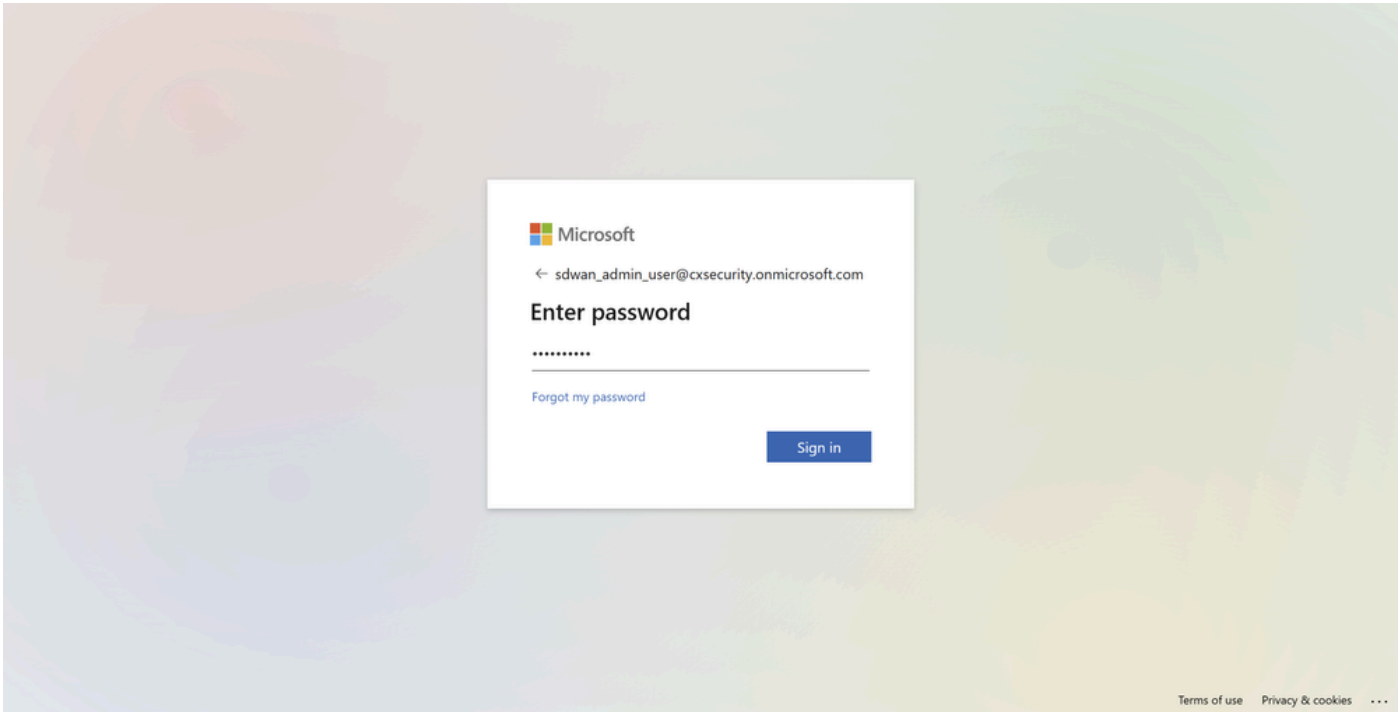
- Fare clic sul nome del profilo nell'angolo superiore destro dell'interfaccia utente per espandere le opzioni, quindi fare clic su Esci per uscire dal portale.



