Agregar múltiples usuarios vía IDP

TABLA DE CONTENIDO

Prerrequisitos

Configurar IDP

Configurar mapeador IDP

> **Licencia:** Ultimate-Cloud
>
> **Relevante para:** Dueño de organización o Admin

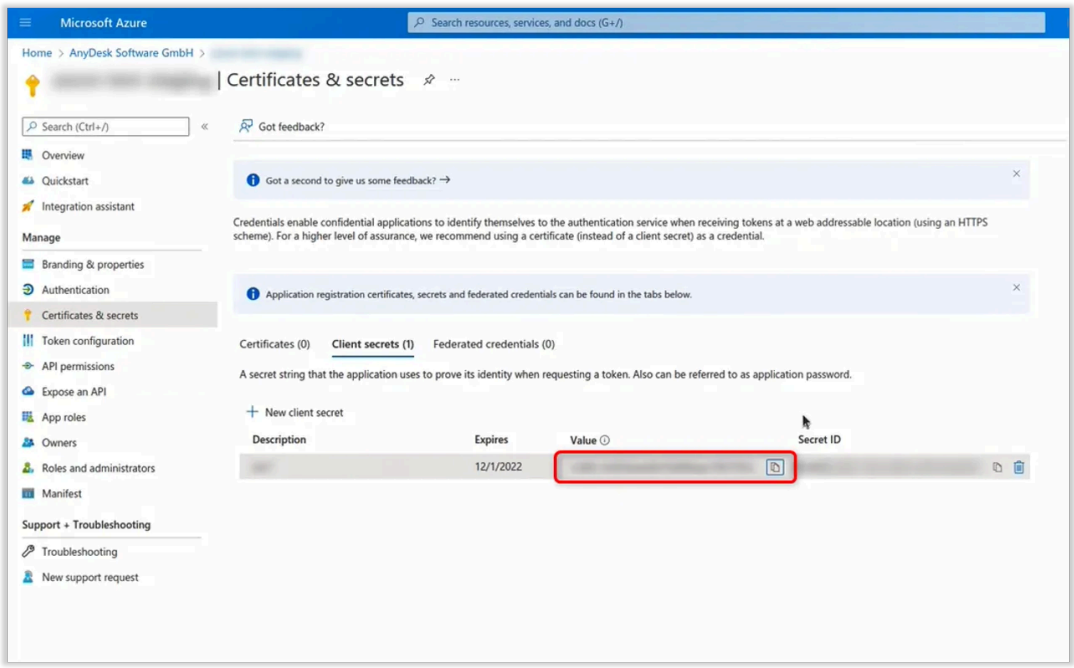
El proveedor de usuarios **IDP** permite a los dueños de organizaciones crear usuarios a través de un proveedor de identidad (IDP) que soporte OpenID Connect, como Microsoft Azure Active Directory. Una vez configurado en my.anydesk II, los usuarios pueden iniciar sesión con SSO usando sus credenciales corporativas y el ID de la organización.

> 🦉 Para más detalles sobre los tipos de proveedores de usuarios, vea **este artículo**.

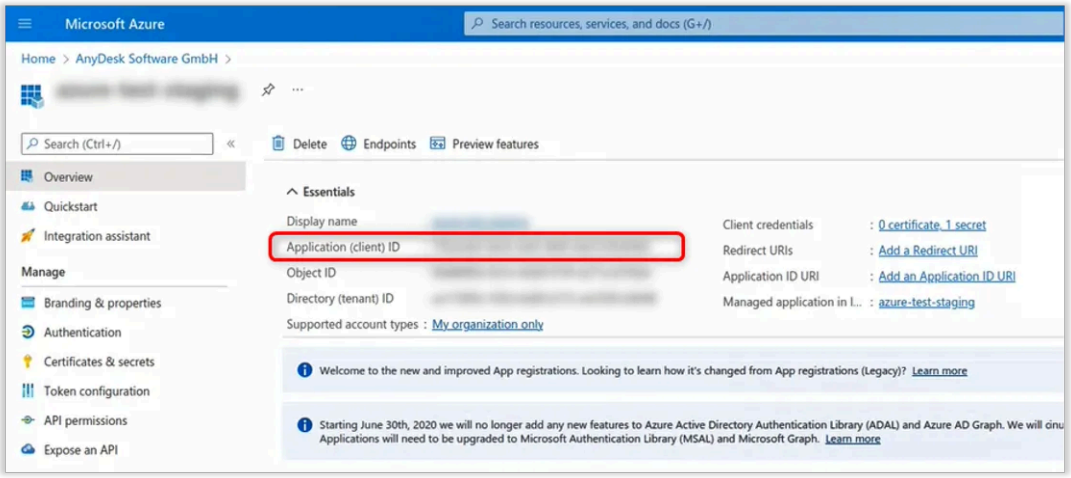
Prerrequisitos

Antes de configurar IDP en my.anydesk II, configure su IDP de terceros con soporte OpenID Connect. Necesitará la siguiente información de su IDP:

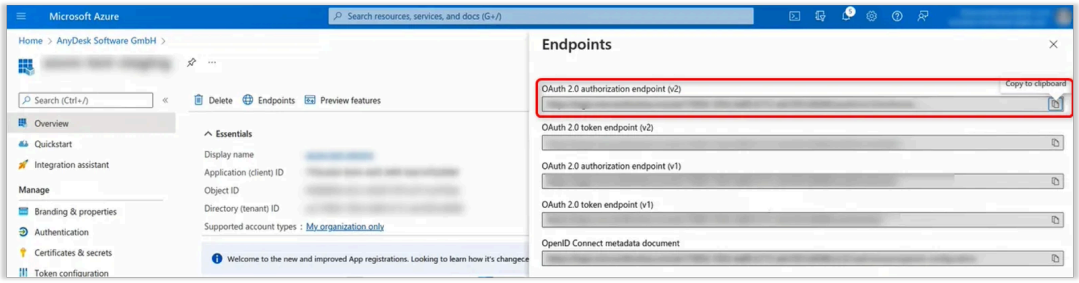
- **Client secret** - usado para autenticación de cliente. Copie la URL al campo **Client Secret** al configurar IDP.



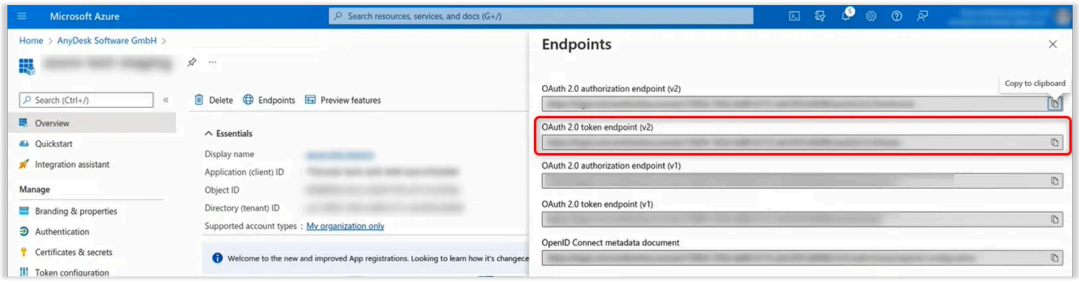
- **Application (Client ID)** - ID de aplicación para my.anydesk. Copie y pegue la URL en el campo **Client ID**.



- **Authorization endpoint** - usado para iniciar la sesión. Copie y pegue la URL en el campo **Authentication URL**.



- **Token endpoint** - usado para emitir tokens. Copie y pegue la URL en el campo **Token URL**.



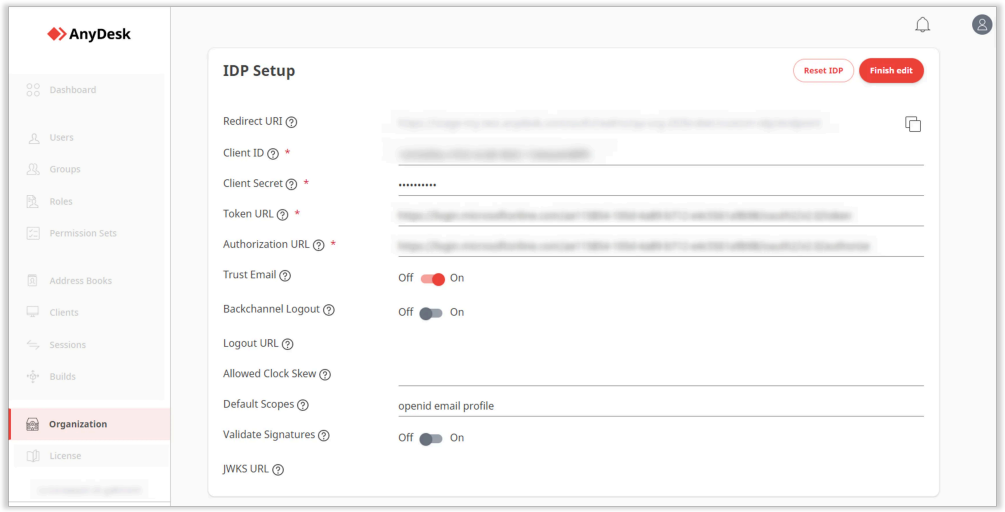
Configurar IDP

> 🚨 **IMPORTANTE**
>
> No puede editar usuarios creados a través de IDP en **my.anydesk II**; se sincronizan desde el proveedor de identidad.

