Configuración de SSO para SD-WAN mediante Microsoft Entra ID

Contenido

Introducción

Este documento describe cómo configurar el inicio de sesión único (SSO) para las redes de área extensa (SD-WAN) definidas por software Cisco Catalyst con Microsoft Entry ID.

Prerequisites

Requirements

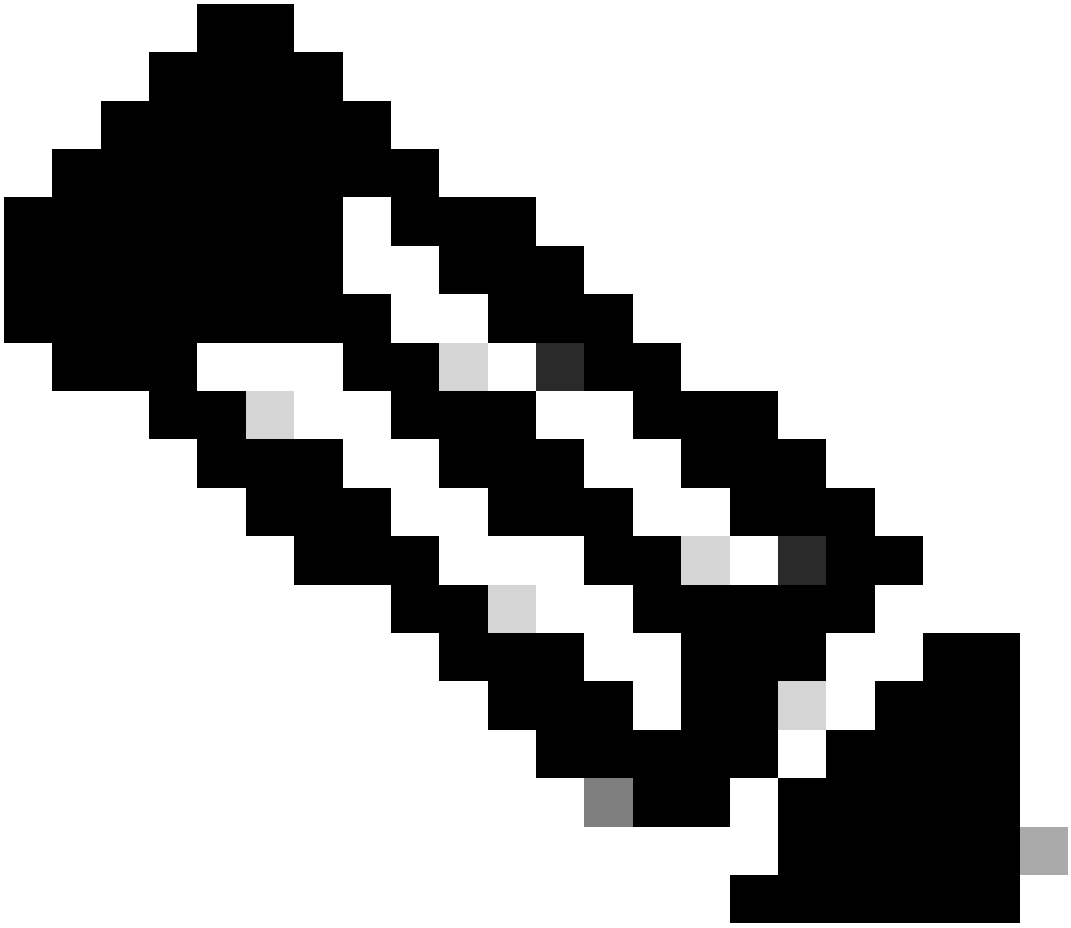
Cisco recomienda que tenga un conocimiento general de estos temas:

- Inicio de Sesión Único
- Solución Cisco Catalyst SD-WAN

Componentes Utilizados

La información de este documento se basa en:

- Cisco Catalyst SD-WAN Manager versión 20.15.3.1
- ID de Microsoft Entra



Nota: La solución anteriormente conocida como Azure Active Directory (Azure AD) ahora se denomina Microsoft Entra ID.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El inicio de sesión único es un método de autenticación que permite a los usuarios acceder de forma segura a varias aplicaciones o sitios web independientes mediante un único conjunto de credenciales. Con SSO, los usuarios ya no necesitan iniciar sesión por separado en cada aplicación; una vez autenticados, pueden acceder sin problemas a todos los recursos permitidos.

Una forma común de implementar SSO es a través de la federación, que establece la confianza entre un proveedor de identidad (IdP) y un proveedor de servicios (SP) mediante protocolos como

SAML 2.0, WS-Federation u OpenID Connect. La federación mejora la seguridad, la fiabilidad y la experiencia del usuario al centralizar la autenticación.

Microsoft Entra ID es un proveedor de identidad basado en la nube ampliamente utilizado que admite estos protocolos de federación. En una configuración de SSO con Cisco Catalyst SD-WAN, Microsoft Entra ID actúa como el IdP, y Cisco SD-WAN Manager actúa como el proveedor de servicios.

La integración funciona de la siguiente manera:

1. Un administrador de red intenta iniciar sesión en el administrador SD-WAN de Cisco.
2. Cisco SD-WAN Manager envía una solicitud de autenticación a Microsoft Entra ID.
3. Microsoft Entra ID solicita al administrador que se autentique con su cuenta Entra ID (Microsoft).
4. Una vez validadas las credenciales, Microsoft Entra ID envía una respuesta segura al Cisco SD-WAN Manager para confirmar la autenticación.
5. Cisco SD-WAN Manager concede acceso sin necesidad de credenciales independientes.

En este modelo:

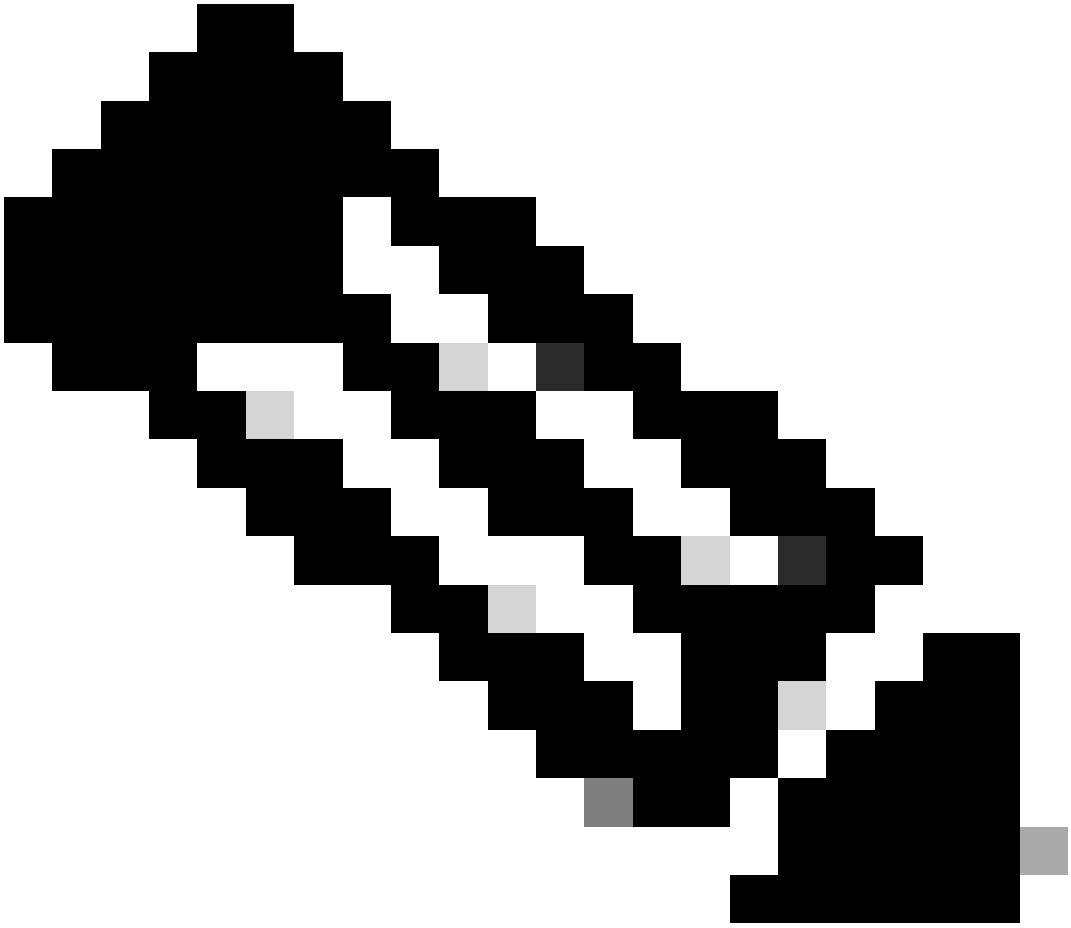
- Proveedor de identidad (IdP): almacena los datos del usuario y valida las credenciales (por ejemplo, Microsoft Entra ID, Okta, PingID, ADFS).
- Proveedor de servicios: aloja la aplicación a la que se desea acceder (por ejemplo, Cisco SD-WAN Manager).
- Usuarios - Tienen una cuenta en el directorio IdP y están autorizados para acceder al proveedor de servicios.

Cisco Catalyst SD-WAN es compatible con cualquier IdP compatible con SAML 2.0 cuando se configura de acuerdo con los estándares del sector.

Ventajas del uso del inicio de sesión único

- Centraliza la administración de credenciales a través del proveedor de identidad.
- Fortalece la seguridad de autenticación al eliminar múltiples contraseñas débiles.
- Simplifica el acceso seguro para los administradores.
- Permite el acceso con un solo clic a Cisco Catalyst SD-WAN Manager y a otras aplicaciones autorizadas.

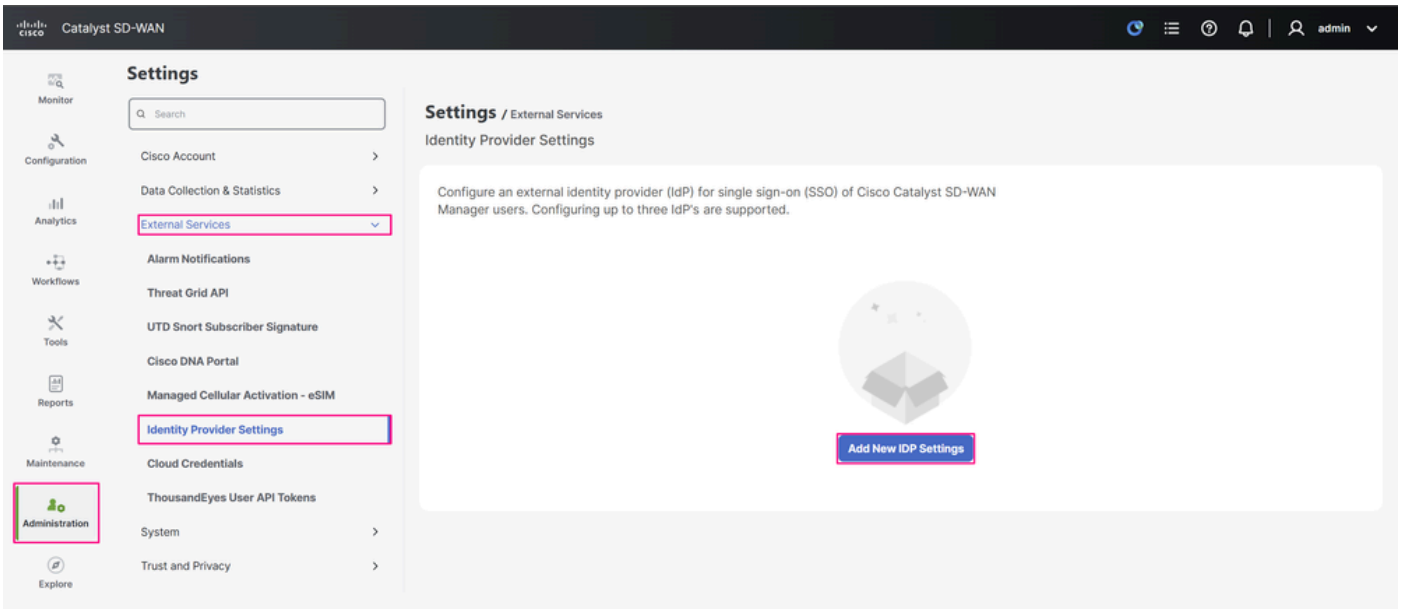
Configurar



Nota: Versión mínima admitida: Cisco Catalyst SD-WAN Manager versión 20.8.1.

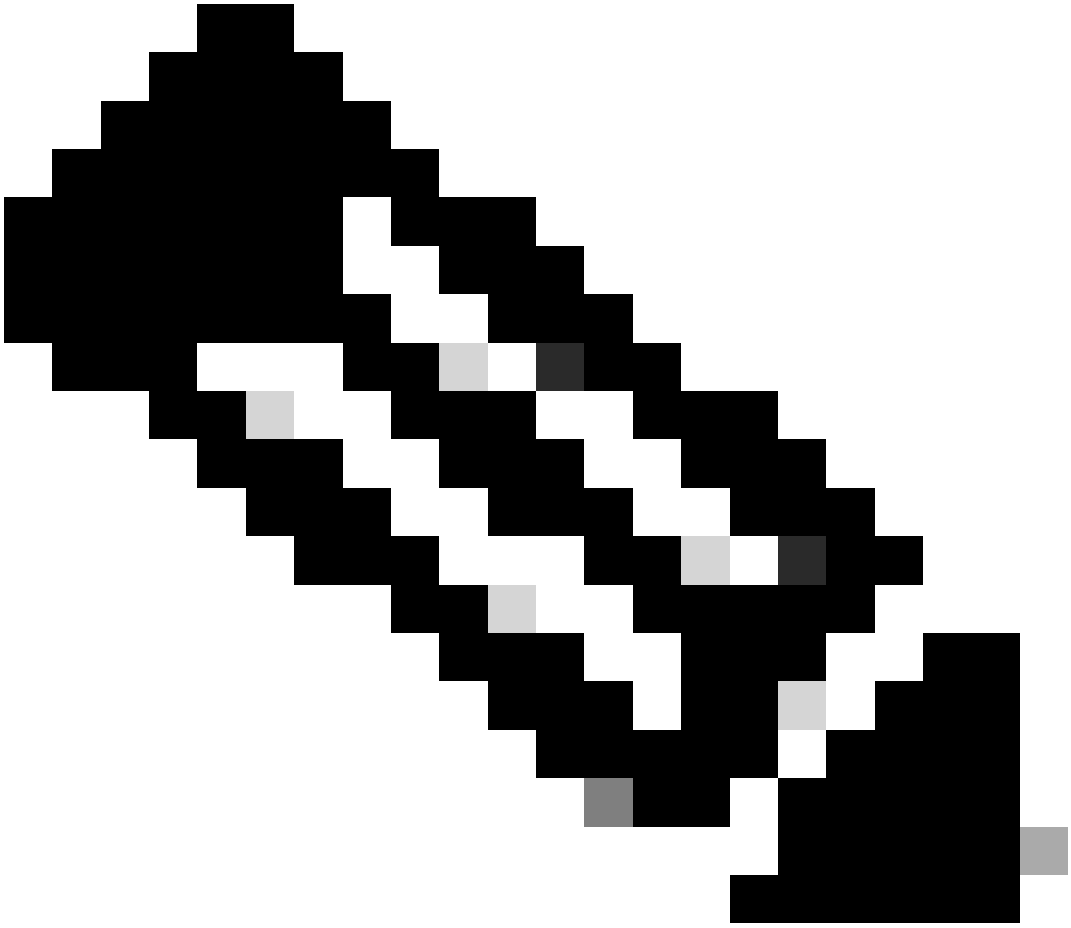
Paso 1. Obtener los metadatos SAML de Cisco SD-WAN Manager

- En Cisco SD-WAN Manager, navegue hasta Administration > Settings > External Services > Identity Provider Settings y haga clic en Add New IDP Settings.



IU de Cisco SD-WAN Manager

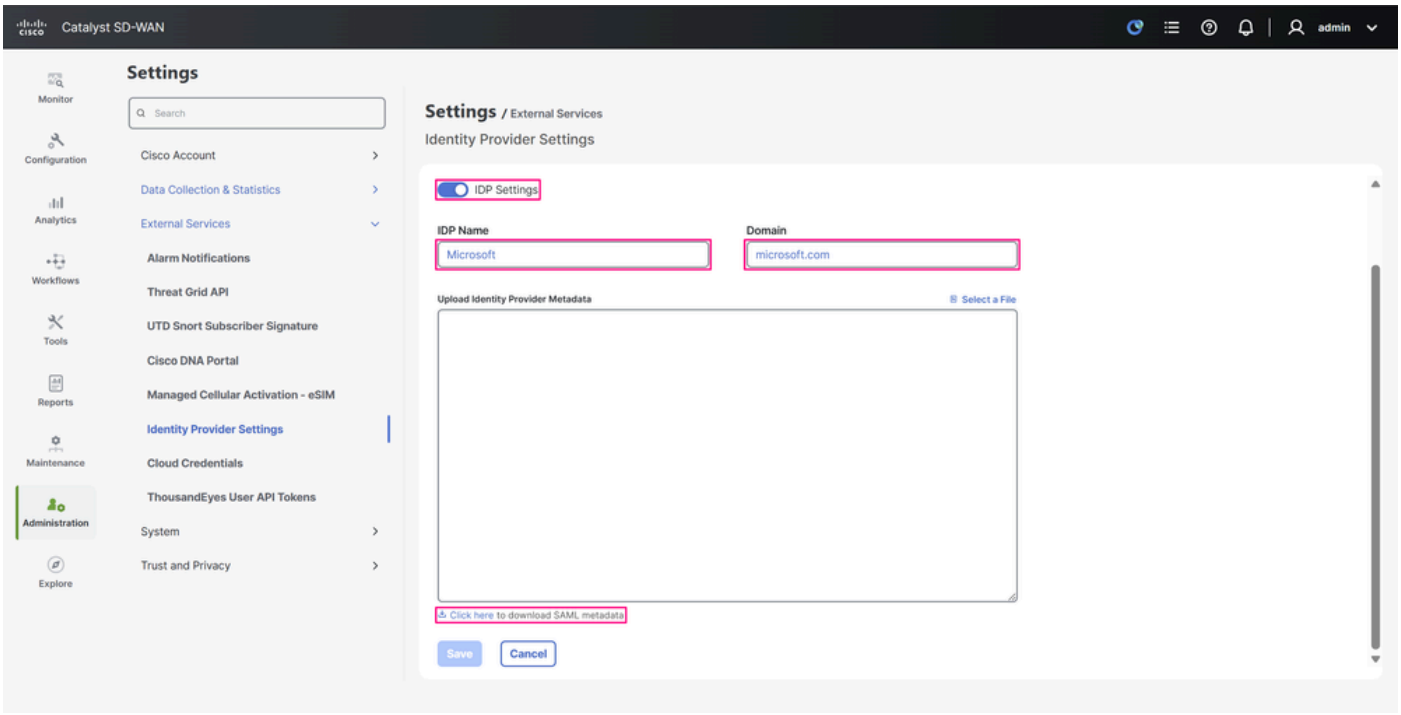
- Cambie IDP Settings para habilitar la configuración del proveedor de identidad. En el campo IDP Name, ingrese un nombre que haga referencia al IdP que está utilizando, y en el campo Domain, ingrese un dominio que coincida con los nombres de dominio utilizados por los usuarios en la aplicación empresarial de su organización. Haga clic en Haga clic aquí para descargar los metadatos SAML y guardar el archivo XML de metadatos en el equipo. Este archivo se utiliza para configurar SSO en Microsoft Entry ID en el paso siguiente.



Nota: En este ejemplo, el archivo XML de metadatos señala directamente a la dirección IP del Cisco SD-WAN Manager, pero en muchos entornos de producción, señala a su nombre de dominio completamente calificado (FQDN). Para un Cisco SD-WAN Manager independiente, el ID de entidad contenido en los metadatos coincide con la URL que se utiliza para iniciar sesión en el Cisco SD-WAN Manager en el momento de descargarlo. Esto significa que funciona con la dirección IP o el FQDN, ya que es una configuración de un solo nodo.

Para un clúster de Cisco SD-WAN Manager, se aplica el mismo principio en el sentido de que el FQDN apunta a uno de los nodos del clúster y los metadatos incluyen este dominio como ID de entidad. La diferencia radica en que, tanto si utiliza metadatos con el FQDN del clúster como si procede de un nodo específico mediante su dirección IP, una vez completada correctamente la integración de SSO con Microsoft Entry ID, los demás nodos también se redirigen al mensaje de inicio de sesión IdP.