Menu Profilo

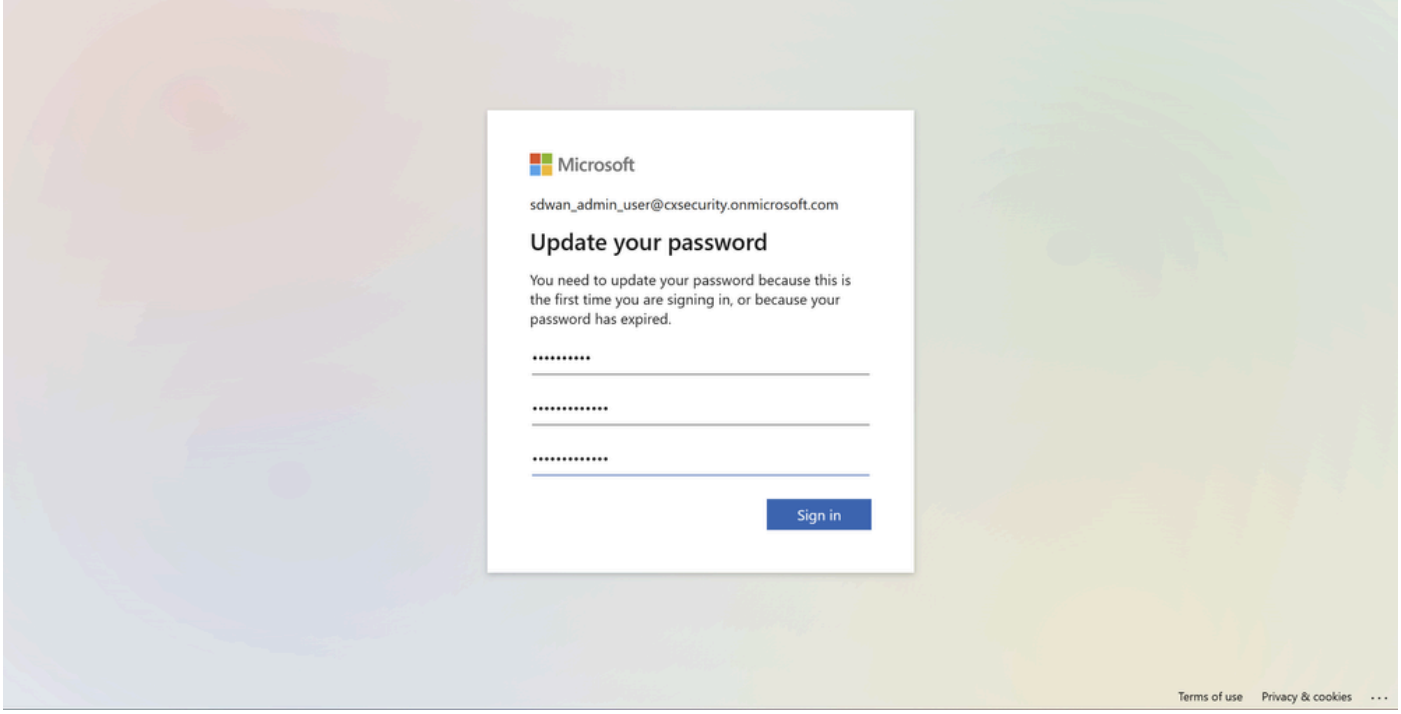
- L'utente viene immediatamente reindirizzato alla schermata di autenticazione Microsoft, in cui accede con le credenziali degli utenti Microsoft Entra ID SSO.





