AnyDesk México: Mayorista oficial. Mejor precio y respaldo.

Cómo agregar múltiples usuarios a través de IDP en Anydesk

TABLA DE CONTENIDO

Agrega múltiples usuarios a través de IDP

Requisitos previos

Configurar IDP

Configurar mapeador IDP

Agrega múltiples usuarios a través de IDP

Aplicable para usuarios con una licencia de **Enterprise-Cloud** o **Ultimate-Cloud**.

El proveedor de usuarios **IDP** permite al propietario de una organización crear usuarios para esa organización utilizando un sistema de gestión de identidades que admite OpenID Connect (por ejemplo, Microsoft Azure Active Directory). De esta manera, puede configurar IDP en mi.anydesk II. Los usuarios de su organización podrán iniciar sesión con SSO utilizando la identificación de la organización y las credenciales de su empresa.

En este capítulo, aprenderás los requisitos previos necesarios para la configuración de IDP, cómo configurar IDP a través de la consola de administración de mi.anydesk II y cómo configurar un mapeador IDP.

Para obtener más información sobre los tipos de proveedores de usuarios, consulta Proveedores de Usuarios.

Requisitos previos

Antes de configurar IDP en mi.anydesk II, debes configurar tu proveedor de identidad primero. Puedes utilizar cualquier proveedor de identidad de terceros que admita OpenID Connect, como

Microsoft Azure Active Directory.

Para la configuración de IDP en mi.anydesk II, necesitarás los siguientes datos:

- **Cliente secreto**. Copia y pega la URL en el campo **Cliente Secreto** al configurar la **Configuración de IDP**.
- **Aplicación (ID de Cliente)**. Copia y pega la URL en el campo **ID de Cliente**.
- **Punto de autorización**. Copia y pega la URL en el campo **URL de Autenticación**.
- **Punto de token**. Copia y pega la URL en el campo **URL del Token**.

Configurar IDP

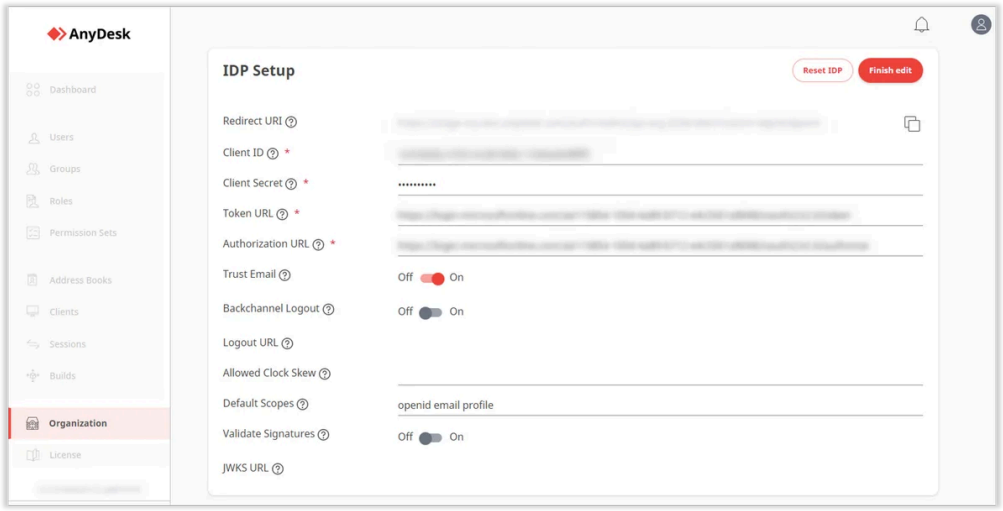
Debes configurar IDP para crear una conexión entre mi.anydesk II y tu proveedor de identidad.

❗ No podrás editar usuarios en mi.anydesk II creados a través de IDP ya que se sincronizan con el proveedor de identidad.

Para configurar IDP en mi.anydesk II:

1. Abre mi.anydesk II y ve a **Organización**.
2. En la sección **General**, haz clic en **Editar**. En el campo **Proveedor de Usuarios**, selecciona **IDP**.
3. En la ventana **Cambiar proveedor activo**, selecciona **Continuar**.
4. Desplázate hacia abajo hasta la sección **Configuración de IDP**, haz clic en **Editar** y proporciona la siguiente información:
    - **URI de Redireccionamiento** - Se genera automáticamente al completar la configuración de IDP. Copia el valor de la URI de Redireccionamiento después de finalizar la configuración y pégalo en tu proveedor de identidad correspondiente.
    - **ID de Cliente** - Copia el valor **Aplicación (ID de Cliente)** de tu IDP y pégalo aquí. Se utiliza para registrar mi.anydesk como un cliente OIDC con tu proveedor.
    - **Cliente Secreto** - Copia el valor **Cliente Secreto** de tu IDP y pégalo aquí. Se utiliza para registrar mi.anydesk como un cliente OIDC con tu proveedor.
    - **URL del Token** - Copia el valor **Punto de token** de tu IDP y pégalo aquí. Devuelve los tokens de acceso, tokens de ID y tokens de actualización al cliente (mi.anydesk).
    - **URL de Autorización** - Copia el valor **Punto de autorización** de tu IDP y pégalo aquí. Se utiliza para la autenticación y autorización del cliente mi.anydesk.
    - **Confianza en el Correo Electrónico** - Desactiva el interruptor para permitir que los usuarios verifiquen su dirección de correo electrónico a través de mi.anydesk II. Activa el interruptor para deshabilitar la verificación de correo electrónico de mi.anydesk II.