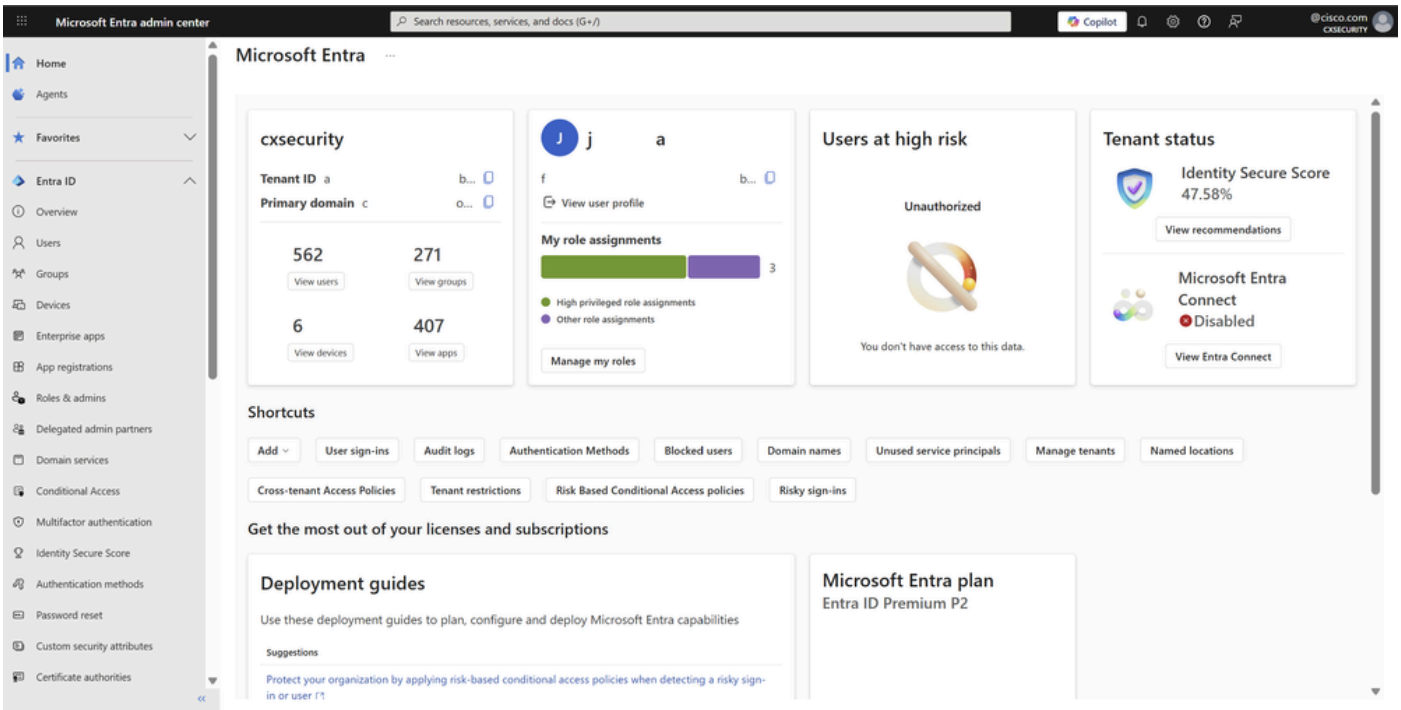
El requisito principal en ambos escenarios es que el Id. de entidad que utiliza en Cisco SD-WAN Manager, ya sea una dirección IP o un FQDN, coincida con el identificador configurado en el lado IdP.



Página Configuración de IdP

Paso 2. Configure una Aplicación Empresarial para SSO en Microsoft Entry ID

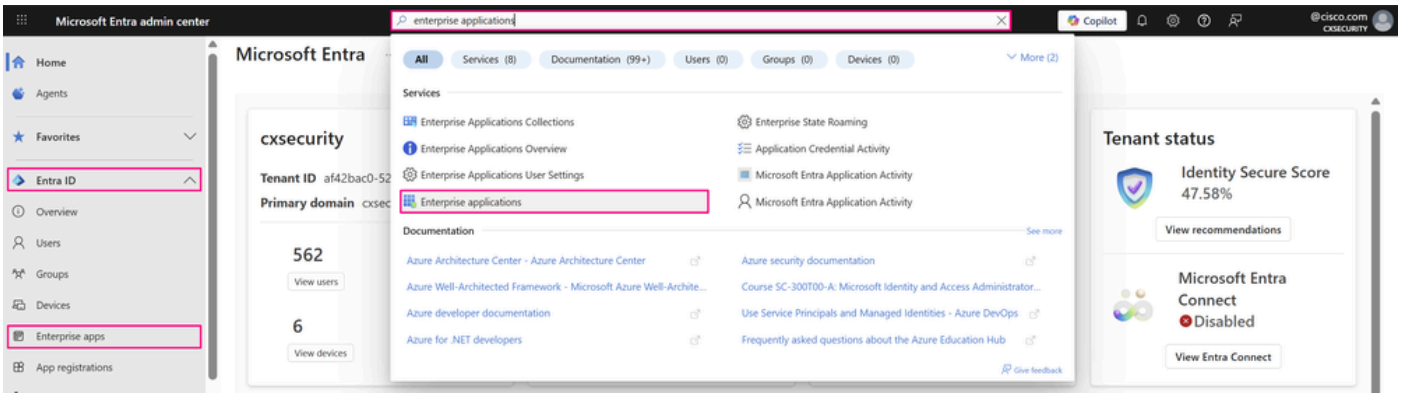
- Inicie sesión en el portal del centro de administración de Microsoft Entra con una de estas funciones: Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de seguridad del servicio.



Portal del Centro de administración de Microsoft Entra

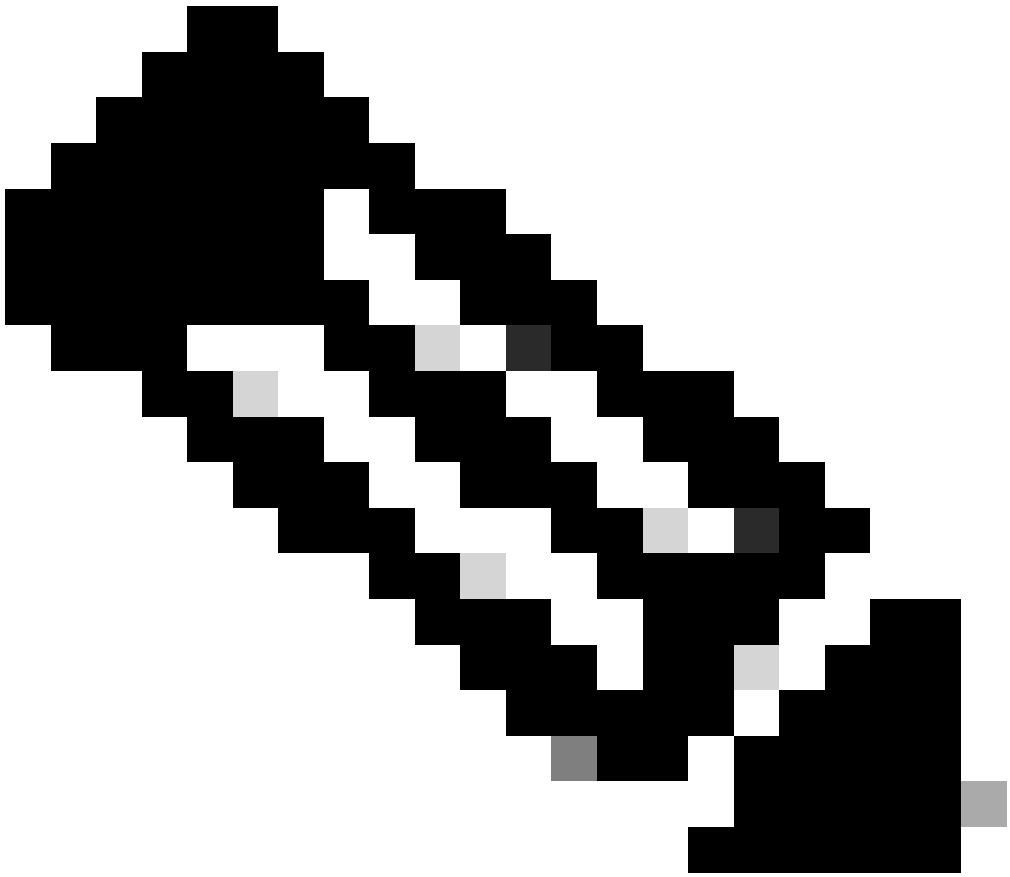
- Navegue hasta Entra ID > Enterprise apps, o también puede acceder a este servicio cuando ingrese aplicaciones empresariales en la barra de búsqueda en la parte superior del portal y

luego elija Enterprise Applications.



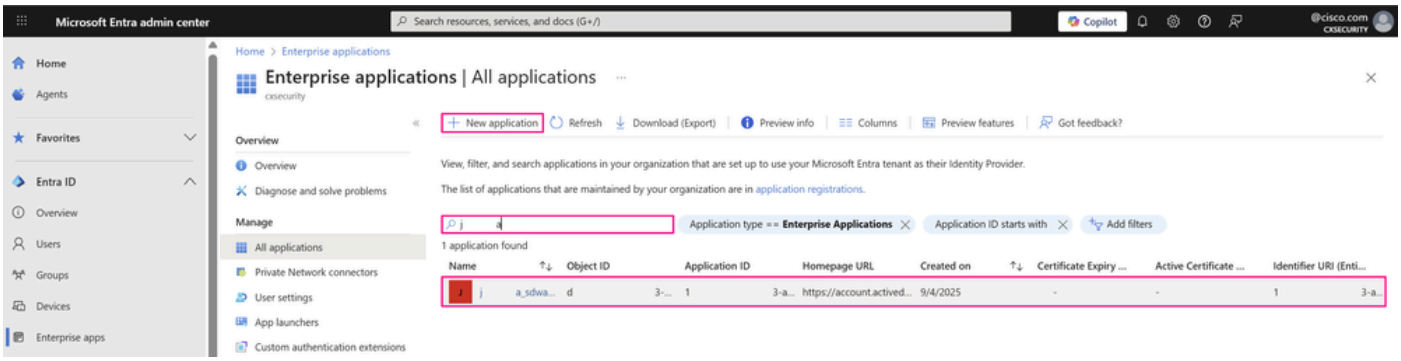
Portal del Centro de administración de Microsoft Entra

- Se abre la página Todas las aplicaciones. Introduzca el nombre de la aplicación existente en el cuadro de búsqueda y, a continuación, seleccione la aplicación en los resultados de la búsqueda.



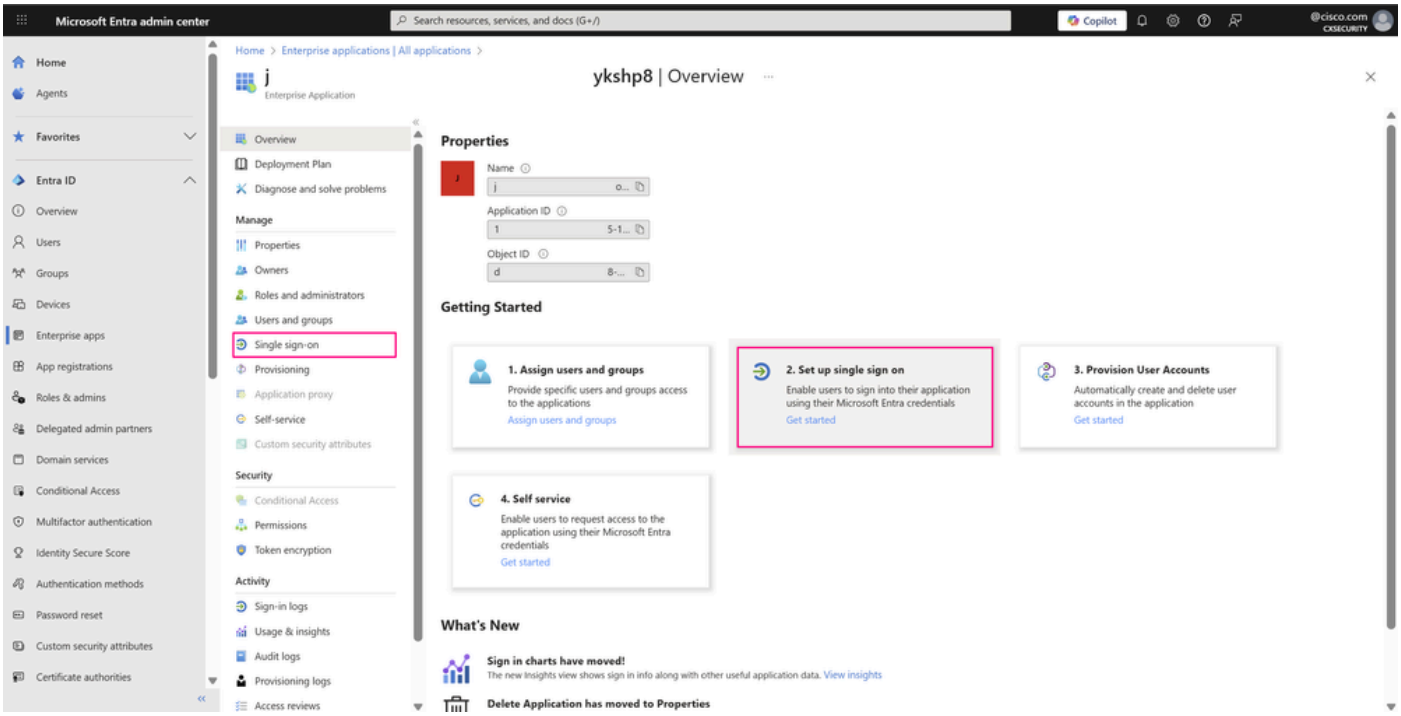
Nota: En esta misma página, puede crear una aplicación empresarial personalizada

basada en los requisitos de su organización y configurarla con autenticación SSO si aún no lo tiene, al hacer clic en Nueva aplicación.



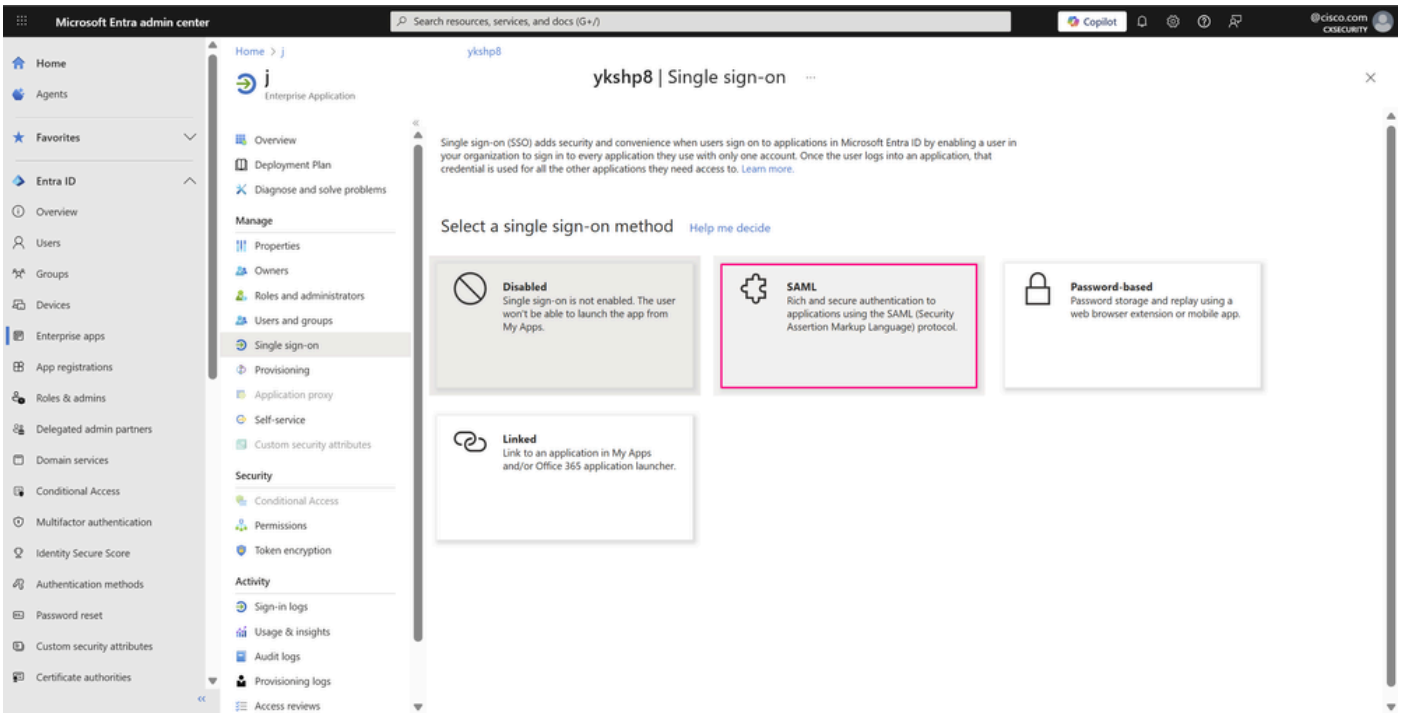
Panel de aplicaciones empresariales

- En la sección Administrar del menú izquierdo, haga clic en Inicio de sesión único, o bien, en el panel Introducción dentro de la sección Información general, haga clic en 2. Configure el inicio de sesión único para abrir el panel Inicio de sesión único para su edición.



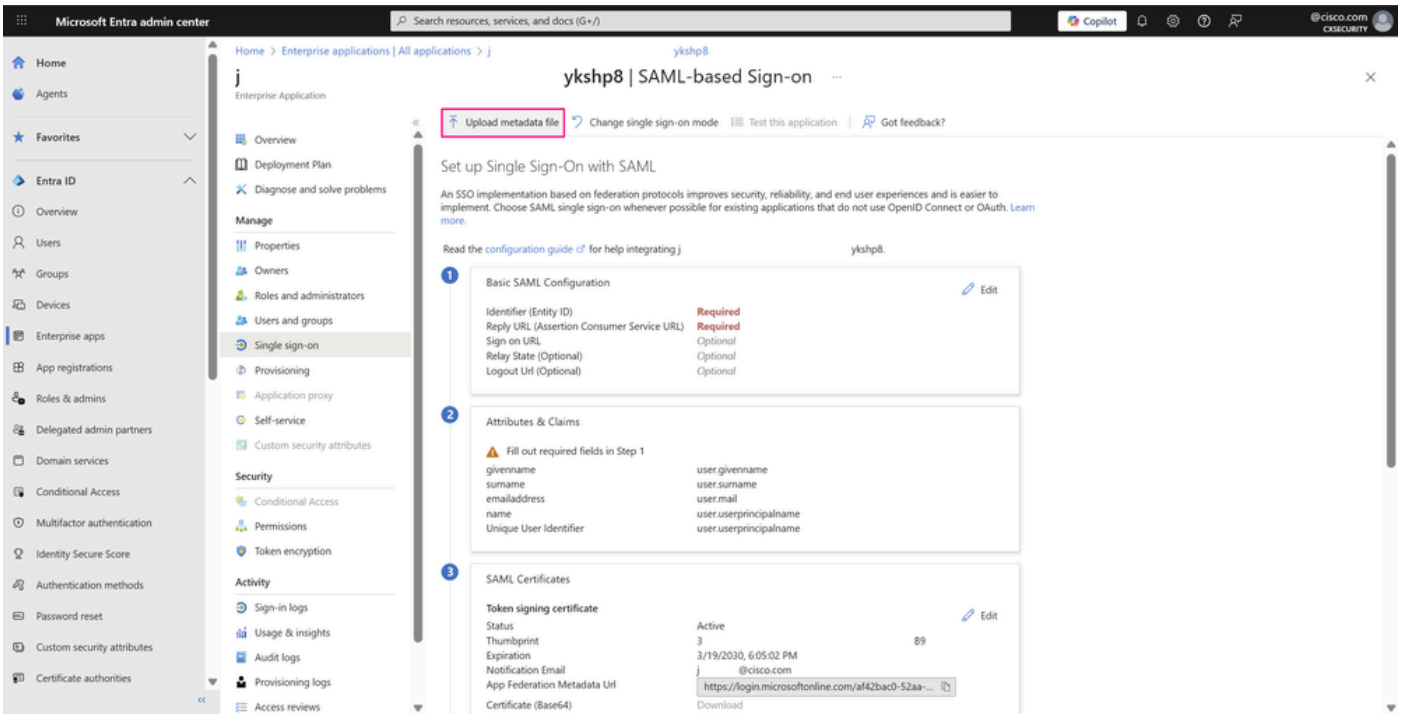
Descripción general de aplicaciones empresariales

- Seleccione SAML para abrir la página de configuración de SSO.



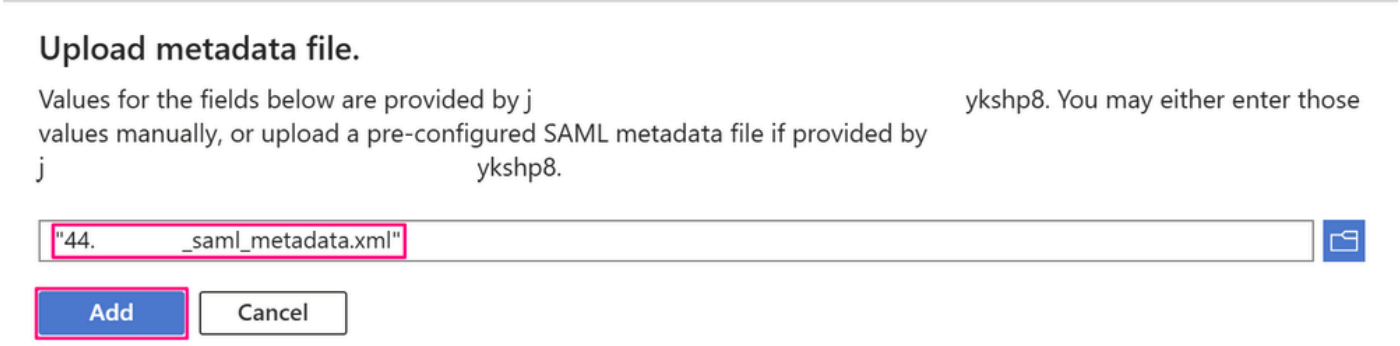
Panel de inicio de sesión único

- En la página Configurar el inicio de sesión único con SAML, haga clic en Cargar archivo de metadatos.