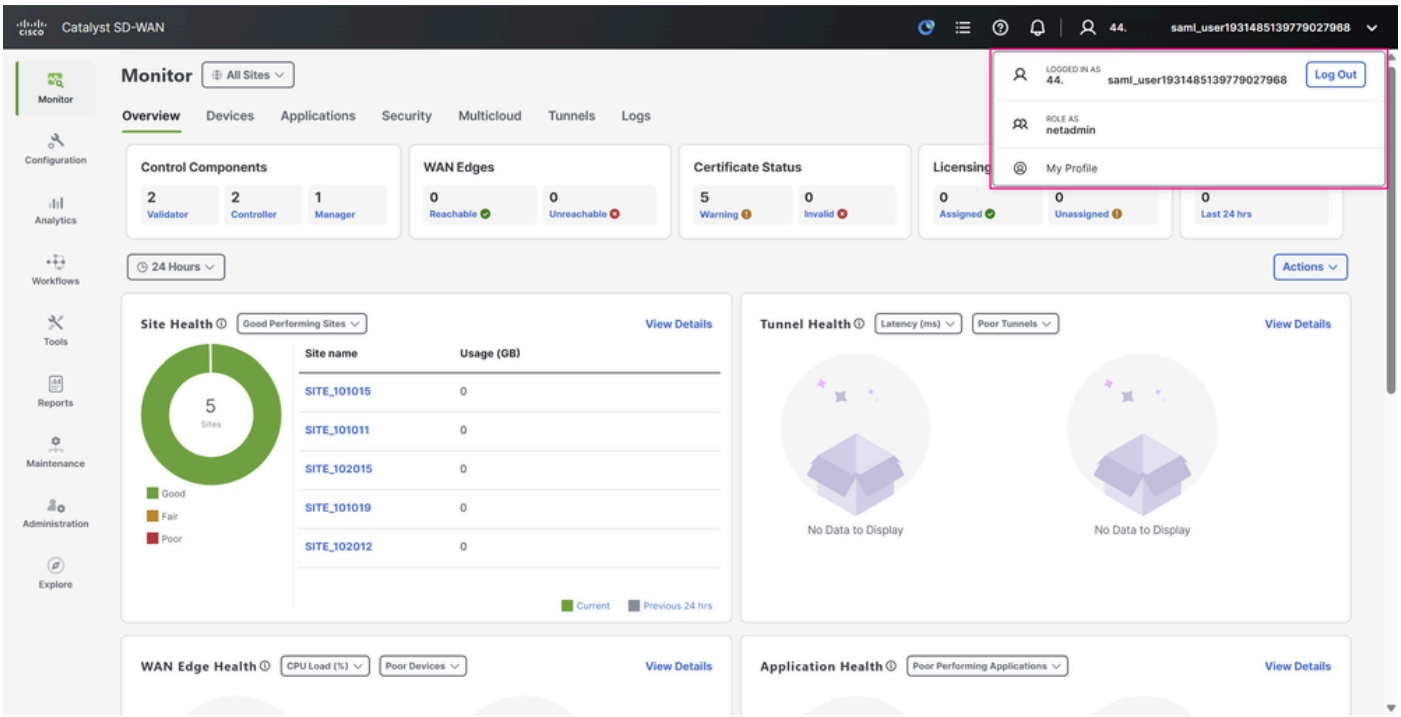
Schermata di accesso Microsoft

- Poiché è la prima volta che l'utente SSO esegue l'accesso, il prompt richiede una modifica della password.



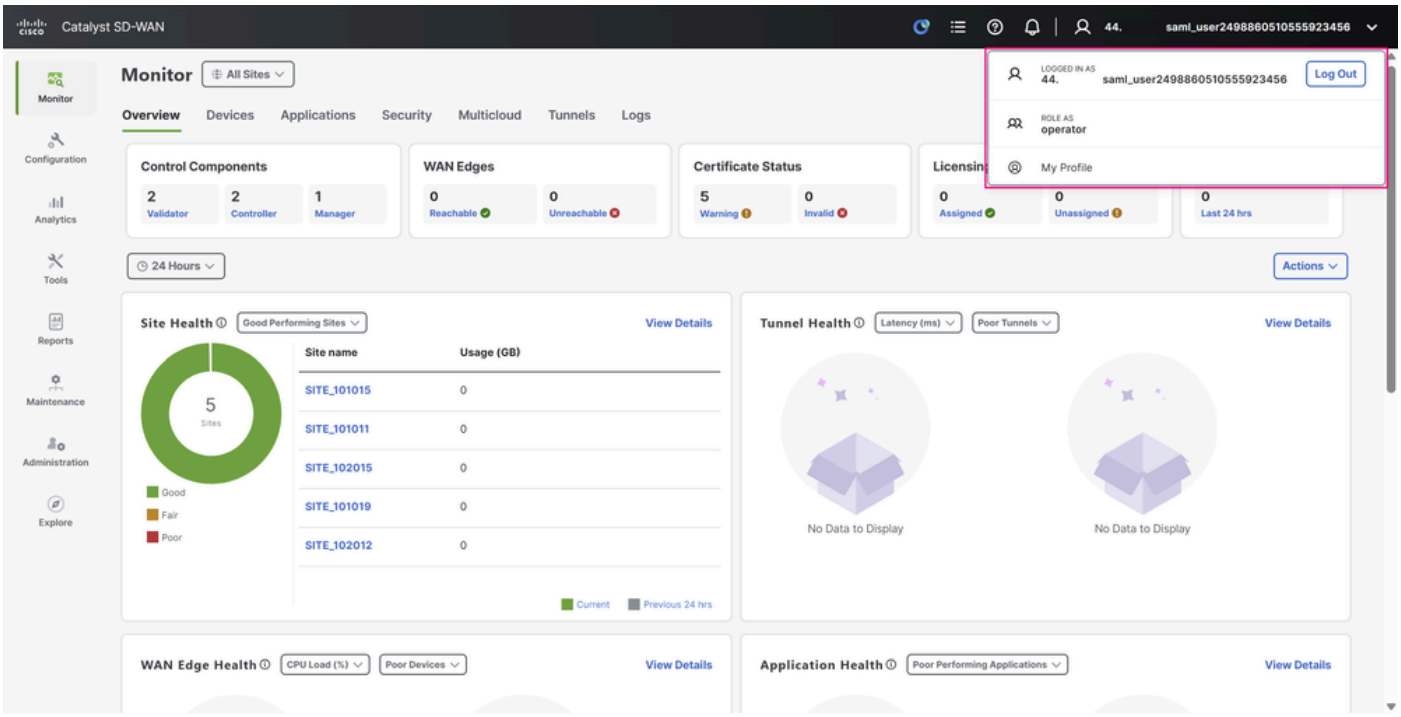
Schermata di accesso Microsoft

- Dopo aver eseguito correttamente l'accesso, espandere nuovamente i dettagli del profilo nell'angolo superiore destro del dashboard e verificare che l'utente sia stato rilevato con un ruolo netadmin, esattamente come configurato in Microsoft Entra ID.



Interfaccia utente di Cisco SD-WAN Manager

- Infine, eseguire lo stesso test di accesso con l'altro utente. Lo stesso comportamento si verifica quando l'utente viene identificato con il ruolo operatore.



Interfaccia utente di Cisco SD-WAN Manager

Informazioni correlate

- Configurazione di Single Sign-On su Cisco IOS XE Catalyst SD-WAN

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).