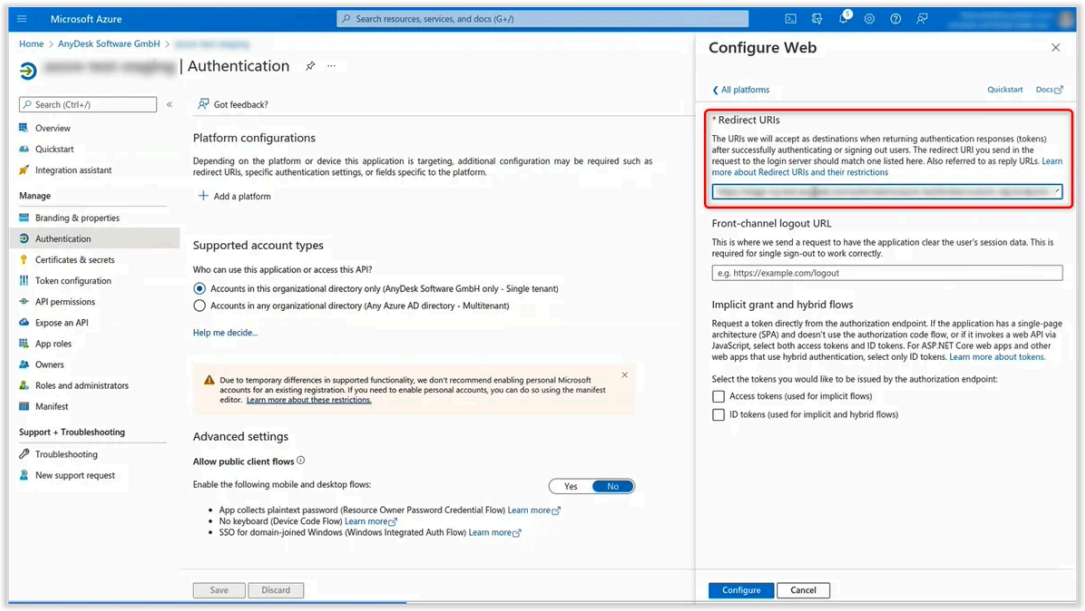
- **Cierre de Sesión de Backchannel** - Activa el interruptor para habilitar el soporte de cierre de sesión de backchannel por parte del IDP configurado. Si está habilitado, se debe proporcionar el campo **URL de Cierre de Sesión**.
- **URL de Cierre de Sesión** - Proporciona el punto final para cerrar la sesión de los usuarios del IDP externo. Debe estar habilitada la opción **Cierre de Sesión de Backchannel**.
- **Permitir Desviación de Reloj** - Proporciona el valor en segundos (el valor predeterminado es *0*). Determina la desviación aceptable al validar los tokens de IDP.
- **Alcances Predeterminados** - Los alcances incluidos al solicitar la autorización. El valor predeterminado es *openid*. Proporciona una lista separada por comas de alcances adicionales que deseas solicitar.
- **Validar Firmas** - Activa el interruptor para habilitar la validación de firmas del IDP configurado. Si está habilitado, se debe proporcionar el campo **URL JWKS**.
- **URL JWKS** - URL donde mi.anydesk II puede recuperar las claves del IDP configurado. Debe estar habilitada la opción **Validar Firmas**.



Configuración de IDP

5. Haz clic en **Finalizar edición**.
6. Después de guardar el proveedor de identidad, copia la **URI de Redireccionamiento** asignada.
7. Abre tu proveedor de identidad y ve a **Autenticación**.

   ❗ En este ejemplo, se utiliza Microsoft AzureAD como proveedor de identidad para mostrar el procedimiento. Puedes usar cualquier otro proveedor de identidad de terceros.
8. Haz clic en **Agregar una plataforma**, selecciona **Web** y pega la **URI de Redireccionamiento** que copiaste después de guardar el proveedor de identidad en [mi.anydesk II].



URI de Redireccionamiento

9. Haz clic en **Configurar**.

Después de completar los pasos anteriores, todos los usuarios de tu proveedor de identidad podrán iniciar sesión en mi.anydesk II con SSO utilizando la ID de la organización.

Configurar mapeador IDP

Puedes asignar roles de tu organización a usuarios en mi.anydesk II. De esta manera, no necesitarás asignar roles a los usuarios manualmente.

Primero, debes configurar un token de grupo en tu proveedor de identidad. Luego, para configurar el mapeador IDP, debe existir al menos un rol en la consola de administración de mi.anydesk II. Este rol se puede asignar a un rol dentro del proveedor de identidad.

Después de asignar el/los rol(es), su estado cambiará a *mapeado*. Esto significa que ya no se pueden vincular usuarios manualmente a ese rol. Eliminar el mapeador IDP eliminará el estado **mapeado**, lo que te permitirá vincular usuarios manualmente a ese rol.