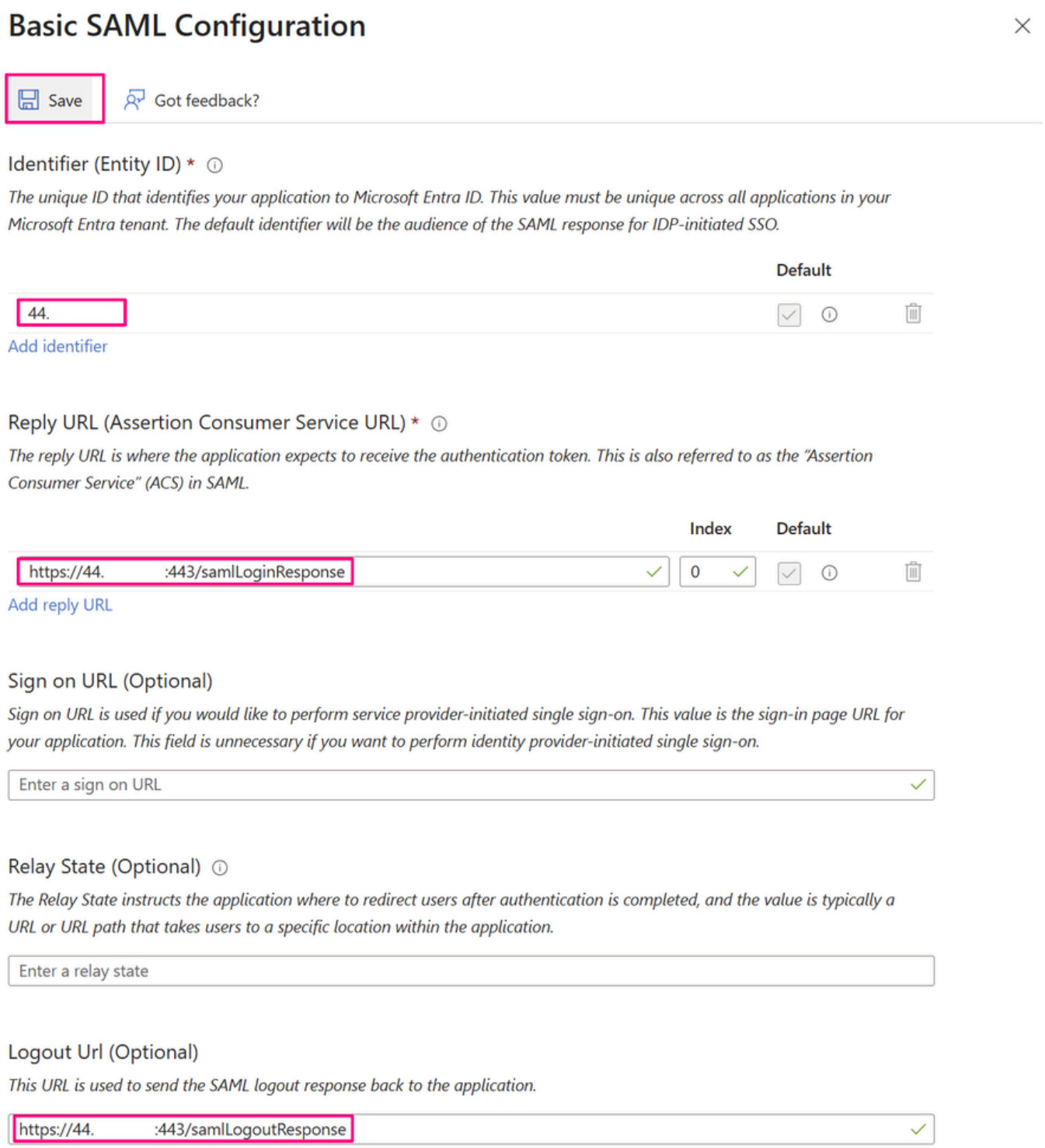
Página SSO con Configuración SAML

- En la ventana Cargar archivo de metadatos, busque y haga clic en el archivo XML de metadatos que descargó anteriormente y, a continuación, haga clic en Agregar.



Ventana Cargar Archivo de Metadatos

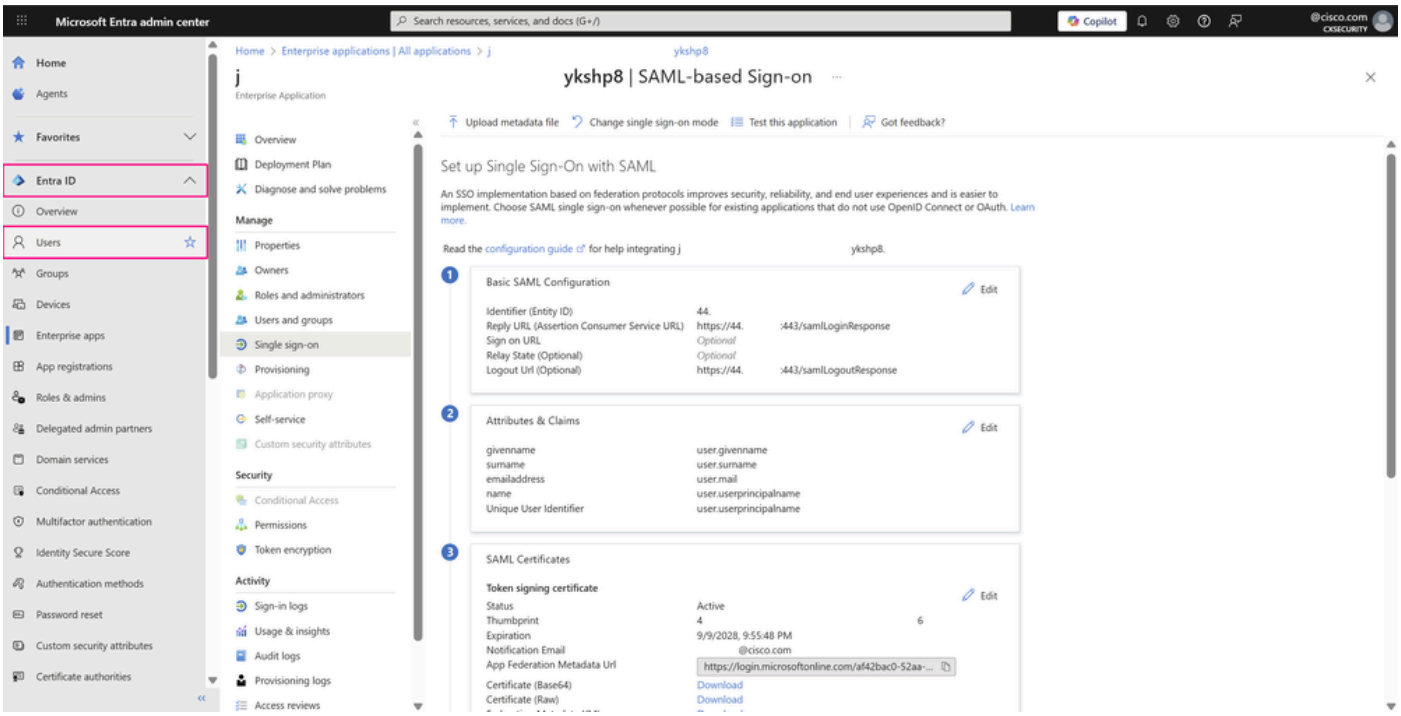
- En la ventana Basic SAML Configuration, el Identificador (Entity ID) es típicamente la URL específica de la aplicación (en este caso, el Cisco SD-WAN Manager) con la que se está integrando (como se explicó en el paso anterior). Los valores URL de respuesta y URL de cierre de sesión se rellenan automáticamente una vez que el archivo se ha cargado correctamente. Para continuar, haga clic en Guardar.



Ventana Configuración básica de SAML

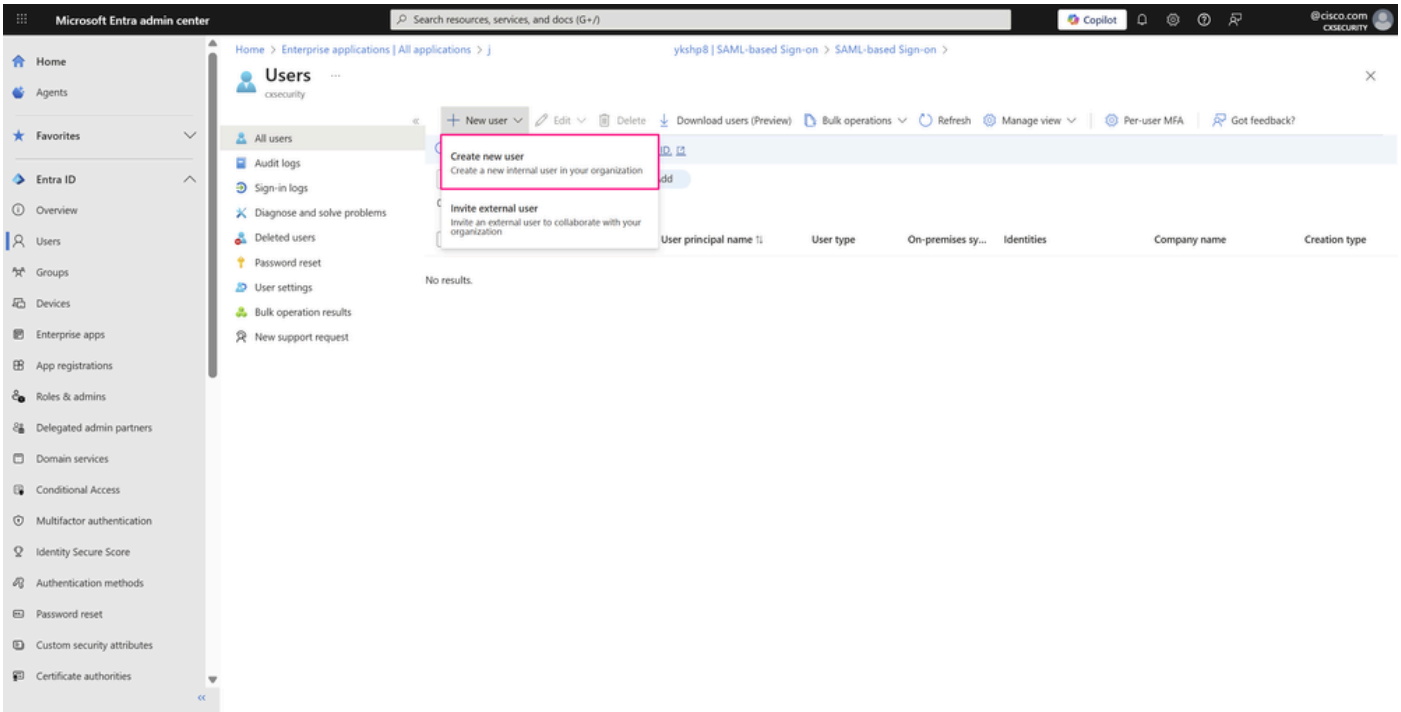
Paso 3. Agregar una cuenta de usuario o de grupo a la aplicación de empresa

- Con los parámetros de configuración SAML de la aplicación definida, se procede a agregar los usuarios o grupos de la aplicación de empresa que inician sesión en la aplicación. Para ello, navegue primero hasta Entra ID > Users, o también puede acceder a este servicio cuando busque el nombre del servicio en la barra de búsqueda en la parte superior del portal, como se muestra en un paso anterior.



Página SSO con Configuración SAML

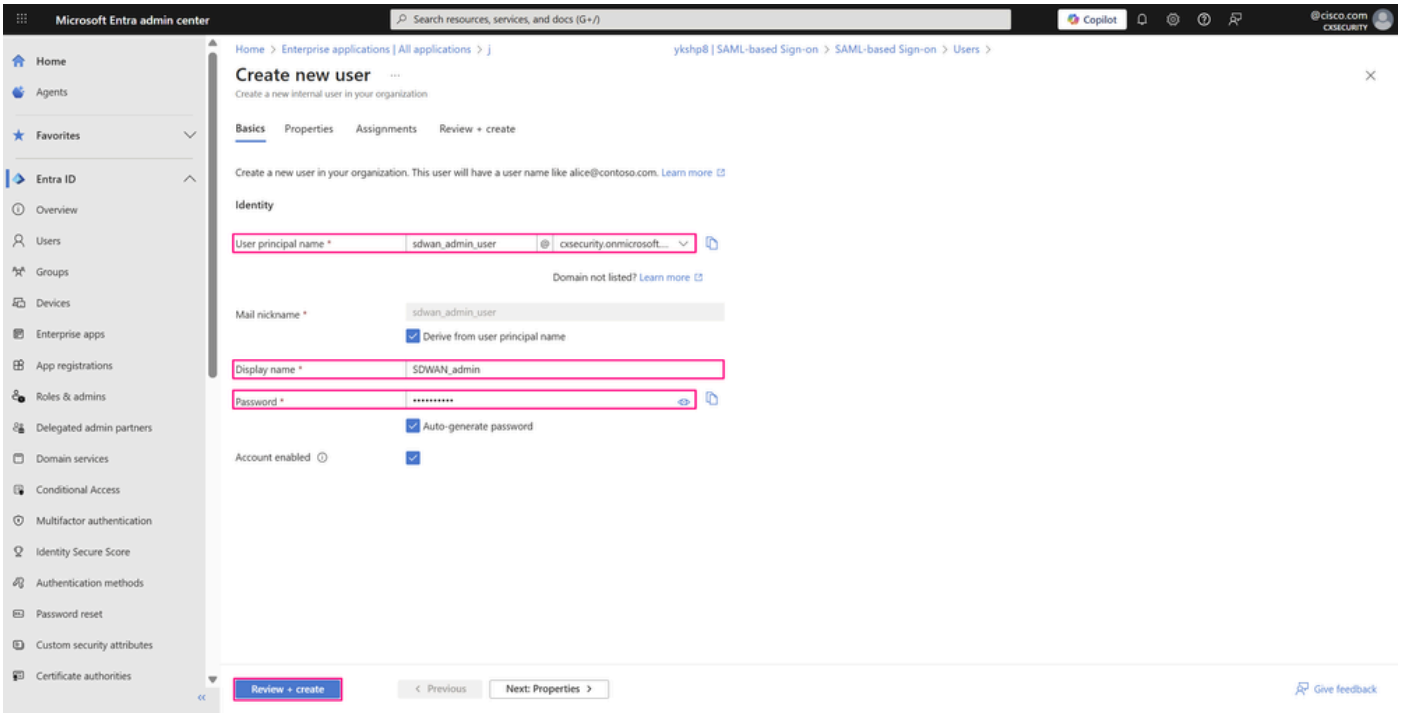
- Cree un usuario que asocie con un grupo para ilustrar la autenticación SSO con Cisco SD-WAN Manager y uno de sus grupos de usuarios, netadmin, que es el más común en los entornos de producción. Para ello, navegue hasta Entra ID > Users. A continuación, haga clic en New user y elija Create new user.



Panel de usuarios

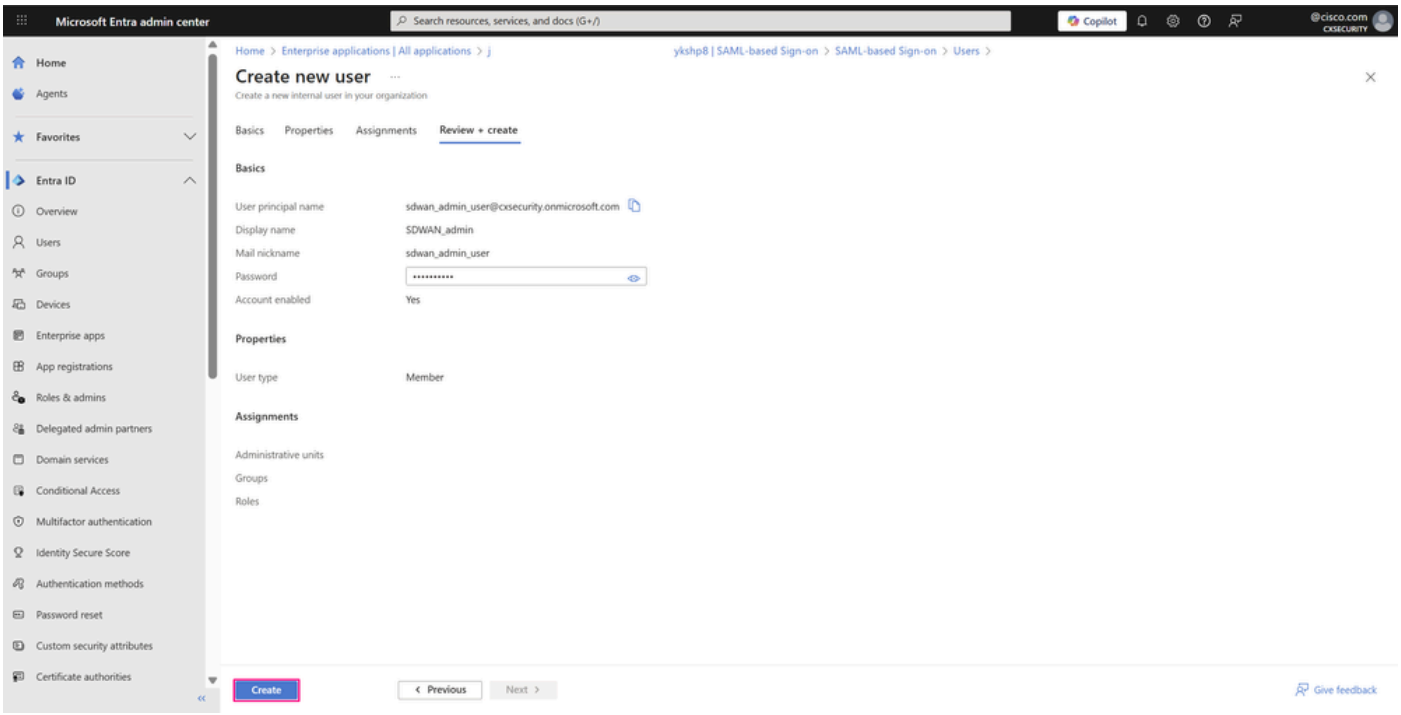
- La ficha Conceptos básicos contiene los campos principales necesarios para crear un nuevo usuario.
  - Para el Nombre principal de usuario, introduzca un nombre de usuario único y elija un dominio de la lista desplegable de dominios disponibles en su organización.

- Introduzca un nombre para mostrar para el usuario.
- Desmarque Auto-generate password si desea introducir una contraseña personalizada, o deje esta opción marcada para que se genere automáticamente.
- Puede agregar el usuario a un grupo en la ficha Asignaciones, pero como la pertenencia al grupo aún no se ha creado, haga clic en Revisar + crear.



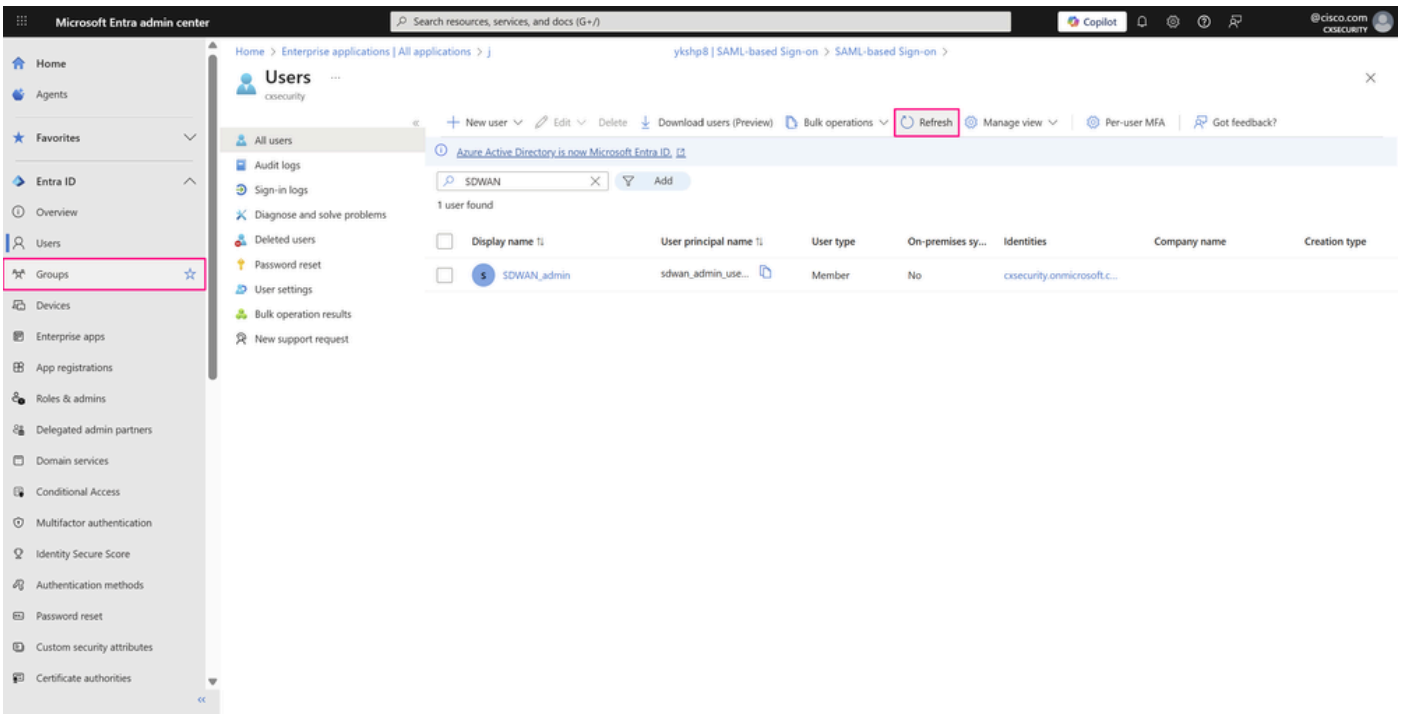
Página de creación de usuario

- La ficha final muestra los detalles clave del flujo de trabajo de creación de usuarios. Revise los detalles y haga clic en Create para completar el proceso.