Para configurar IDP:

1. Inicie sesión en my.anydesk II y vaya a **Organization**.
2. Bajo **General**, haga clic en **Edit** y seleccione **IDP** como el proveedor de usuarios.
3. En la ventana **Switch active provider**, seleccione **Proceed**.
4. Desplácese hacia abajo hasta la sección **IDP Setup**, haga clic en **Edit** y proporcione la siguiente información:
    - **Redirect URI** - generado automáticamente cuando se completa la configuración de IDP. Copie el valor de Redirect URI después de finalizar la configuración y péguelo en su proveedor de identidad.
    - **Client ID** - copie el valor **Application (Client ID)** de su IDP y péguelo aquí. Se usa para registrar *my.anydesk* como un cliente OIDC con su proveedor.
    - **Client Secret** - copie el valor **Client Secret** de su IDP y péguelo aquí. Se usa para registrar *my.anydesk* como un cliente OIDC con su proveedor.
    - **Token URL** - copie el valor **Token endpoint** de su IDP y péguelo aquí. Devuelve los tokens de acceso, tokens de ID y tokens de actualización al cliente (*my.anydesk*).
    - **Authorization URL** - copie el valor **Authorization endpoint** de su IDP y péguelo aquí. Se usa para la autenticación y autorización del cliente *my.anydesk*.
    - **Trust Email** - desactive la opción para permitir que los usuarios verifiquen su dirección de correo electrónico a través de *my.anydesk II*. Active la opción para deshabilitar la verificación de correo electrónico de *my.anydesk II*.

- **Backchannel Logout** - active la opción para habilitar el soporte de cierre de sesión backchannel por el IDP configurado. Si está habilitado, *se debe proporcionar el campo **Logout URL***.
- **Logout URL** - proporcione el endpoint para cerrar la sesión de los usuarios desde el IDP externo. ***Backchannel Logout** debe estar habilitado.*
- **Allowed Clock Skew** - proporcione el valor en segundos (el valor predeterminado es *0*). Determina la desviación aceptable al validar tokens IDP.
- **Default Scopes** - los ámbitos incluidos al solicitar autorización. El predeterminado es `openid`. Proporcione una lista separada por comas de ámbitos adicionales que desee solicitar (por ejemplo, `openid` , `email`).
- **Validate Signatures** - active la opción para habilitar la validación de firma del IDP configurado. Si está habilitado, *se debe proporcionar el campo **JWKS URL***.
- **JWKS URL** - URL donde my.anydesk II puede recuperar las claves para el IDP configurado. ***Validate Signatures** debe estar habilitado.*



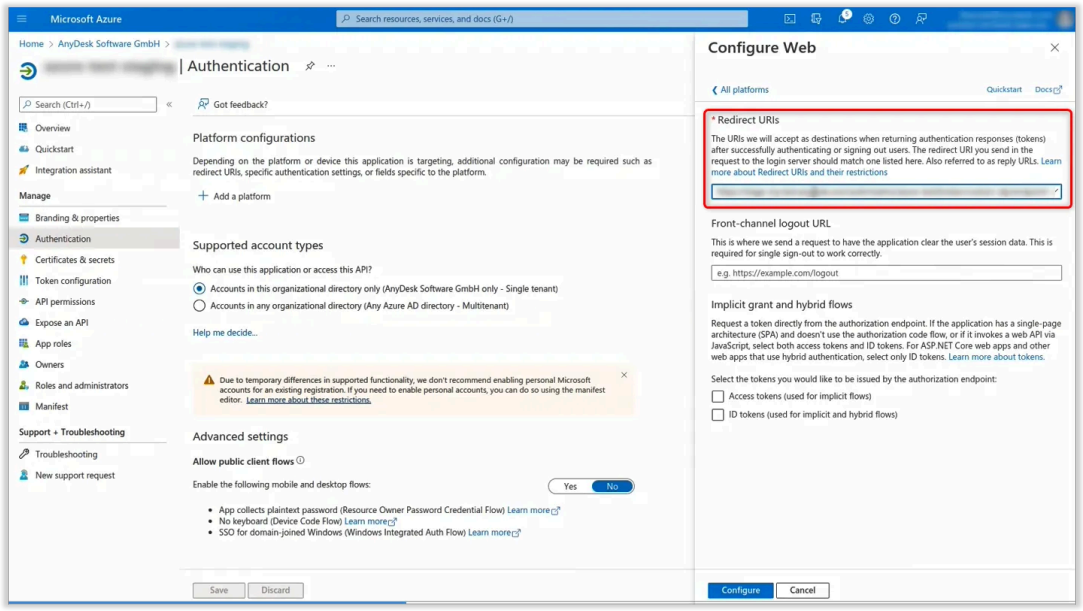
5. Haga clic en **Finish edit**.

