AnyDesk Colombia

Agrega múltiples usuarios a través de IDP: Guía de configuración para licencias Enterprise-Cloud y Ultimate-Cloud

TABLA DE CONTENIDO

Agrega múltiples usuarios a través de IDP

Prerrequisitos

- Configurar IDP

Configurar el mapeador de IDP

Agrega 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 gestión de identidades que admite OpenID Connect (por ejemplo, Microsoft Azure Active Directory). De esta manera, puedes configurar IDP en my.anydesk II. Los usuarios de tu organización podrán iniciar sesión con SSO utilizando la ID de la organización y sus credenciales de la empresa.
En este capítulo, aprenderás qué prerrequisitos son necesarios para la configuración de IDP, cómo configurar IDP a través de la consola de gestión my.anydesk y cómo configurar un mapeador de IDP.

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

Prerrequisitos

Antes de configurar IDP en my.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 my.anydesk II, necesitarás los siguientes datos:

- **Secreto del cliente.** Copia y pega la URL en el campo **Secreto del cliente** al configurar la **Configuración de IDP**.
- **Aplicación (ID de cliente).** Copia y pega la URL en el campo **ID de cliente**.
- **Punto de conexión de autorización.** Copia y pega la URL en el campo **URL de autenticación**.
- **Punto de conexión del token.** Copia y pega la URL en el campo **URL de token**.

Configurar IDP

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

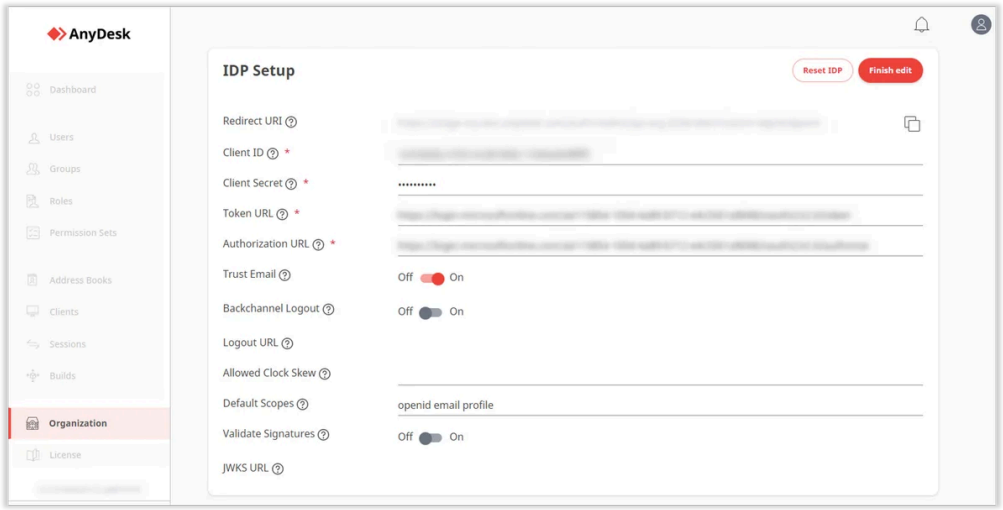
❗ No podrás editar usuarios en my.anydesk II creados a través de IDP, ya que están sincronizados con el proveedor de identidad.

Para configurar IDP en my.anydesk II:

1. Abre my.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 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 proveedor de identidad y pégalo aquí. Se utiliza para registrar my.anydesk como cliente de OIDC con tu proveedor.
    - **Secreto del cliente** - Copia el valor **Secreto del cliente** de tu proveedor de identidad y pégalo aquí. Se utiliza para registrar my.anydesk como cliente de OIDC con tu proveedor.
    - **URL de token** - Copia el valor **Punto de conexión del token** de tu proveedor de identidad y pégalo aquí. Devuelve los tokens de acceso, los tokens de ID y los tokens de actualización al cliente (my.anydesk).
    - **URL de autorización** - Copia el valor **Punto de conexión de autorización** de tu proveedor de identidad y pégalo aquí. Se utiliza para la autenticación y autorización del cliente my.anydesk.
    - **Confianza de correo electrónico** - Desactiva el interruptor para permitir que los usuarios verifiquen su dirección de correo electrónico a través de my.anydesk II. Activa el

interruptor para desactivar la verificación de correo electrónico de my.anydesk II.

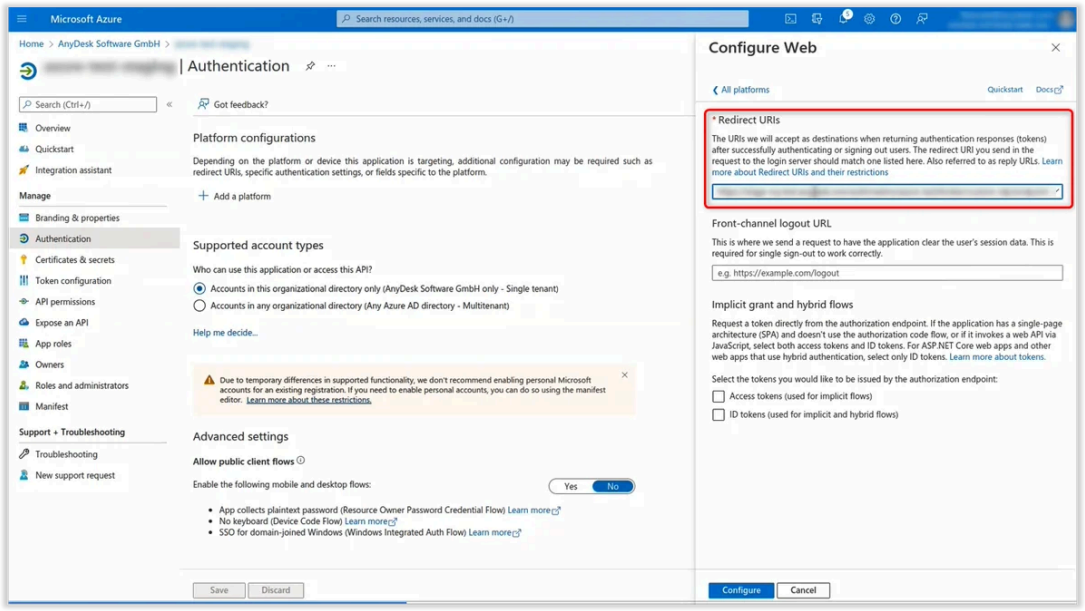
- **Cierre de sesión en segundo plano** - Activa el interruptor para habilitar el soporte de cierre de sesión en segundo plano por el IDP configurado. Si está habilitado, se debe proporcionar el campo **URL de cierre de sesión**.
- **URL de cierre de sesión** - Proporciona el punto de conexión para cerrar sesión a los usuarios desde el IDP externo. Se debe habilitar **Cierre de sesión en segundo plano**.
- **Margen de tolerancia permitido** - Proporciona un valor en segundos (el valor predeterminado es *0*). Determina el margen de tolerancia aceptable al validar los tokens de IDP.
- **Ámbitos por defecto** - Los ámbitos incluidos al solicitar autorización. El valor predeterminado es *openid*. Proporciona una lista separada por comas de ámbitos adicionales que deseas solicitar.
- **Validación de 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 my.anydesk II puede obtener las claves para el IDP configurado. Se debe habilitar la **Validación de 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 el proveedor de identidad 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 redireccionamiento** que copiaste después de guardar el proveedor de identidad en [my.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 my.anydesk II con SSO utilizando la ID de la organización.

Configurar el mapeador de IDP

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

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

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