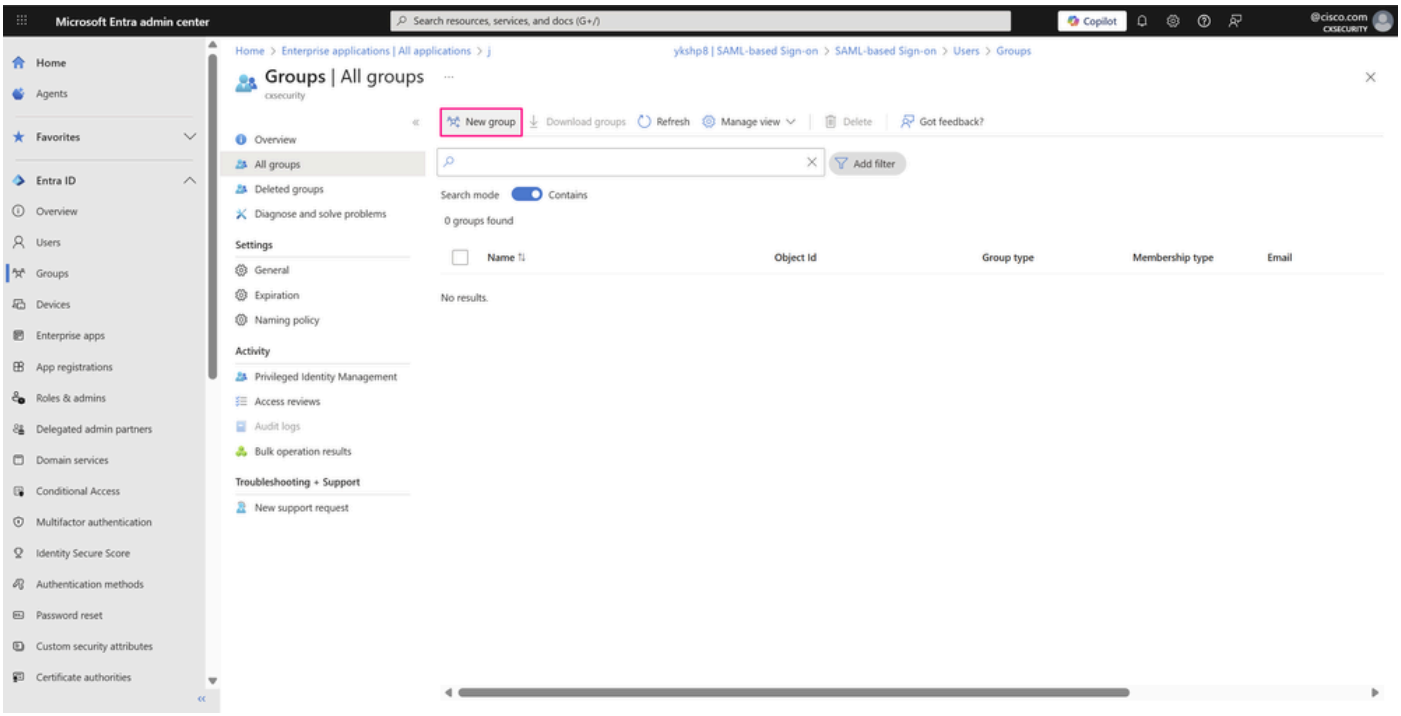
Página de creación de usuario

- El nuevo usuario aparecerá poco después. Si no es así, haga clic en Refresh (Actualizar) y busque el usuario mediante la barra de búsqueda del servicio. A continuación, navegue hasta Entrar ID > Grupos > Todos los grupos para crear el nuevo grupo.



Panel de usuarios

- En esta página puede administrar los distintos grupos y sus permisos dentro de la organización. Haga clic en Nuevo grupo para crear el grupo que tiene privilegios de administrador de red.

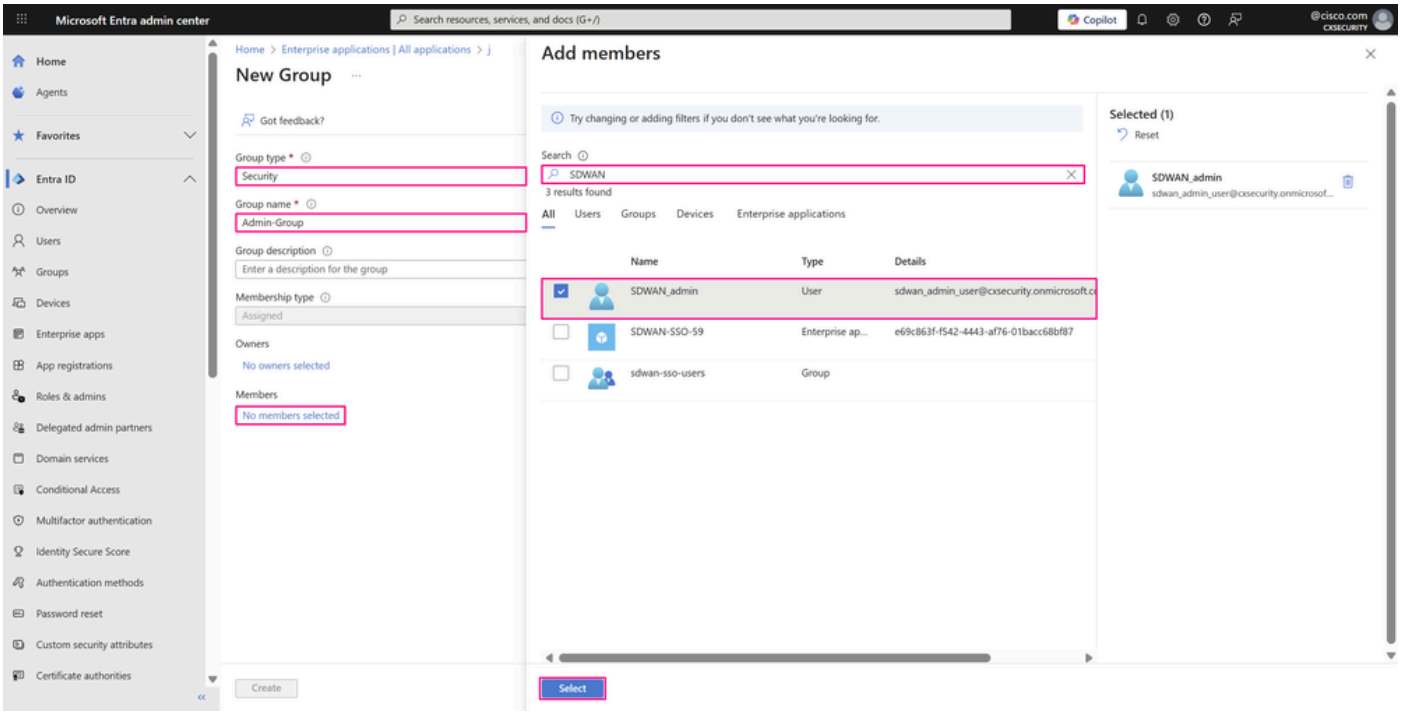


Página Todos los Grupos

- Elija un tipo de grupo en la lista desplegable; en este caso, Seguridad, ya que sólo se

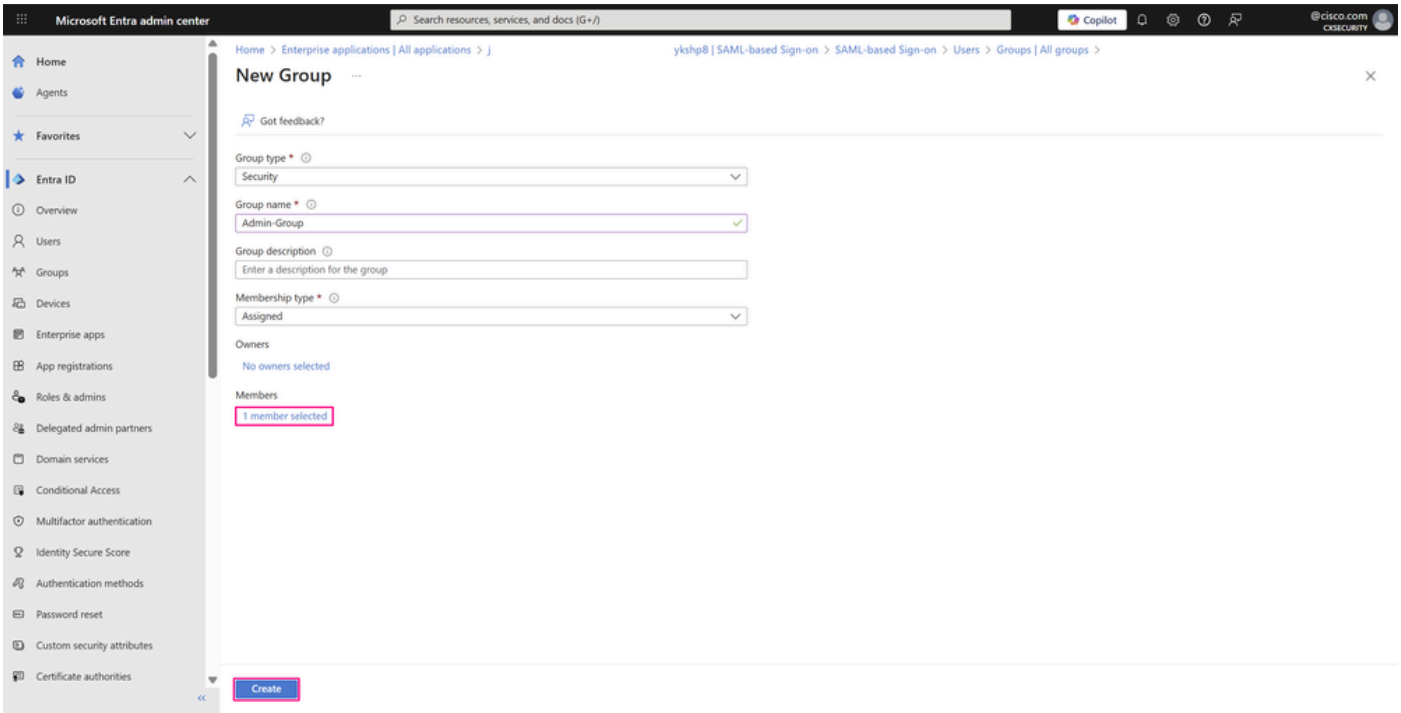
requiere acceso a los recursos compartidos. Introduzca el nombre de grupo que desee que haga referencia a la función o los permisos del grupo. En este punto, asocie los usuarios al grupo cuando haga clic en los miembros seleccionados en el campo Miembros.

- En la ventana Add members, navegue y elija los usuarios que desea agregar, en nuestro ejemplo, el usuario que acaba de crear, y luego haga clic en Select.



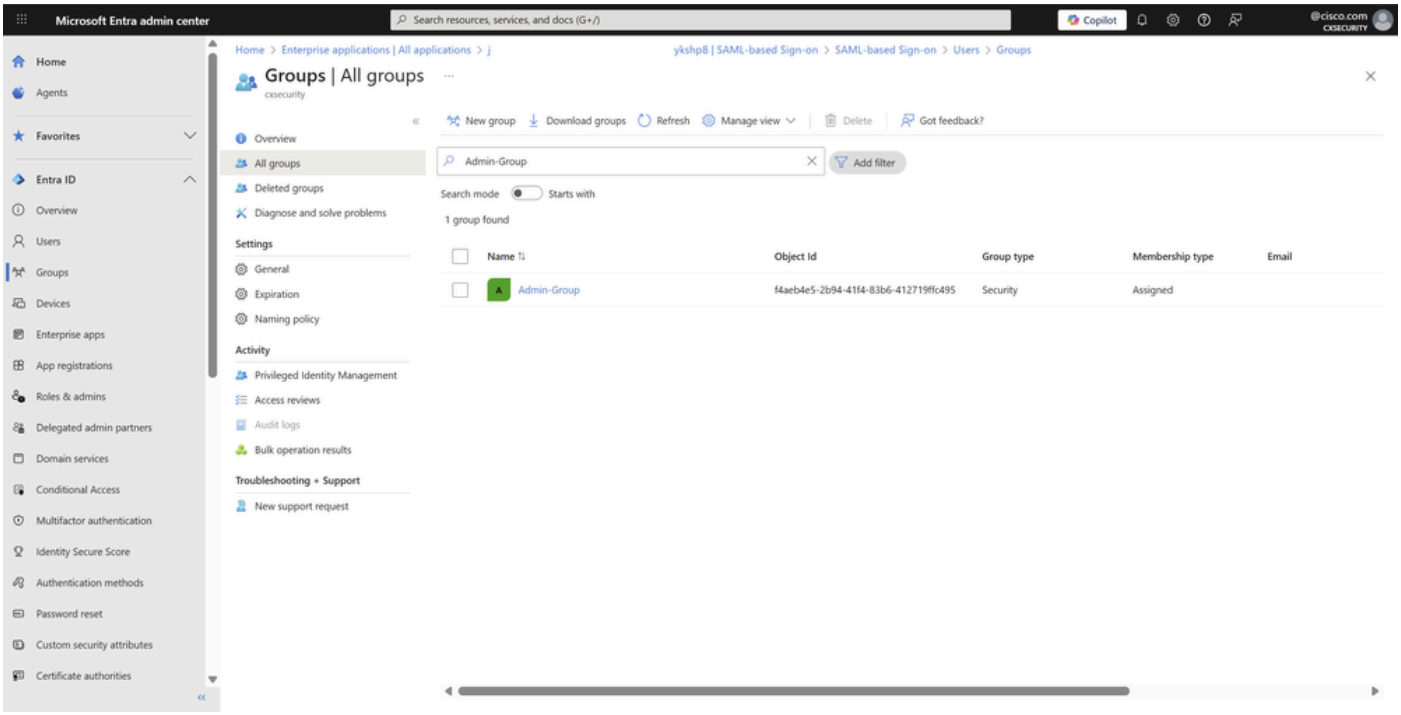
Página Creación de Grupo

- Haga clic en Create para crear el grupo.



Página Creación de Grupo

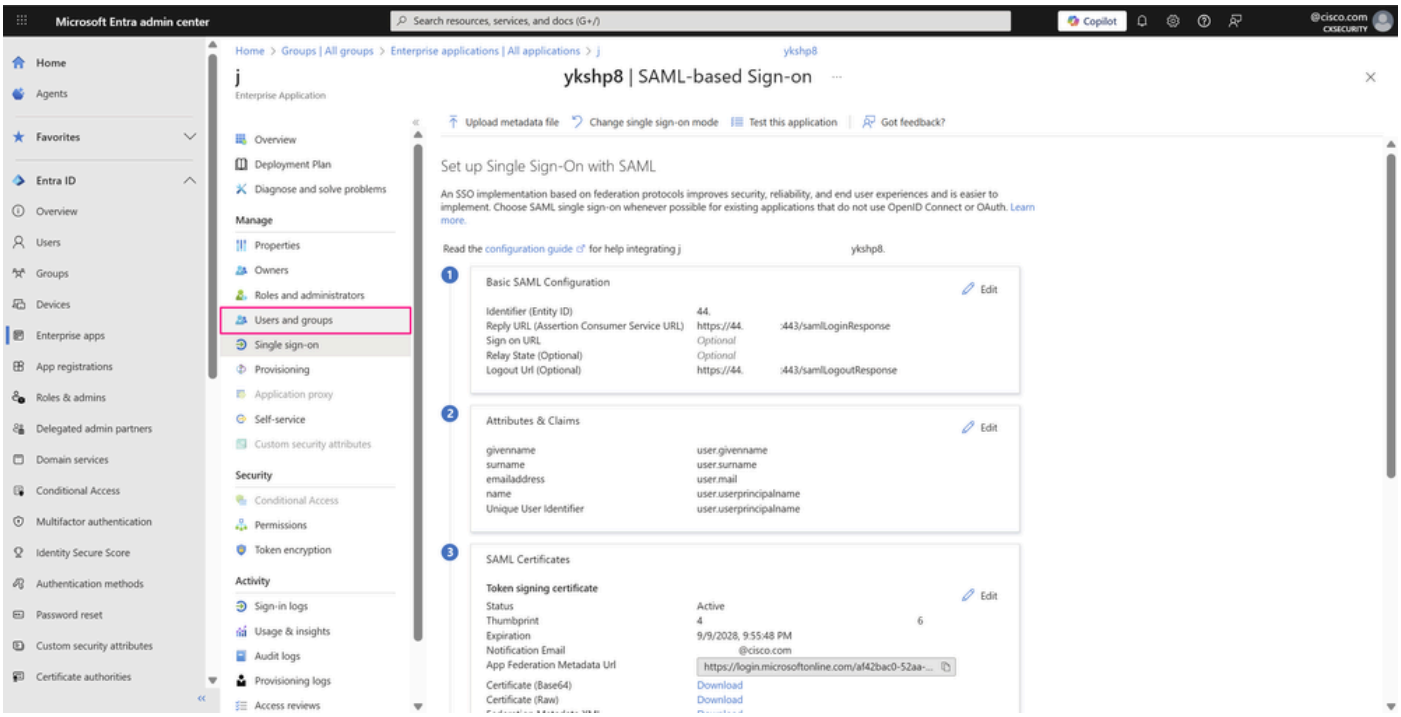
- El nuevo grupo aparecerá poco después. Si no es así, haga clic en Refresh y busque el nombre del grupo con la barra de búsqueda dentro del servicio. Repita los pasos anteriores para crear otro usuario y agregarlo a una pertenencia al grupo diferente para validar el inicio de sesión de SSO con la aplicación y uno de sus otros grupos de usuarios, como operator.



Página Todos los Grupos

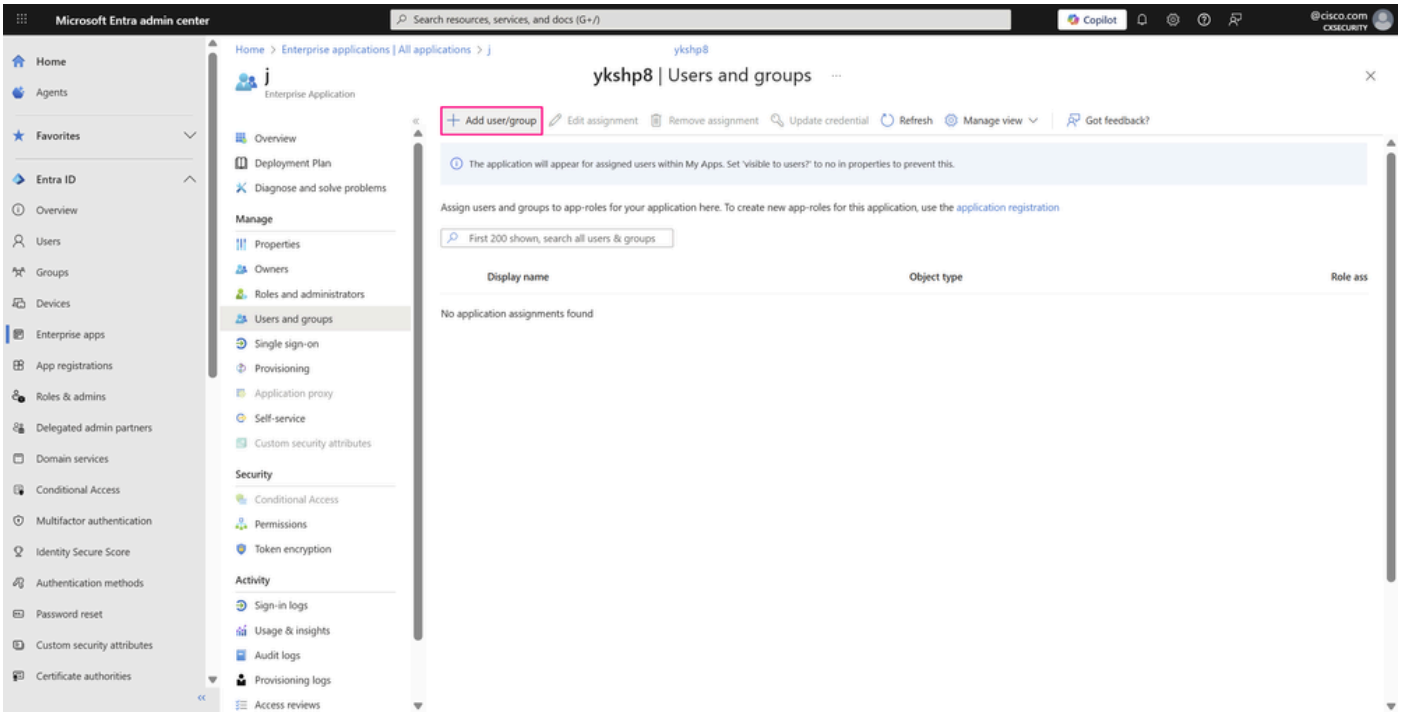
Paso 4. Configuración del Aprovisionamiento de Grupos SAML para Microsoft Entry ID

- Para aprovisionar los grupos o los usuarios asociados a ellos en la configuración SAML, debe asignarlos a la aplicación de empresa para que tengan permisos de inicio de sesión para la aplicación, por ejemplo, Cisco SD-WAN Manager. Navegue hasta Entra ID > Enterprise apps y abra su aplicación empresarial. En la sección Administrar del menú izquierdo, haga clic en Usuarios y grupos.