6. Copie **Redirect URI** generada.

7. Abra su proveedor de identidad y vaya a **Authentication.**

   ⚠️ *Se usa el proveedor de identidad Microsoft AzureAD aquí como ejemplo. Se puede usar cualquier proveedor compatible con OpenID Connect.*

8. Haga clic en **Add a platform**, seleccione **Web** y pegue la **Redirect URI** que copió después de guardar el proveedor de identidad en my.anydesk II.



9. Haga clic en **Configure**.

Una vez configurado, los usuarios en su IDP pueden iniciar sesión en my.anydesk II con sus credenciales corporativas vía SSO.

Configurar mapeador IDP

El mapeador IDP le permite asignar roles a los usuarios automáticamente basándose en atributos del IDP. De esta manera, no necesita asignar roles a los usuarios manualmente.

Por ejemplo, si desea que los usuarios con el nombre *John* reciban el rol **admin**:

- Key: `FirstName`
- Value: `John`
- Role: `admin`

Estos usuarios heredarán el rol de admin al iniciar sesión.

Requisitos:

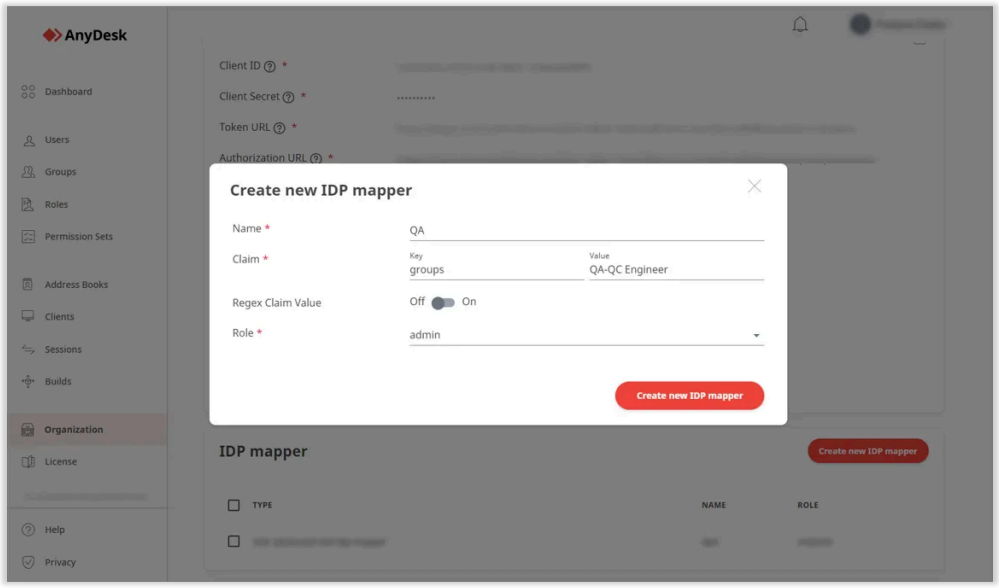
- Un token de grupo debe estar configurado en su IDP.
- Al menos un rol ya debe existir en my.anydesk II

Para configurar el mapeador IDP:

1. En my.anydesk II, vaya a **Organization**.

2. Desplácese hacia abajo hasta la sección **IDP mapper**, haga clic en **Create new IDP mapper** y proporcione la siguiente información:

    - **Name** - ingrese el nombre para el mapeador IDP.
    - **Claim** - proporcione la siguiente información:
        - **Key** - el nombre del atributo IDP (por ejemplo, `FirstName`).
        - **Value** - el valor esperado para la clave (por ejemplo, `John`).
    - **Role** - seleccione el rol de la lista desplegable que desea asignar al usuario IDP especificado.



3. Haga clic en **Create new IDP mapper.**

Una vez creado, a los usuarios que coincidan con la reclamación especificada se les asignará automáticamente el rol seleccionado. Los roles mapeados no se pueden asignar manualmente hasta que se elimine el mapeador.