Añadir múltiples usuarios a través de IDP: Guía paso a paso con AnyDesk

TABLA DE CONTENIDO

Añadir múltiples usuarios a través de IDP

Pre-requisitos

- Configurar IDP
- Configurar mapeador de IDP

Añadir múltiples usuarios a través de IDP

Aplicable para usuarios con una licencia **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 administración de identidad que admite OpenID Connect (por ejemplo, Microsoft Azure Active Directory). De esta manera, puedes configurar IDP en mi.anydesk II. Los usuarios de tu organización podrán iniciar sesión con SSO utilizando la identificación de la organización y las credenciales de su empresa.

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

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

Pre-requisitos

Antes de configurar IDP en mi.anydesk II, primero debes configurar tu proveedor de identidad. 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:

- **Secreto del Cliente.** Copia y pega la URL en el campo **Secreto del Cliente** al configurar **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 de Token**.

Configurar IDP

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

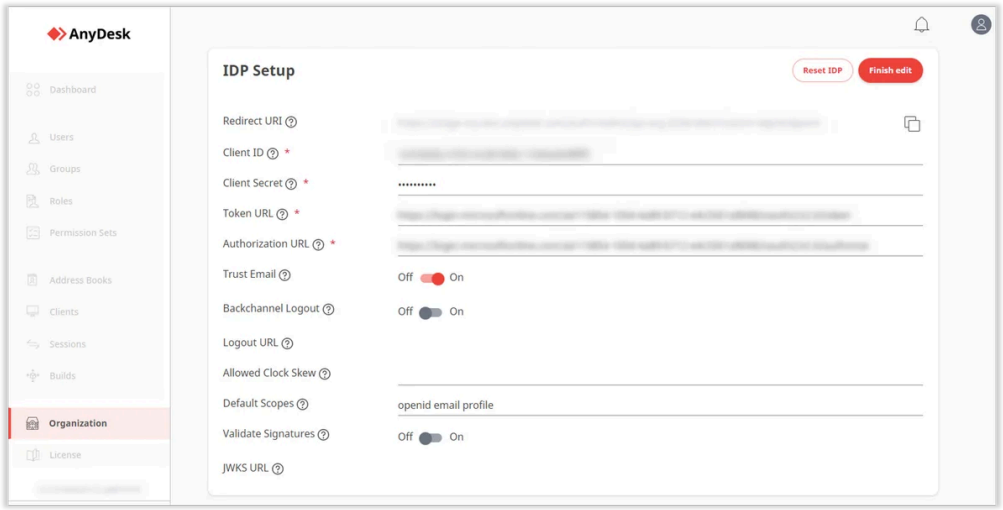
❗ No podrás editar los usuarios en mi.anydesk II creados a través de IDP, ya que se sincronizan con el proveedor de identidad.

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 Redirección** - Se genera automáticamente cuando se completa la configuración de IDP. Copia el valor de la URI de Redirección después de finalizar la configuración y pégalo en tu proveedor de identidad correspondiente.
    - **ID de Cliente** - Copia el valor de **Aplicación (ID de Cliente)** de tu proveedor de identidad y pégalo aquí. Se utiliza para registrar mi.anydesk como un cliente OIDC en tu proveedor.
    - **Secreto del Cliente** - Copia el valor de **Secreto del Cliente** de tu proveedor de identidad y pégalo aquí. Se utiliza para registrar mi.anydesk como un cliente OIDC en tu proveedor.
    - **URL de Token** - Copia el valor de **Punto de Token** de tu proveedor de identidad 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 de **Punto de Autorización** de tu proveedor de identidad y pégalo aquí. Se utiliza para la autenticación y autorización del cliente mi.anydesk.
    - **Confiar en Email** - 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.

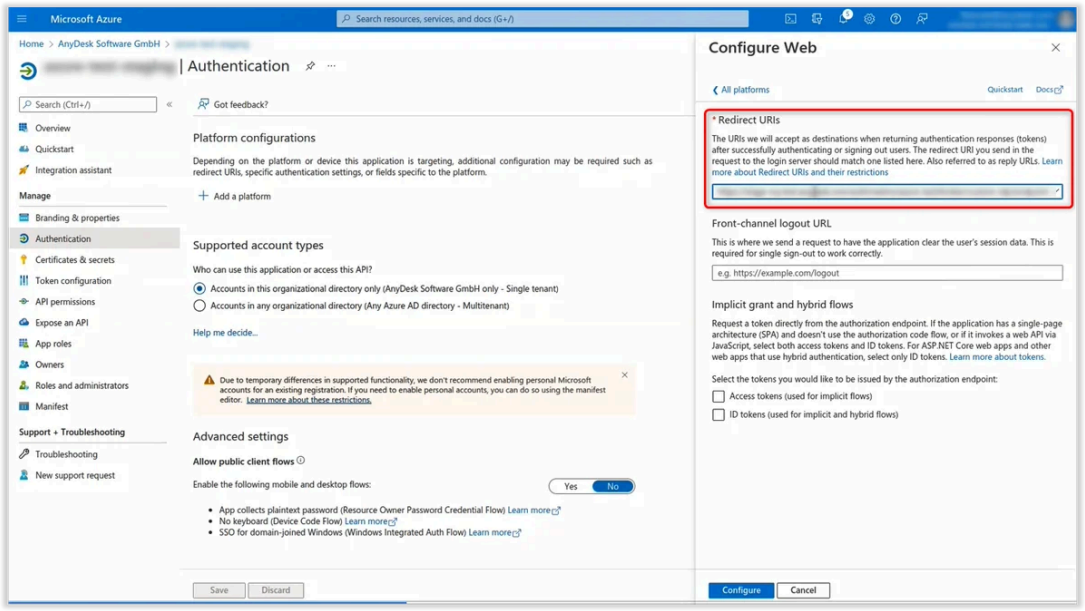
- **Cierre de Sesión en Segundo Plano** - Activa el interruptor para habilitar el soporte de cierre de sesión en segundo plano por parte de IDP configurado. Si está habilitado, se debe proporcionar el campo **URL de Cierre de Sesión**.
- **URL de Cierre de Sesión** - Proporciona el punto final para cerrar la sesión de los usuarios desde IDP externo. **Cierre de Sesión en Segundo Plano** debe estar habilitado.
- **Diferencia de Tiempo Permitida** - Proporciona el valor en segundos (el valor predeterminado es *0*). Determina el margen de tiempo aceptable al validar los tokens de IDP.
- **Alcance Predeterminado** - Los alcances incluidos al solicitar autorización. El 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 firma del IDP configurado. Si está habilitado, se debe proporcionar el campo **URL de JWKS**.
- **URL de JWKS** - URL donde mi.anydesk II puede obtener las claves para el IDP configurado. **Validar Firmas** debe estar habilitado.



configuracion_idp

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

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



uri_redireccion

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 identificación de la organización.

Configurar mapeador de IDP

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

Primero, debes configurar un token de grupo en tu proveedor de identidad. Luego, para configurar el mapeador de IDP, ya debe existir al menos un rol en la consola de administración de mi.anydesk II. Este rol luego 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 los usuarios ya no se pueden vincular manualmente a ese rol. Eliminar el mapeador de IDP eliminará el estado **mapeado**, lo que te permitirá vincular manualmente usuarios a ese rol.