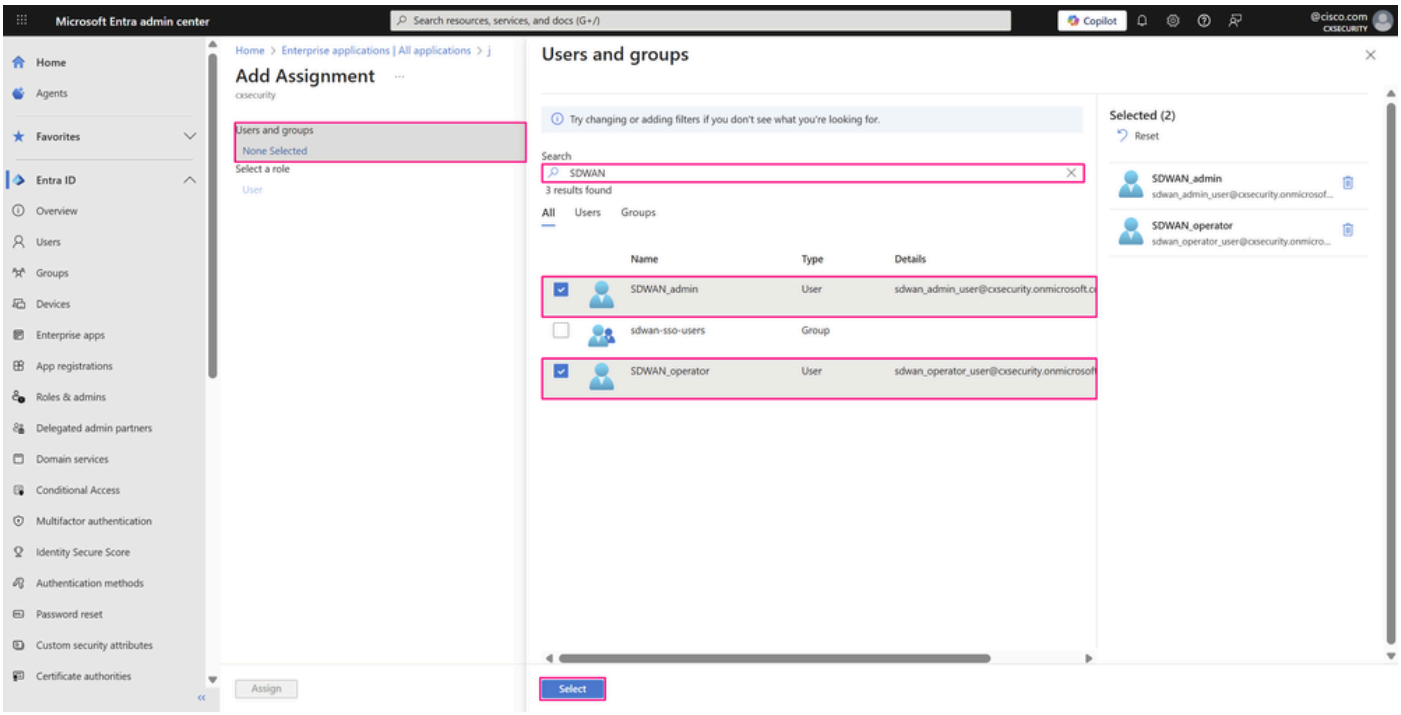
Página SSO con Configuración SAML

- A continuación, haga clic en Agregar usuario/grupo.



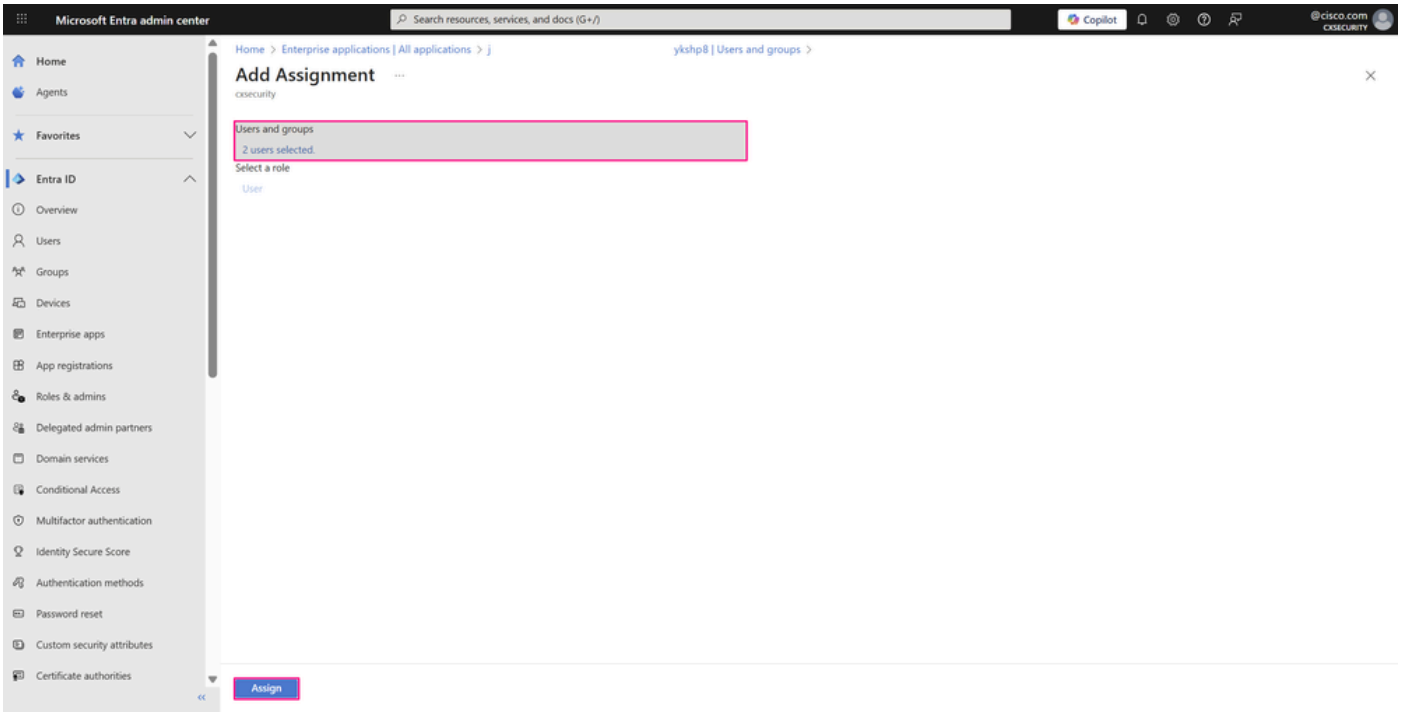
Página Usuario y Grupos

- En el panel Add Assignment, haga clic en None Selected en el campo Users and groups. Busque y elija el usuario o grupo que desea asignar a la aplicación (en nuestro ejemplo, los dos usuarios creados en los pasos anteriores) y, a continuación, haga clic en Seleccionar.



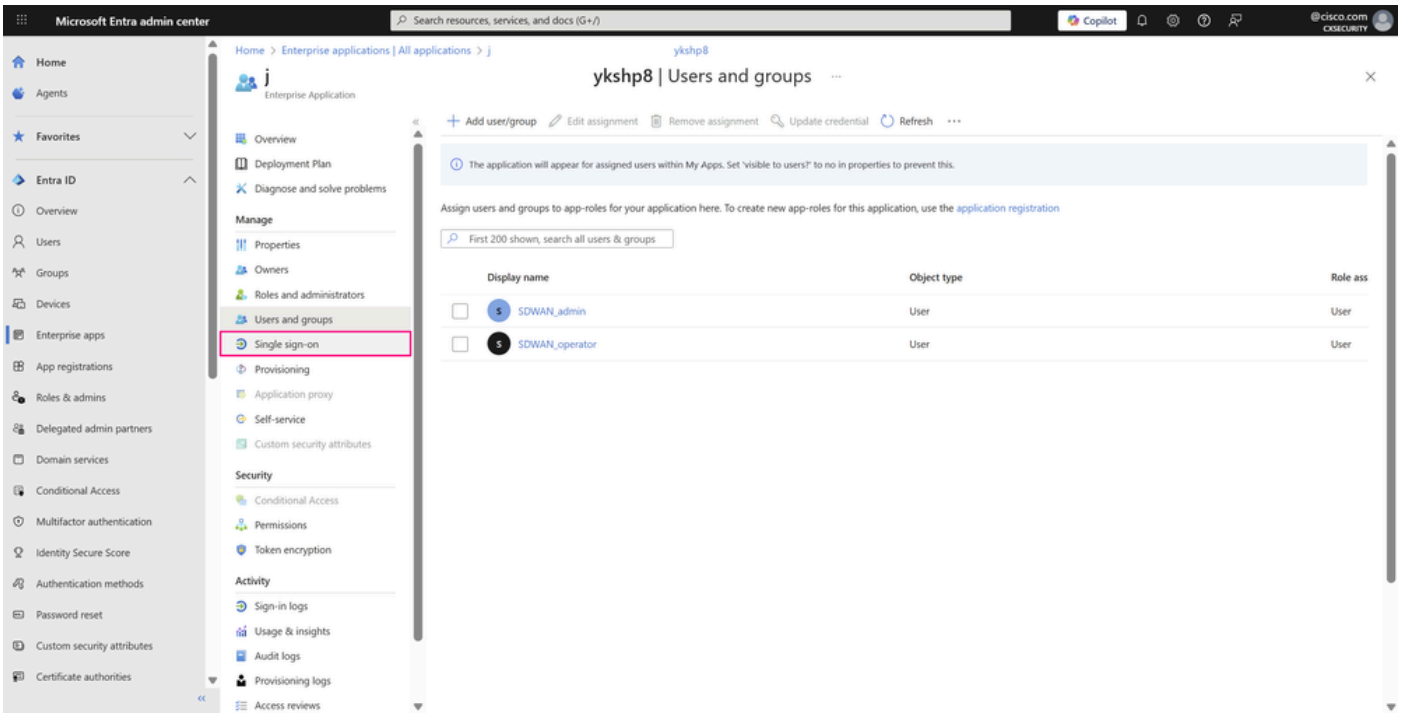
Panel de asignación de usuario/grupo

- Haga clic en Asignar para asignar el usuario o grupo a la aplicación.



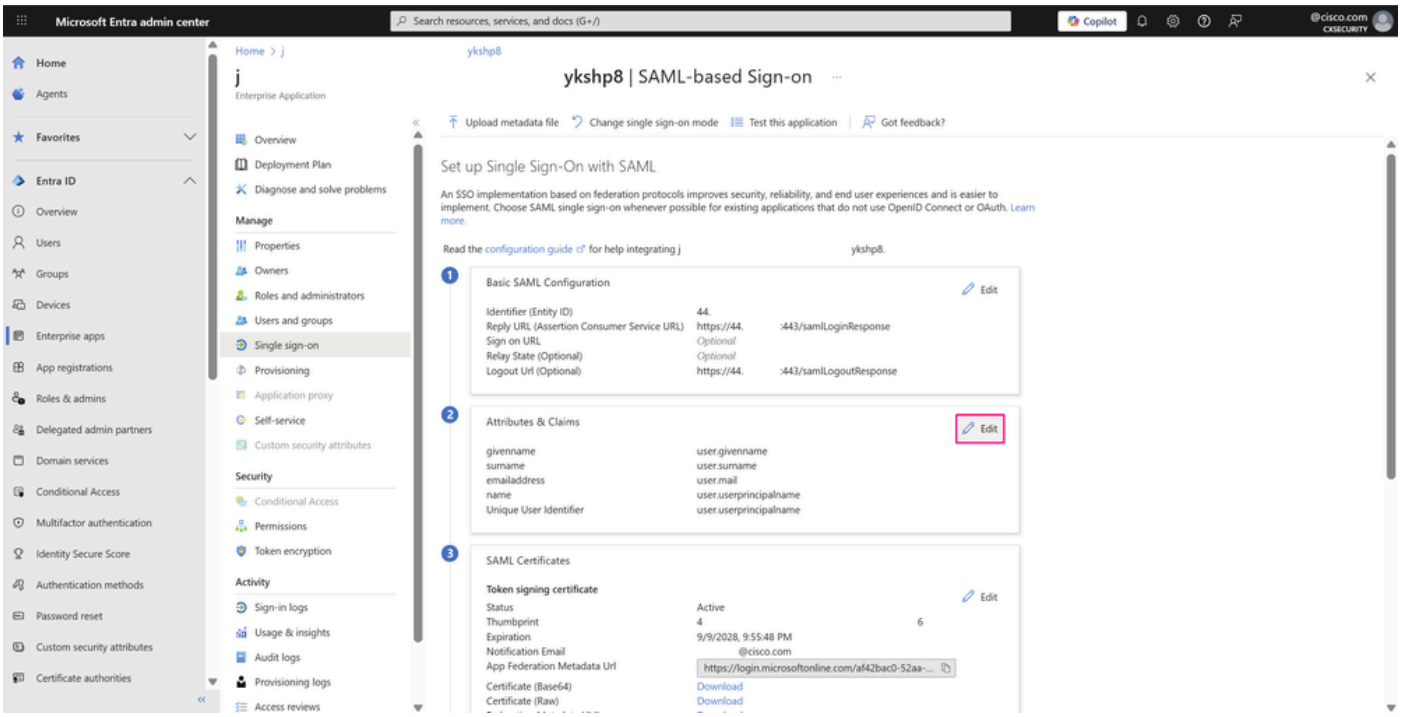
Panel de asignación de usuario/grupo

- Los usuarios asignados a la aplicación de empresa se muestran poco después de la asignación. Haga clic en Single Sign-on en la sección Manage del menú izquierdo para acceder a la configuración SAML de SSO de su aplicación y completar el resto de la configuración necesaria.



Página Usuario y Grupos

- En la página Configurar el inicio de sesión único con SAML, en Atributos y reclamaciones, haga clic en Editar.

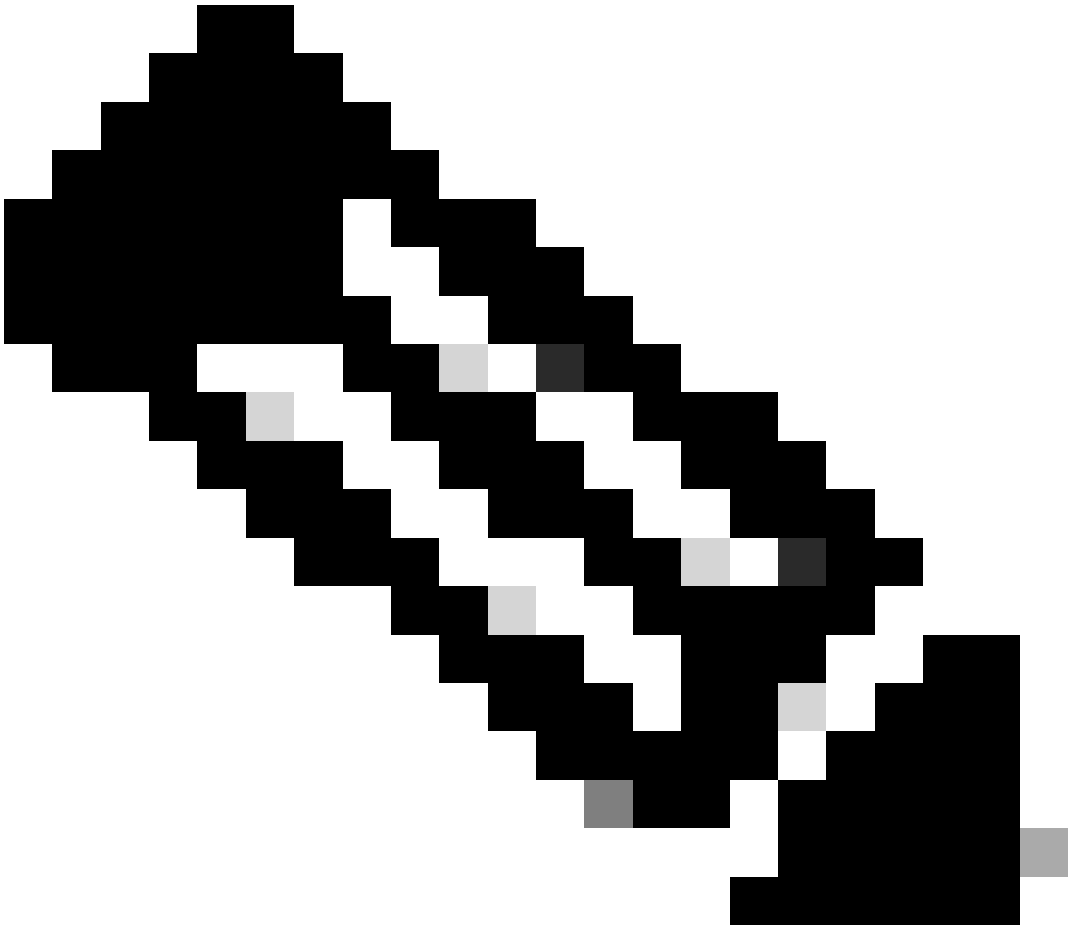


Página SSO con Configuración SAML

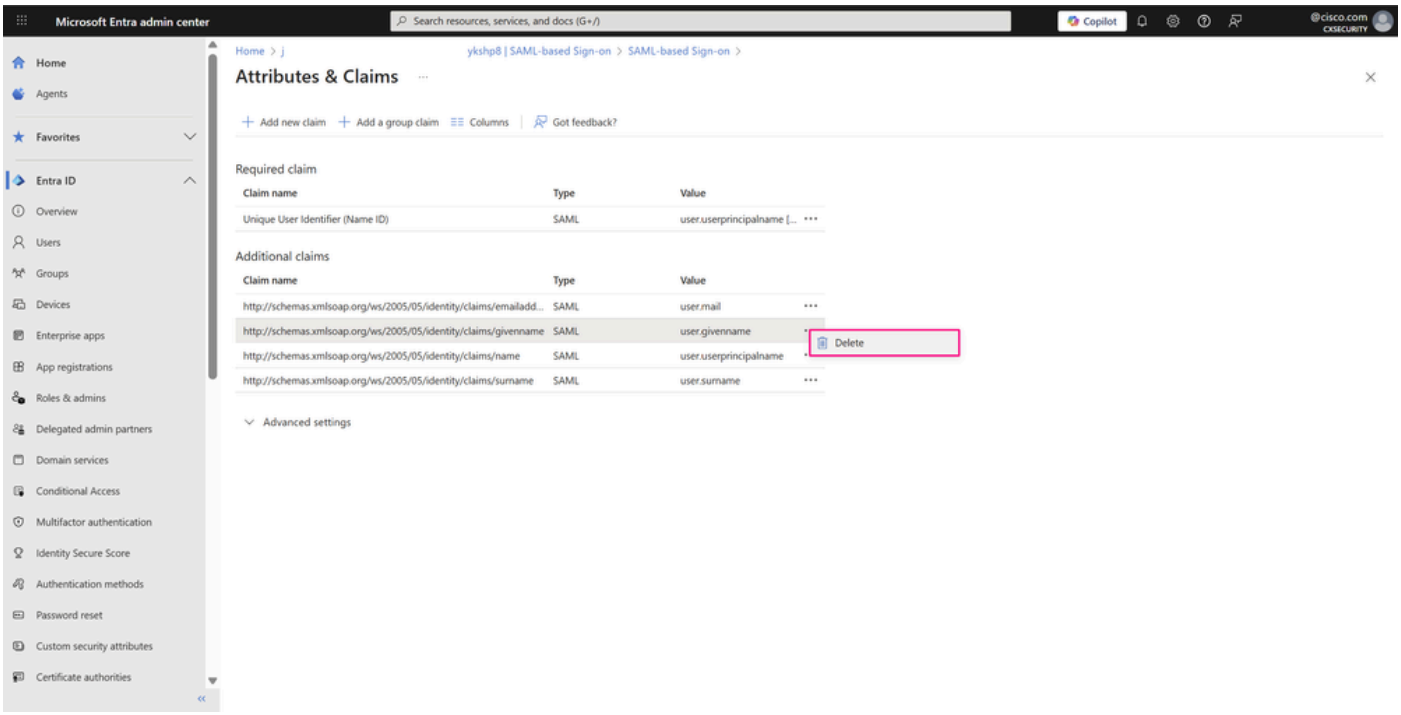
- En la página Atributos y reclamaciones, haga clic en el icono de tres puntos y, a continuación, en Eliminar para eliminar la reclamación con el valor user.givenname y la reclamación con el valor user.surname, ya que no son necesarias para este ejemplo.Sólo son necesarias las siguientes reclamaciones para la autenticación básica de SSO con su aplicación:

- Dirección de correo electrónico del usuario -user.mail
- Nombre principal de usuario (UPN) del usuario -user.userprincipalname

---

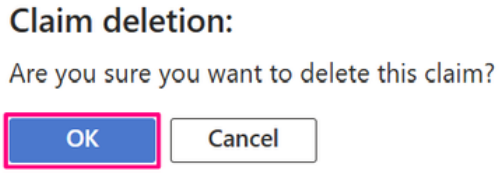


Nota: Su organización puede requerir reclamaciones adicionales en función de sus necesidades específicas.



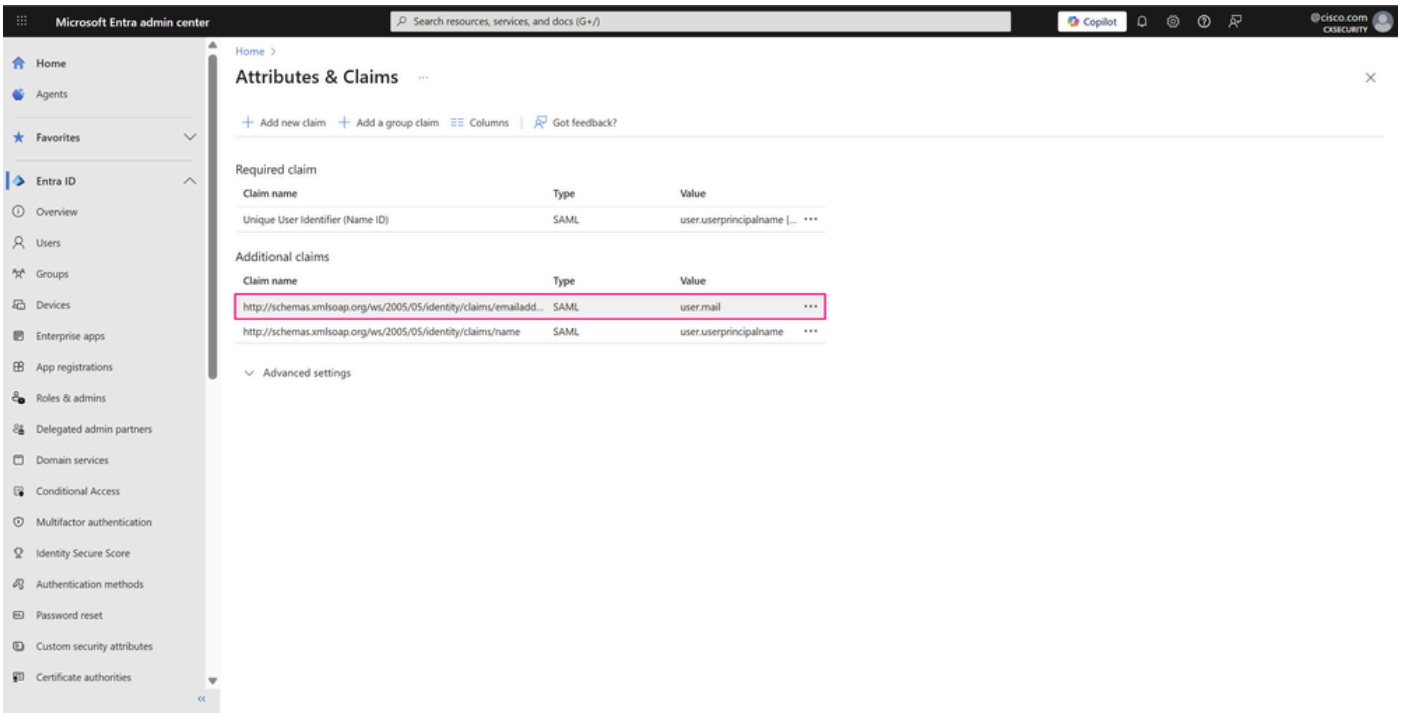
Página Atributos y Reclamaciones

- En la ventana Eliminación de reclamación, haga clic en Aceptar para eliminar la reclamación.



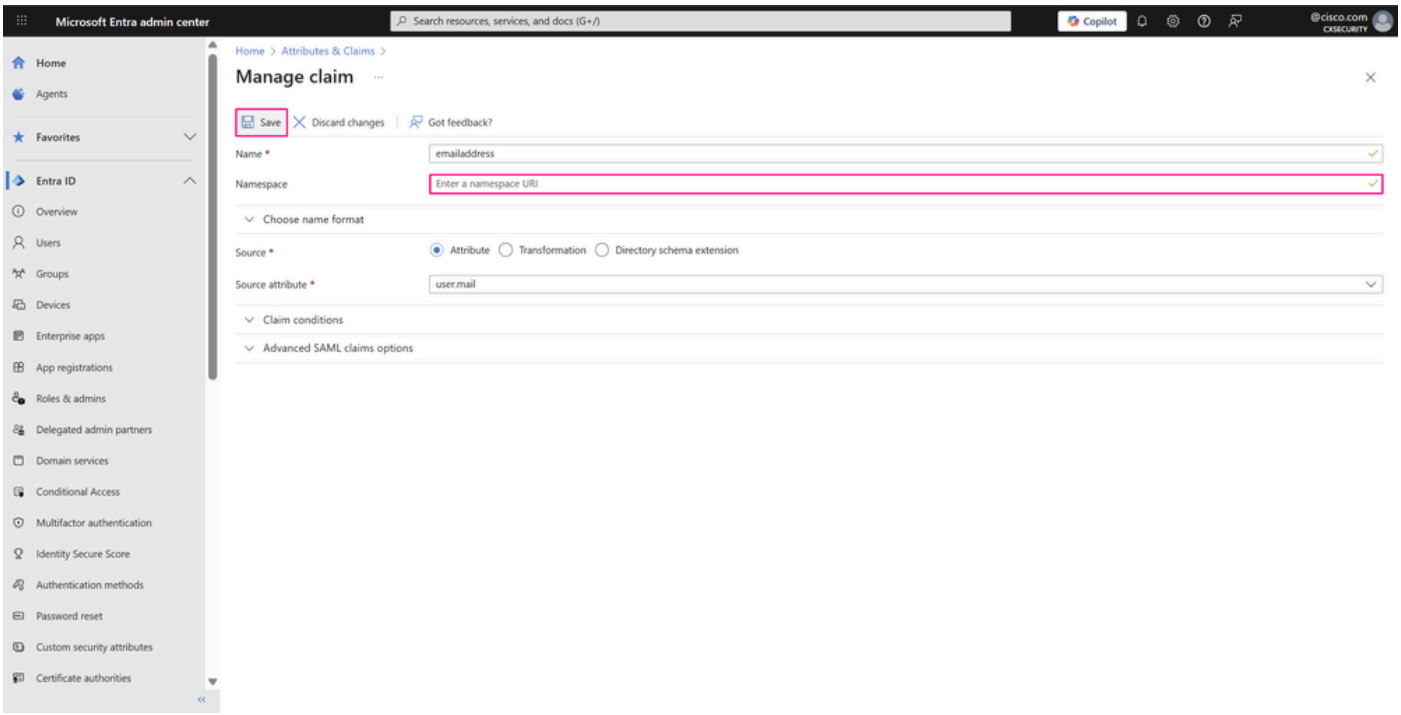
Ventana Eliminación de reclamación

- A continuación, quite el espacio de nombres del nombre de reclamación en las dos reclamaciones restantes, ya que este campo es opcional. Este cambio permite que el nombre real de cada uno se muestre en esta página para una identificación más sencilla. Pase el ratón sobre cada justificante y haga clic en él para acceder a su configuración.



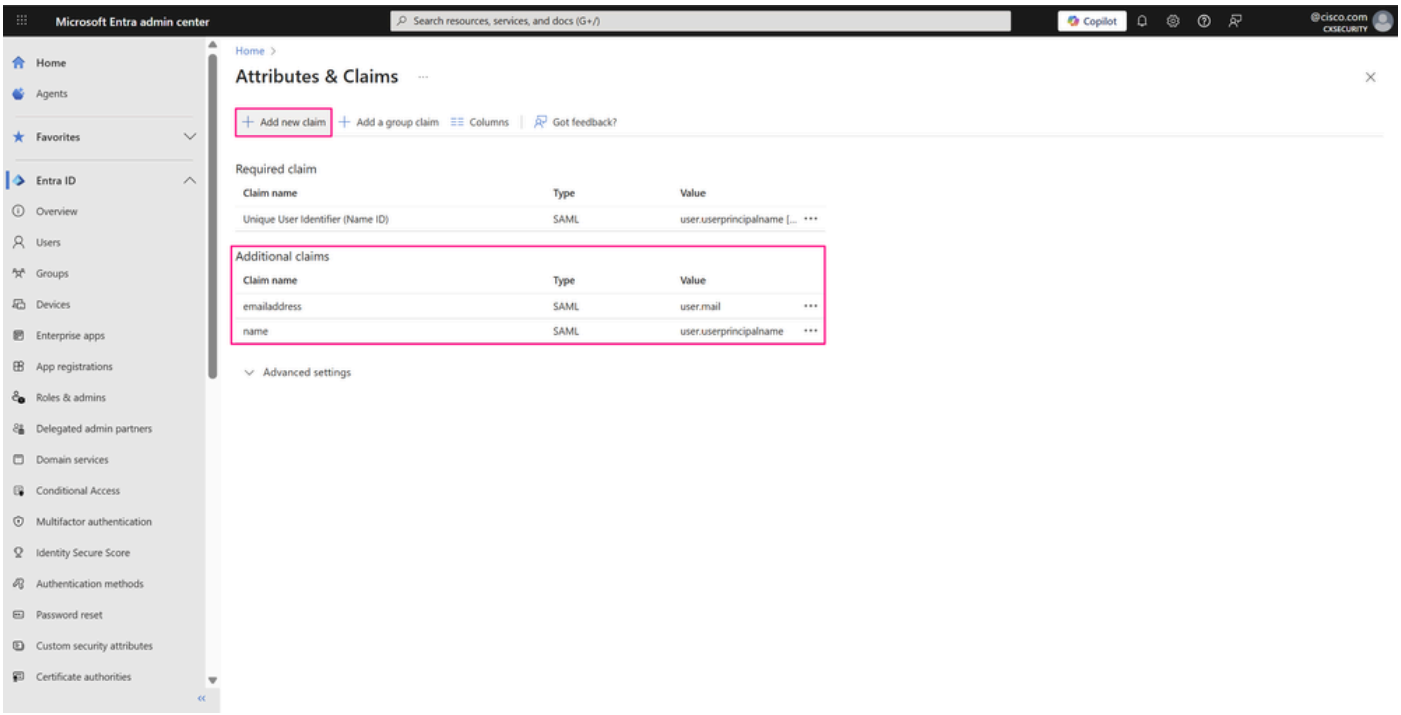
Página Atributos y Reclamaciones

- En la página Administrar notificación, elimine el campo Espacio de nombres y haga clic en Guardar para aplicar los cambios.



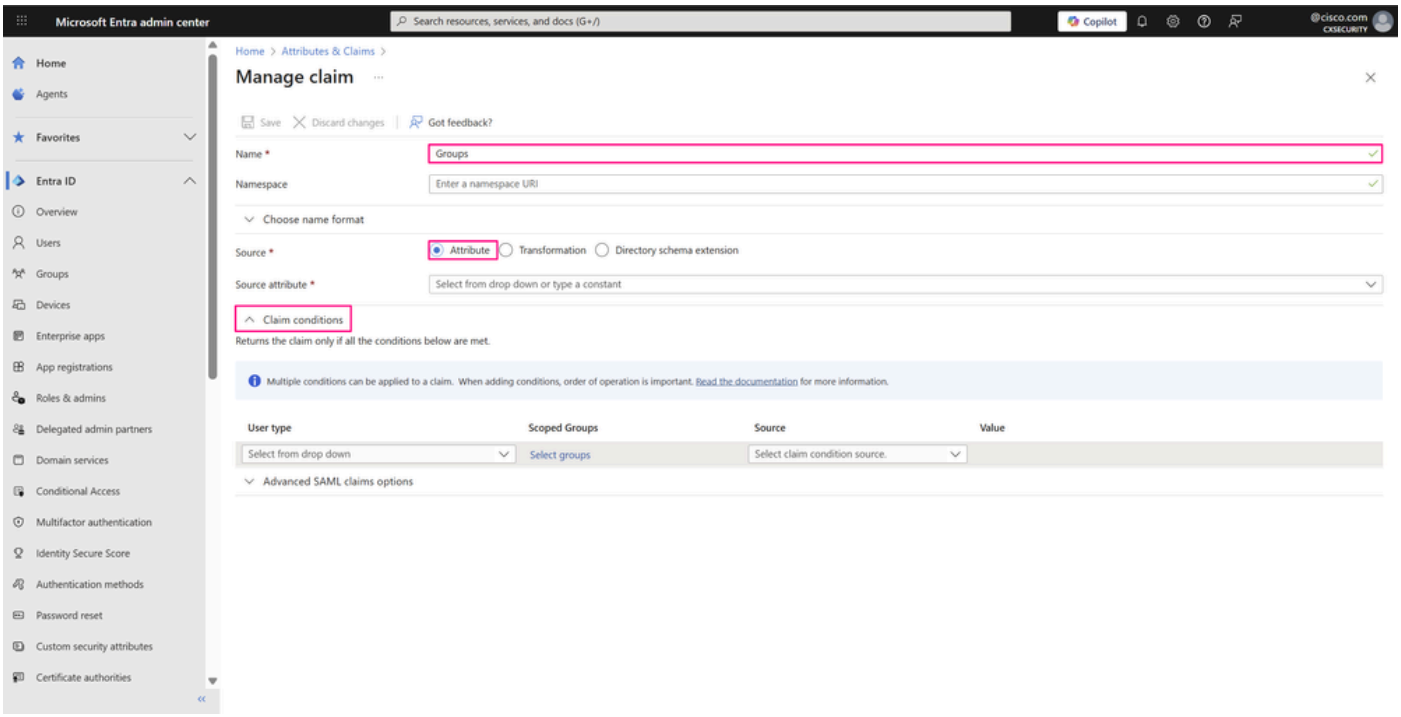
Página Gestionar reclamación

- Ahora se pueden ver los nombres de las dos reclamaciones necesarias. Sin embargo, todavía se necesita una reclamación adicional para definir los grupos a los que pertenecen los usuarios y que están autorizados para acceder a los recursos de la aplicación. Para ello, haga clic en Agregar nueva reclamación.



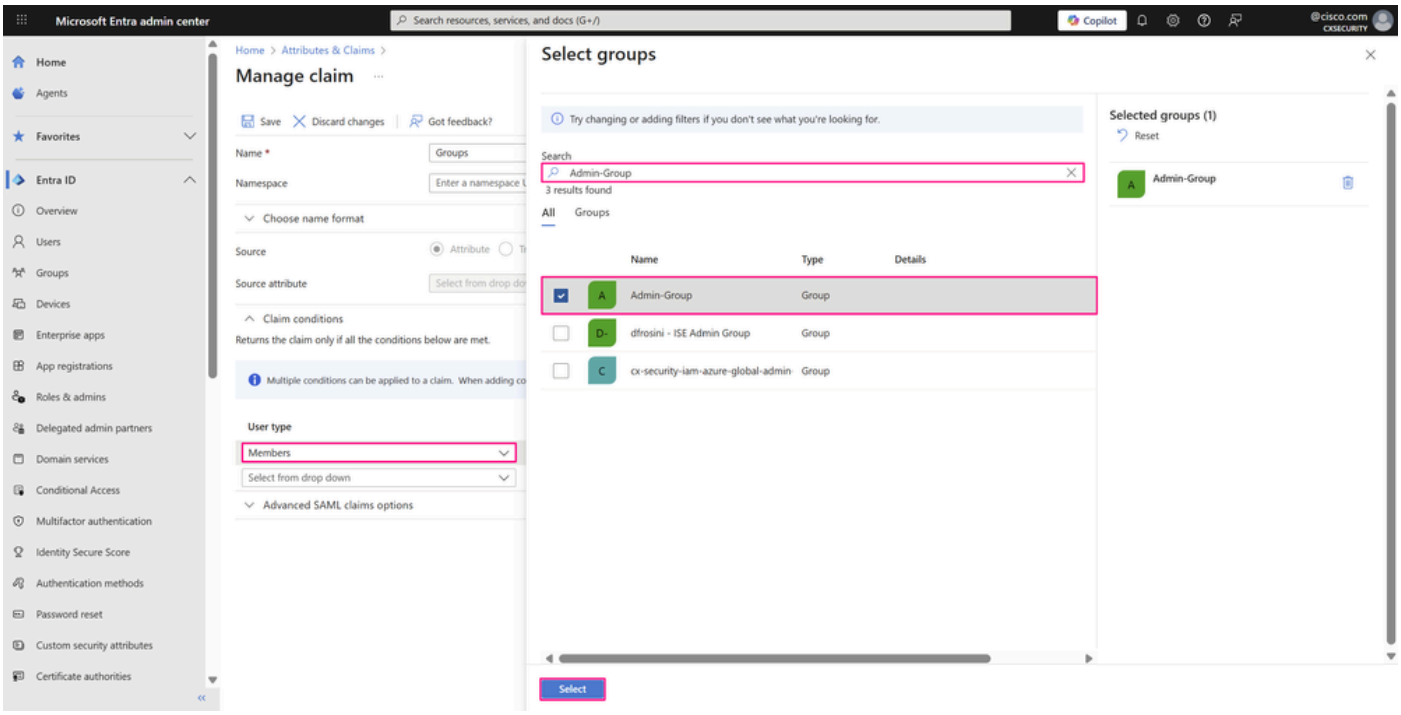
Página Atributos y Reclamaciones

- Introduzca un nombre para identificar esta reclamación. Junto a Origen, seleccione Atributo. A continuación, haga clic en Condiciones de reclamación para ampliar las opciones y configurar varias condiciones.



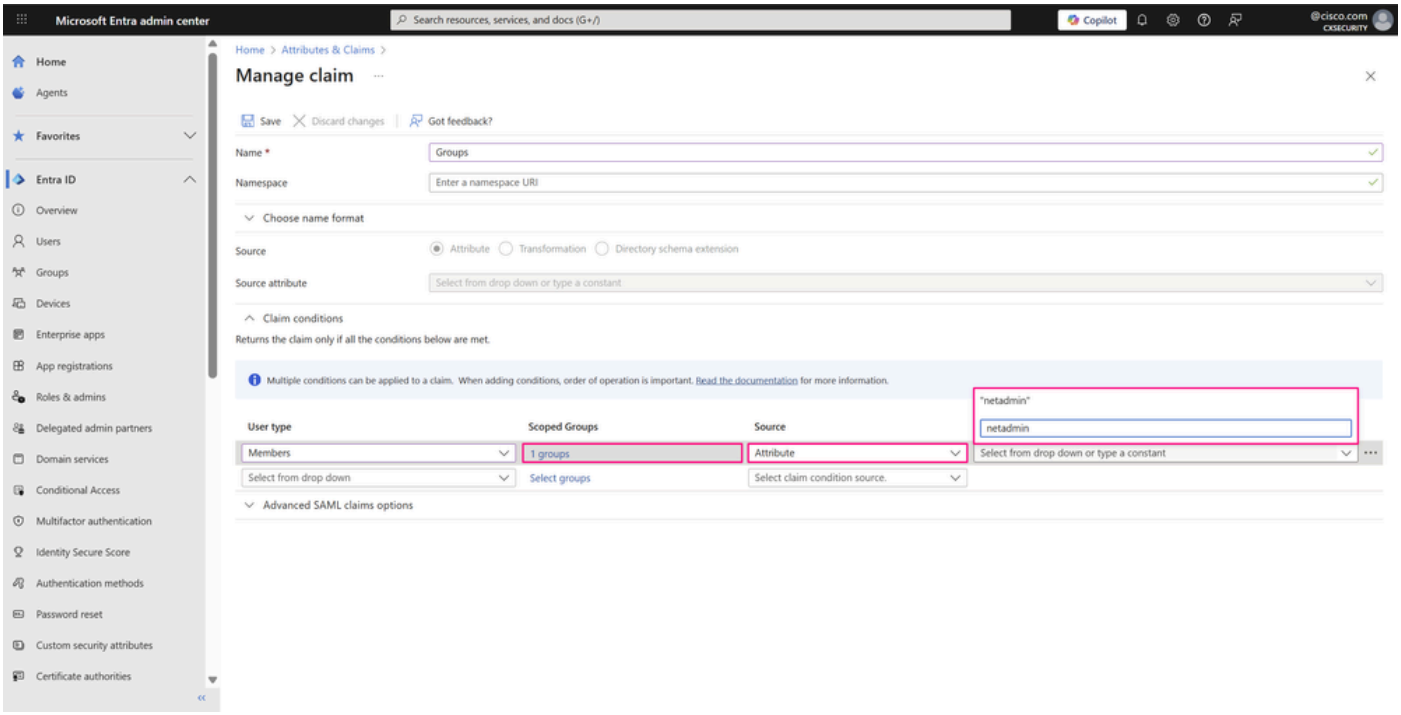
Página Gestionar reclamación

- En la condición de reclamación, elija Miembros en la lista desplegable Tipo de usuario y haga clic en Seleccionar grupos para elegir los grupos a los que debe pertenecer el usuario, luego haga clic en Seleccionar.



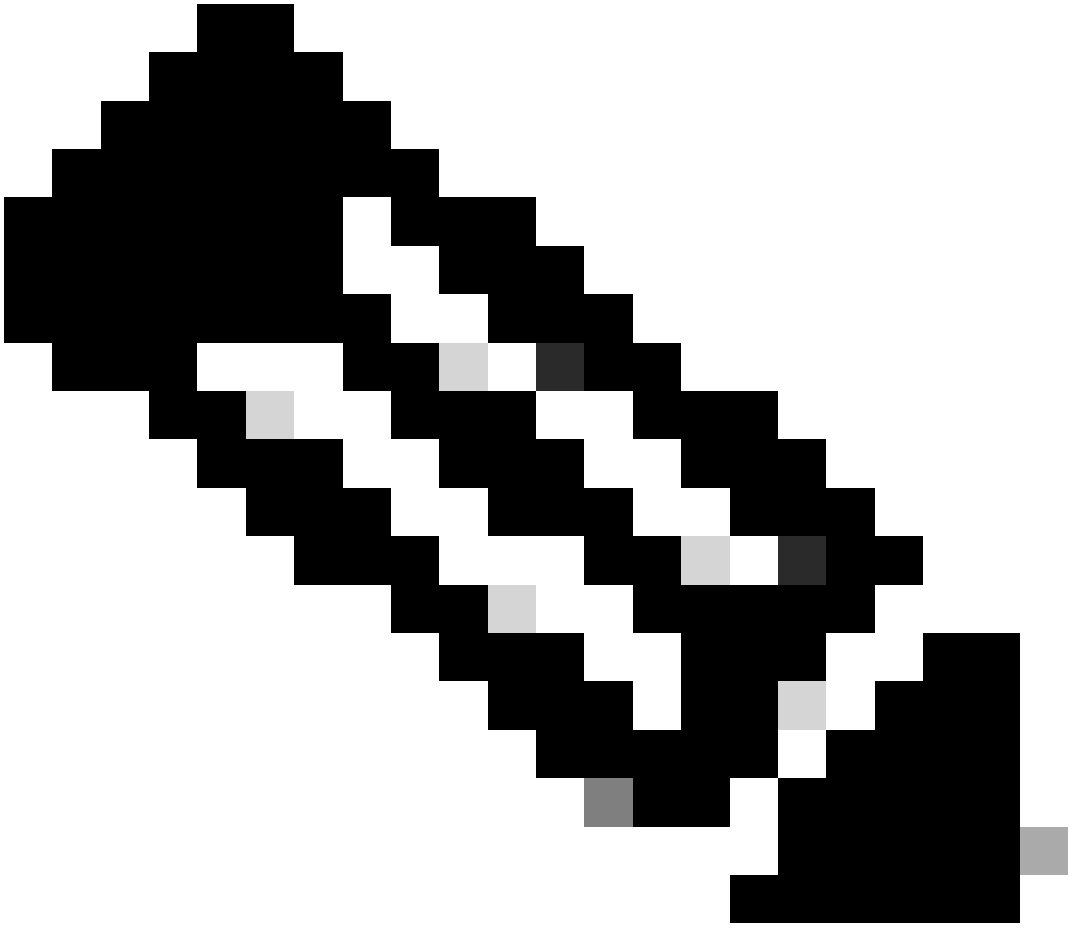
Página Gestionar reclamación

- Elija Attribute en la lista desplegable Source donde la reclamación recupera su valor. En el campo Valor, introduzca el atributo personalizado del usuario que hace referencia al grupo de usuarios definido en la aplicación. En este ejemplo, netadmin es uno de los grupos de usuarios estándar en Cisco SD-WAN Manager. Ingrese el valor del atributo sin comillas y presione Enter.

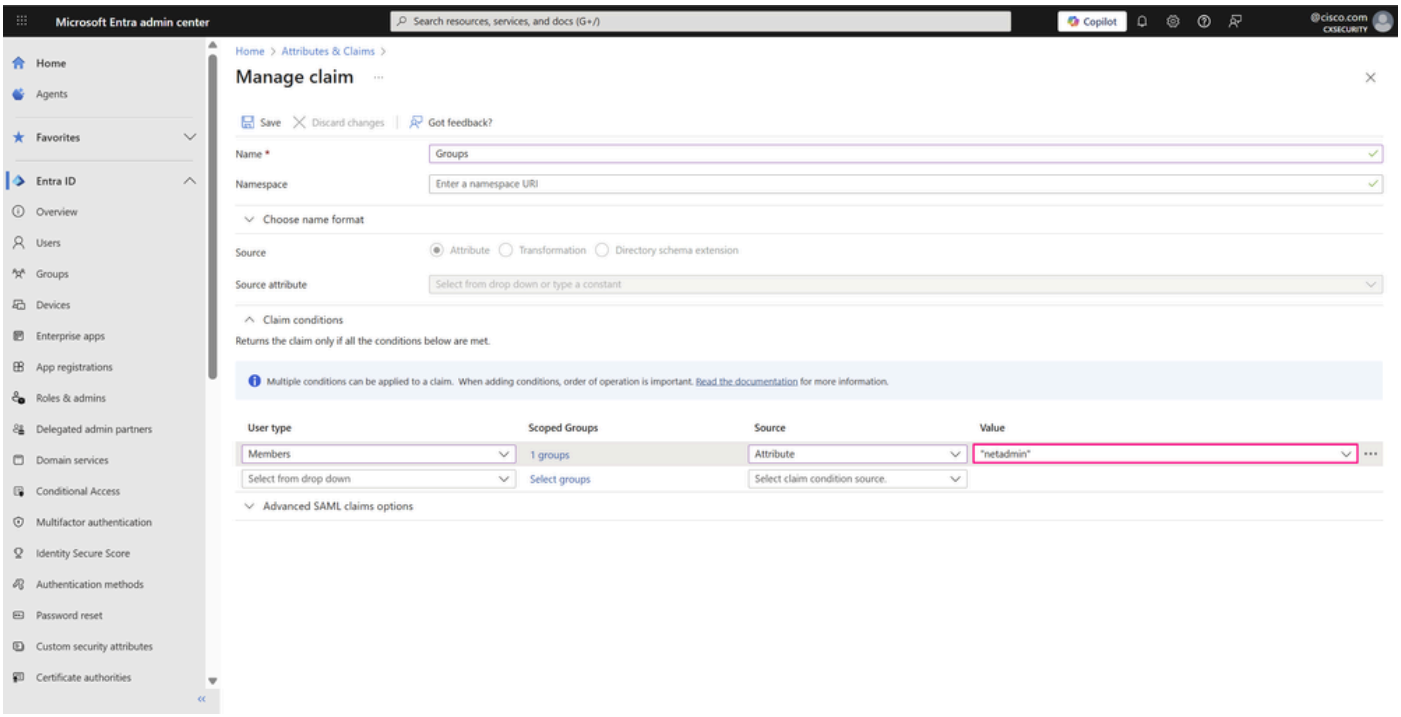


Página Gestionar reclamación

- Inmediatamente después, el valor del atributo aparece entre comillas, ya que Microsoft Entry ID controla este valor como una cadena.

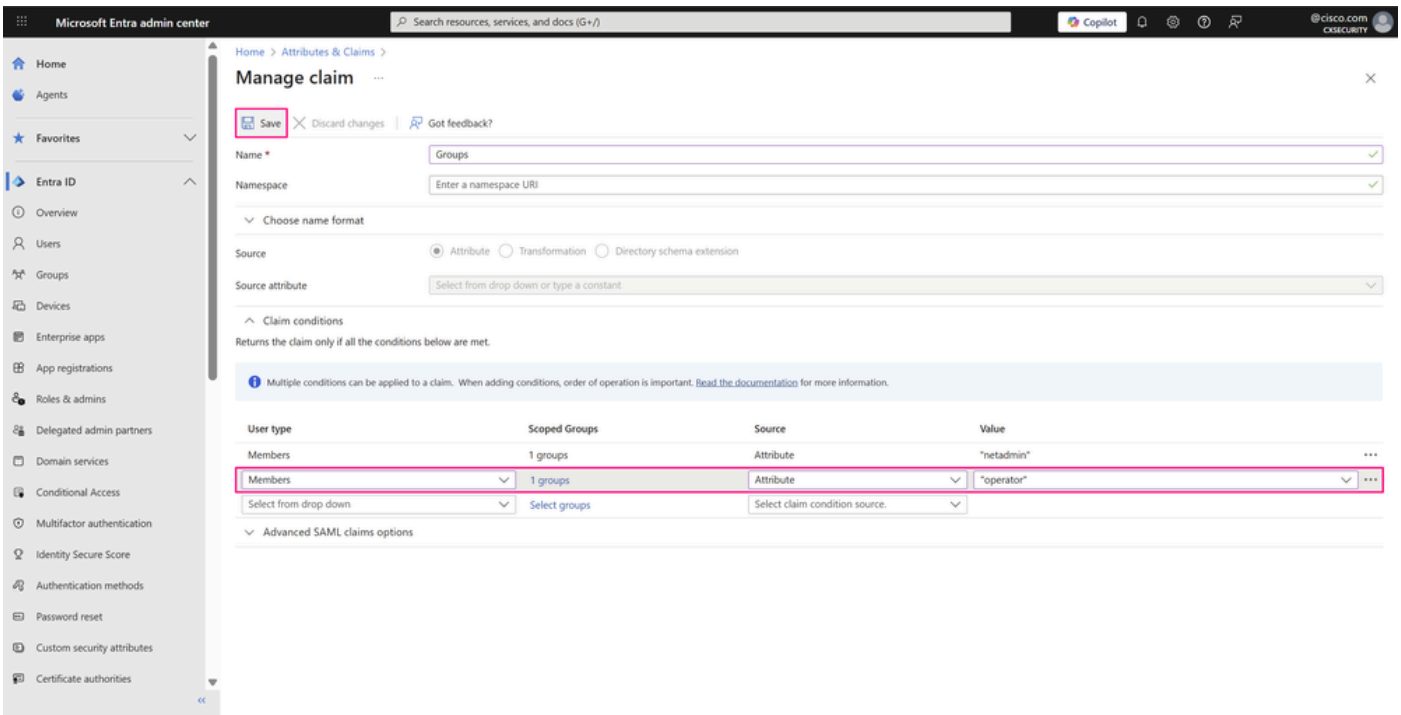


Nota: Estos parámetros de las condiciones de notificación son muy relevantes en la configuración SAML de SSO de la aplicación empresarial, ya que estos atributos personalizados siempre deben coincidir con los grupos de usuarios definidos en Cisco SD-WAN Manager. Esta coincidencia determina los privilegios o permisos concedidos a los usuarios en función del grupo al que pertenecen en Microsoft Entry ID.



Página Gestionar reclamación

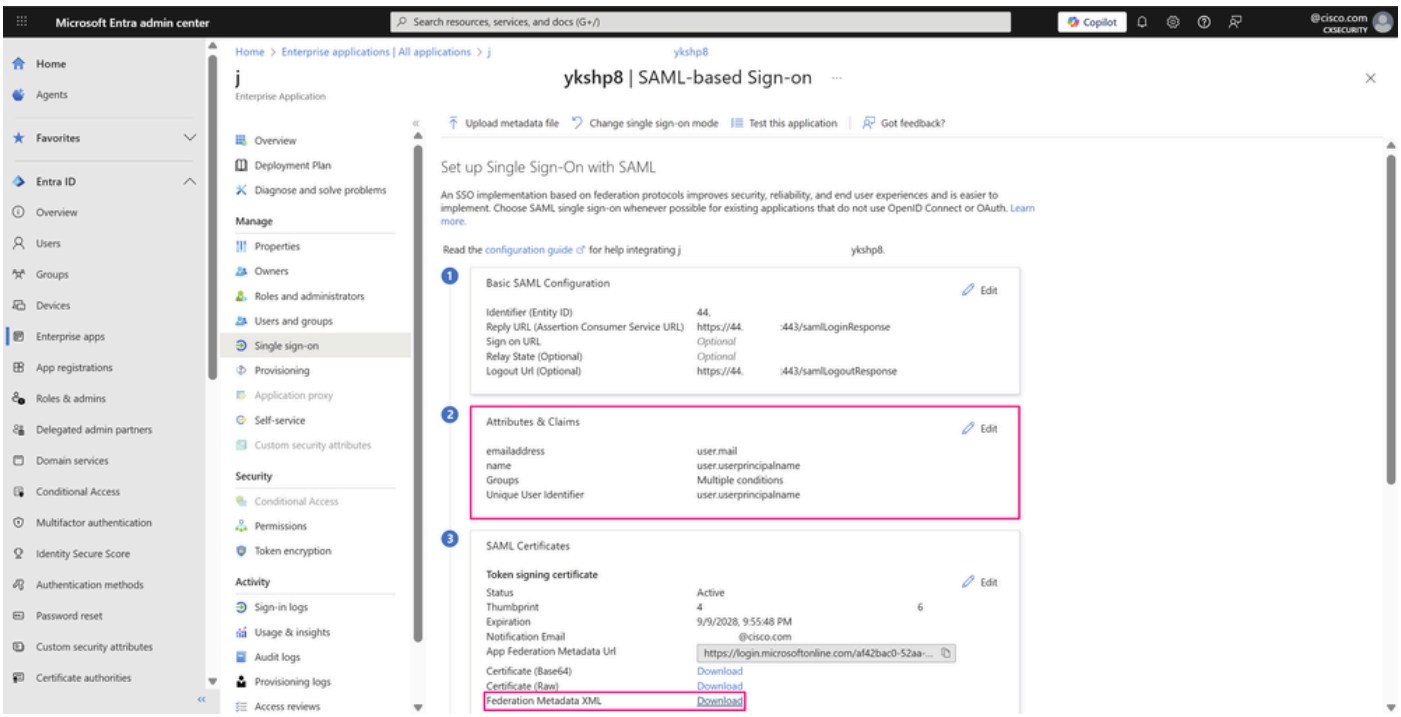
- Repita los mismos pasos para una segunda condición de reclamación para el segundo grupo creado, que se asigna al grupo de usuarios de operador en Cisco SD-WAN Manager. Este proceso es necesario para cada grupo con permisos específicos que desee iniciar sesión en la aplicación. También puede agregar varios grupos dentro de una misma condición. Haga clic en Guardar para guardar los cambios.



Página Gestionar reclamación

- En la página Configurar el inicio de sesión único con SAML, la sección Atributos y reclamaciones muestra los nuevos cambios realizados. Para finalizar la configuración en el

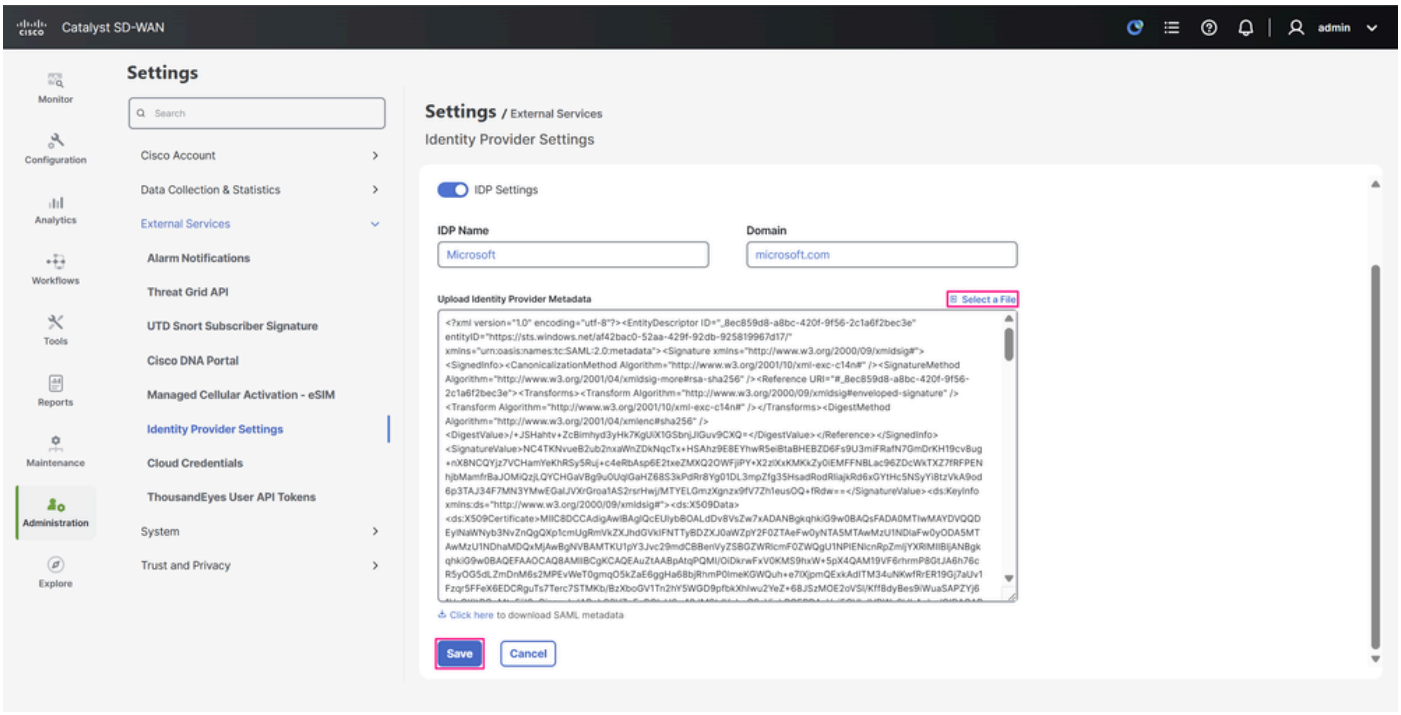
Id. de entrada de Microsoft, en Certificados SAML, haga clic en Descargar junto a XML de metadatos de federación para descargar el archivo XML que proporciona servicios de identidad a la aplicación.



Página SSO con Configuración SAML

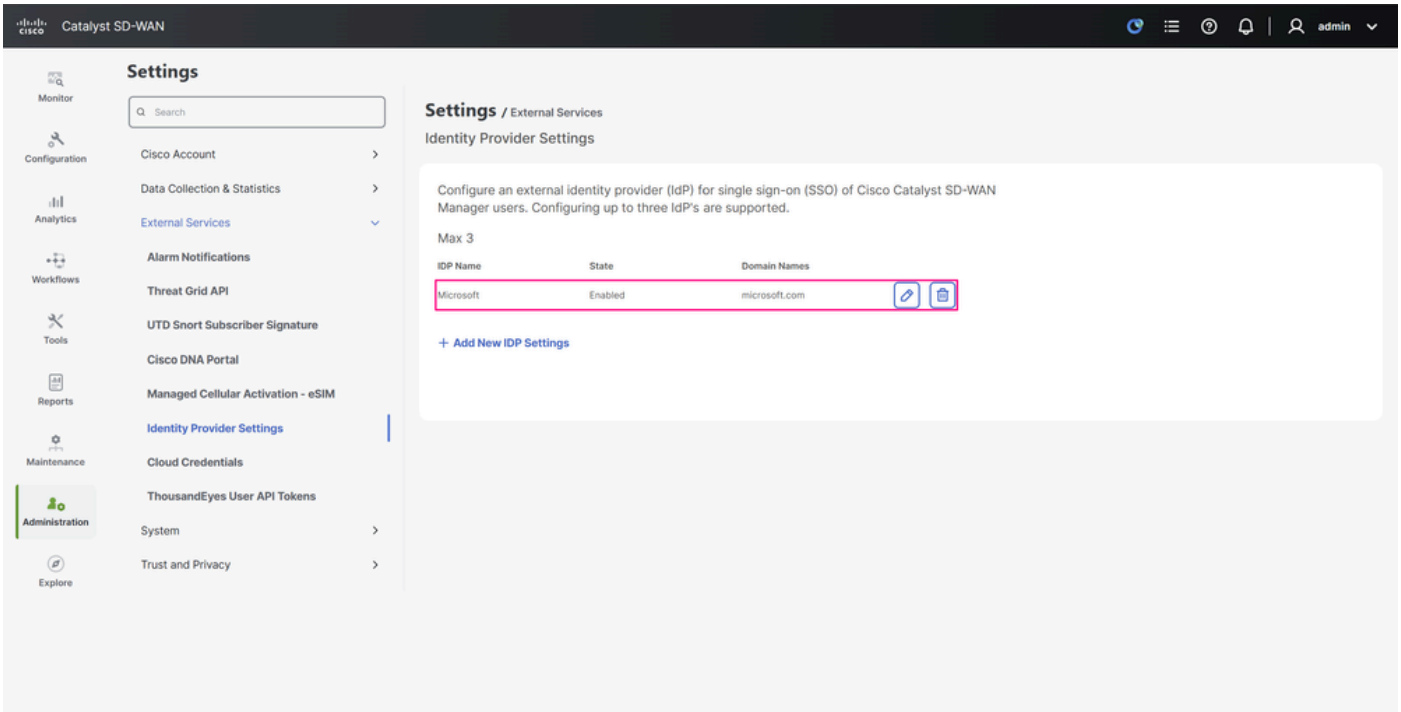
Paso 5. Importe el archivo de metadatos SAML de Microsoft Entra ID en Cisco SD-WAN Manager

- Para cargar los metadatos de federación en el Cisco SD-WAN Manager, navegue hasta Administration > Settings > External Services > Identity Provider Settings y haga clic en Select a file. Elija el archivo que acaba de descargar de Microsoft Entry ID y, a continuación, haga clic en Guardar.



Página Configuración de IdP

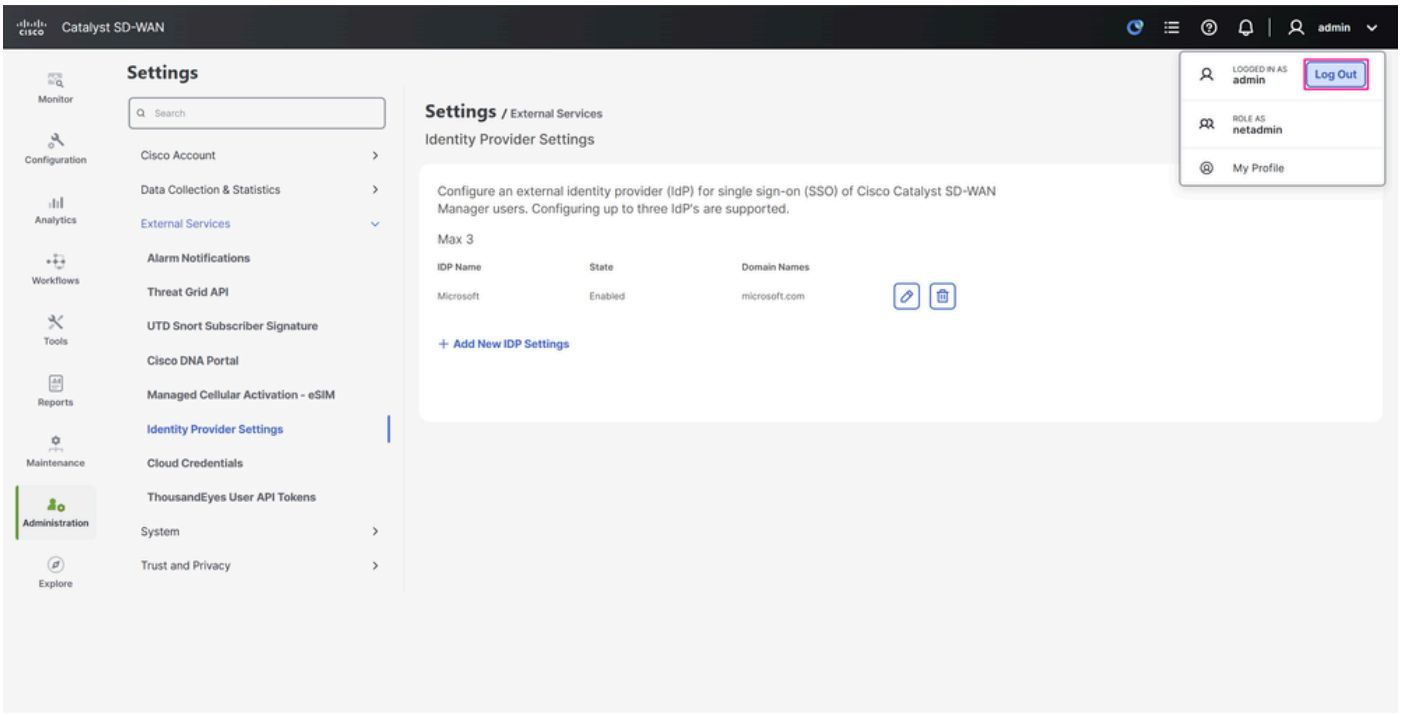
- La configuración de IdP y los metadatos se guardan ahora.



Página Configuración de IdP

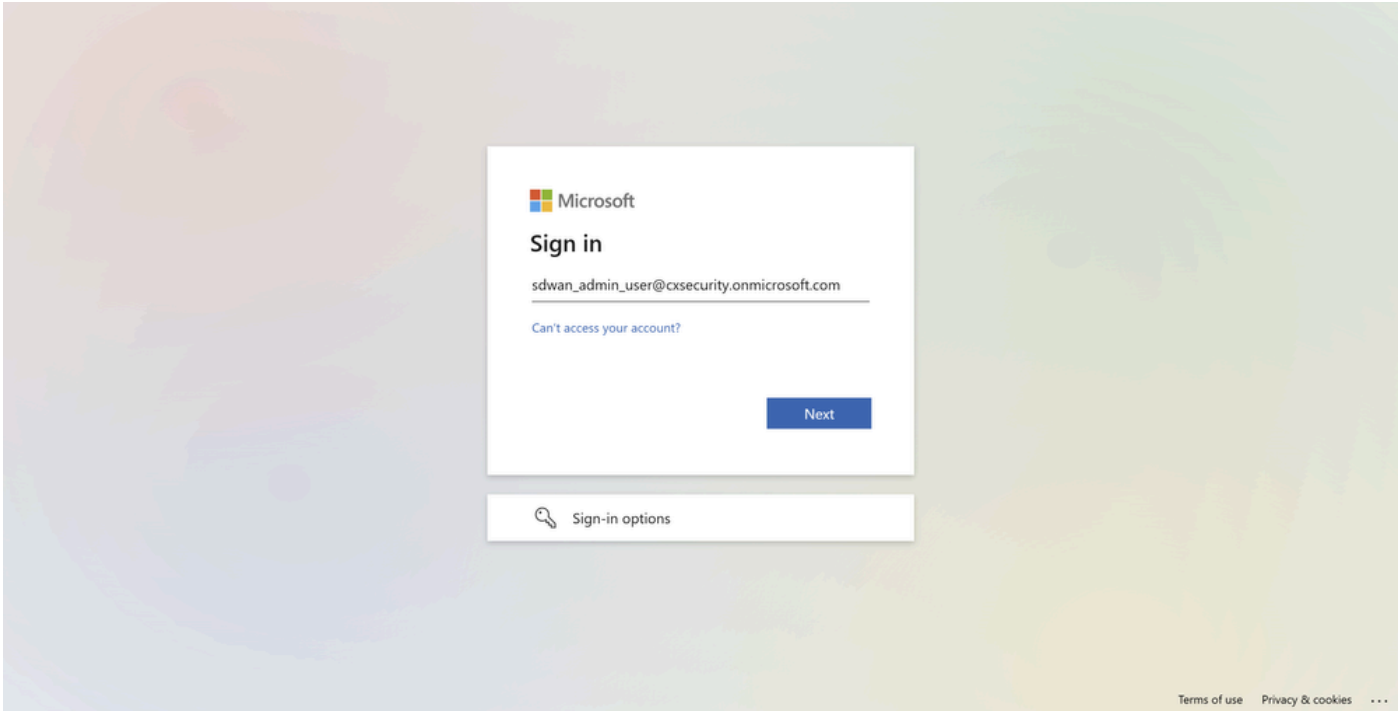
Verificación

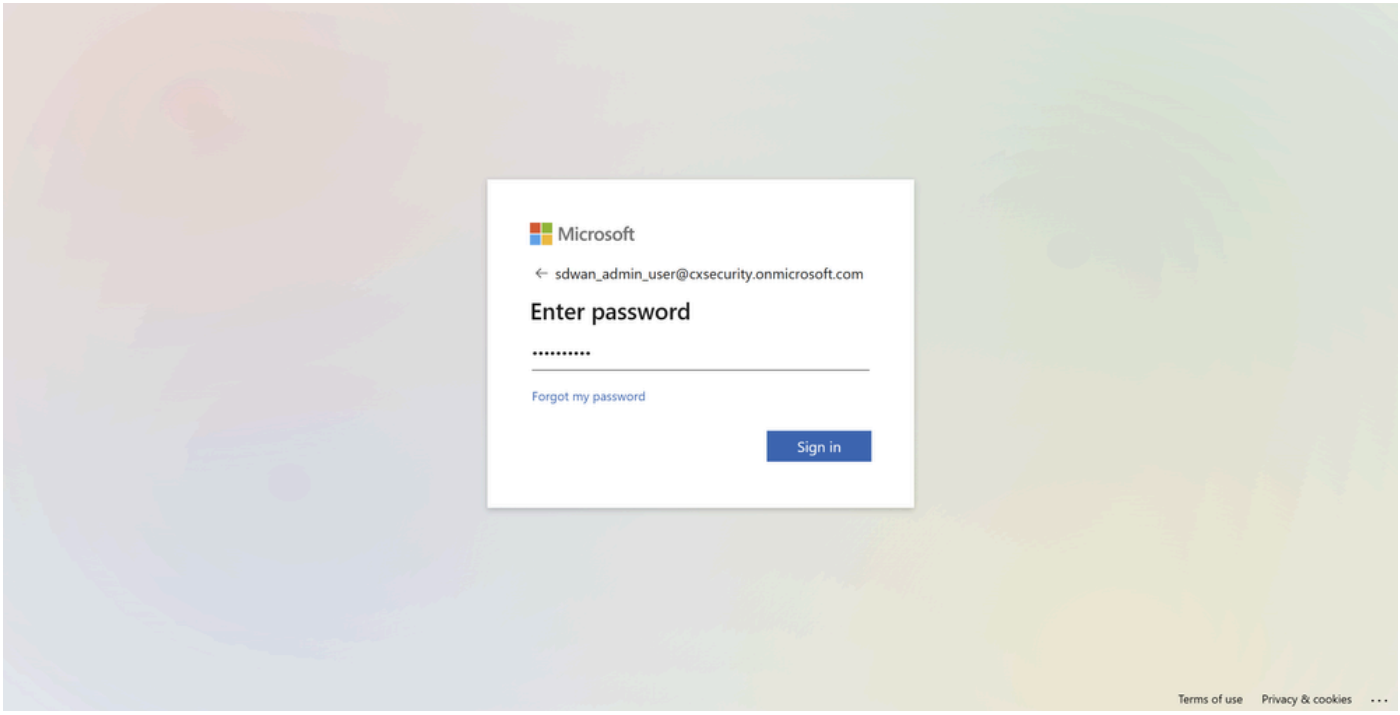
- Haga clic en el nombre del perfil en la esquina superior derecha de la interfaz de usuario para expandir las opciones. A partir de ahí, haga clic en Cerrar sesión para cerrar la sesión del portal.



Menú Perfil

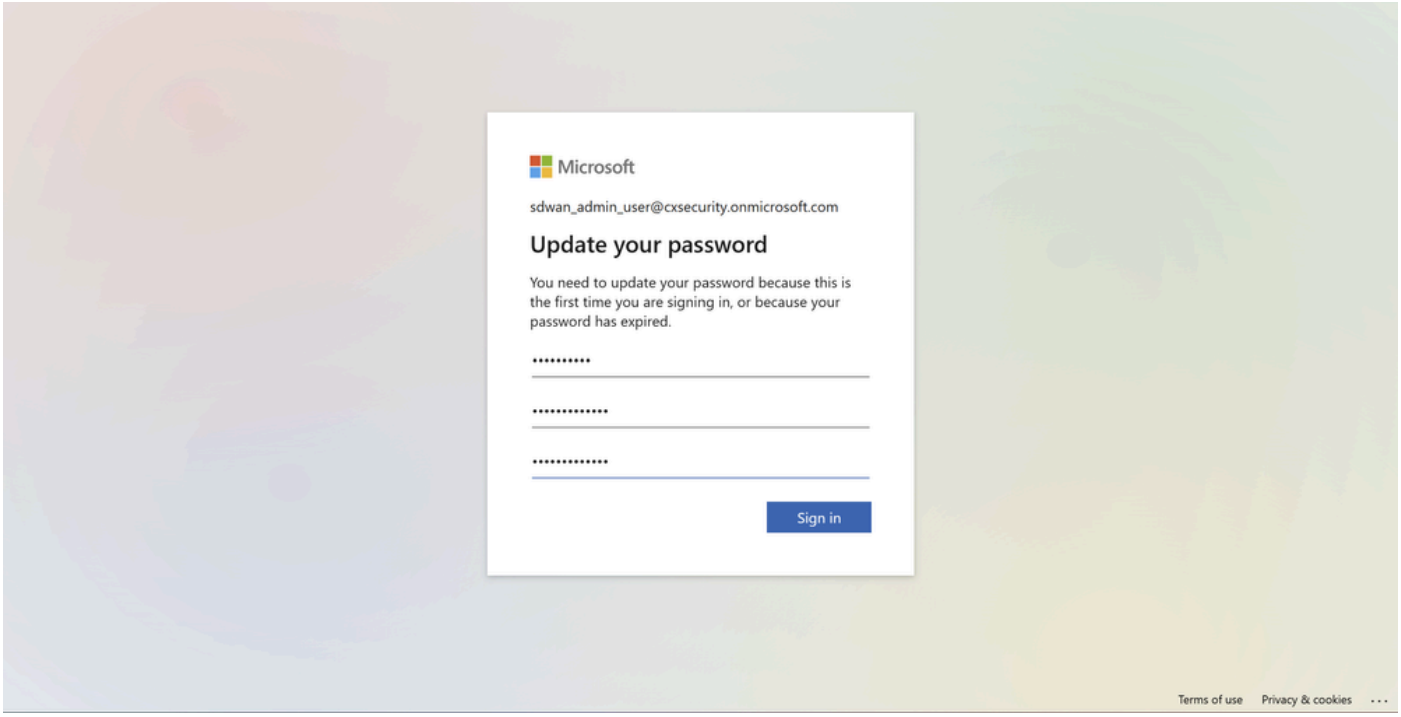
- Se le redirige inmediatamente a la pantalla de autenticación de Microsoft, donde inicia sesión con las credenciales de los usuarios SSO de Microsoft Entra ID.





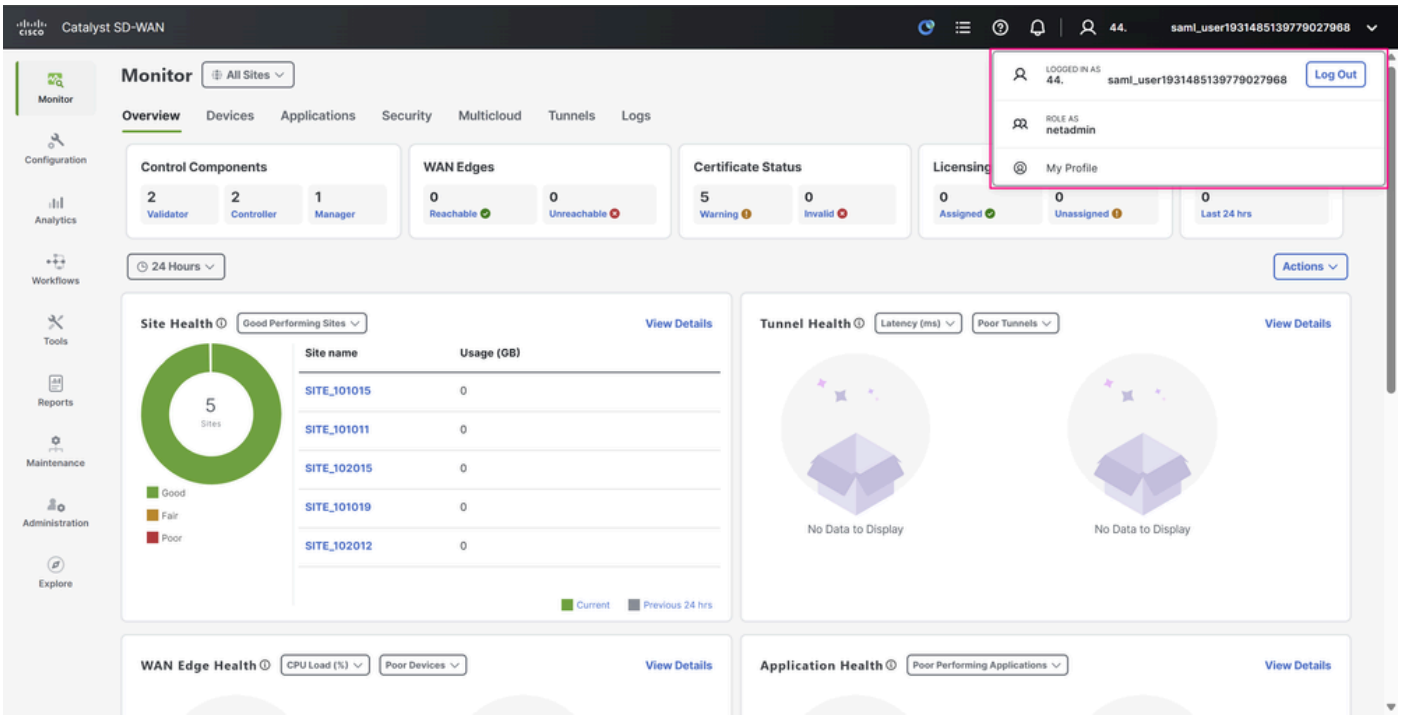
Pantalla de inicio de sesión de Microsoft

- Dado que es la primera vez que el usuario de SSO inicia sesión, el mensaje solicita un cambio de contraseña.



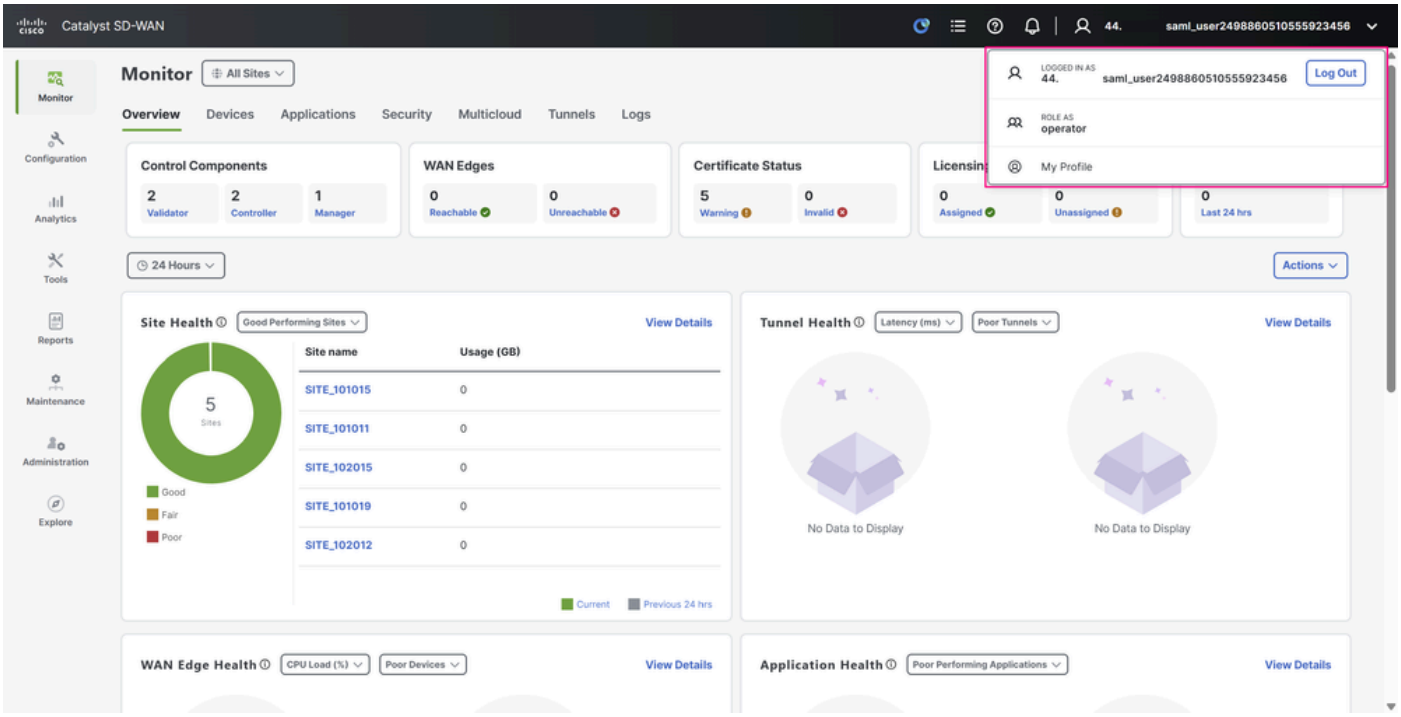
Pantalla de inicio de sesión de Microsoft

- Después de un inicio de sesión correcto, expanda los detalles de su perfil nuevamente en la esquina superior derecha del panel, y puede confirmar que el usuario es detectado con un rol netadmin, exactamente como está configurado en Microsoft Entra ID.



IU de Cisco SD-WAN Manager

- Por último, realice la misma prueba de inicio de sesión con el otro usuario. Verá el mismo comportamiento: el usuario se identifica ahora con la función de operador.



IU de Cisco SD-WAN Manager

Información Relacionada

- [Configuración del inicio de sesión único en Catalyst SD-WAN de Cisco IOS XE]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).