Como adicionar múltiplos usuários via Provedor de Identidade (IDP) para Enterprise-Cloud ou Ultimate-Cloud | AnyDesk

ÍNDICE

Pré-requisitos
Configurar IDP
Configurar mapeador IDP
Exemplo

“# Adicionar múltiplos usuários via Provedor de Identidade (IDP)

Aplicável para usuários com licença **Enterprise-Cloud** ou **Ultimate-Cloud**.

O provedor de usuários **IDP** permite ao proprietário de uma organização criar usuários para essa organização usando um sistema de gerenciamento de identidade que suporte OpenID Connect (por exemplo, Microsoft Azure Active Directory). Dessa forma, é possível configurar o IDP em my.anydesk II. Os usuários da sua organização poderão fazer login com SSO utilizando a identidade da organização e suas credenciais corporativas.

Neste capítulo, você aprenderá quais são os pré-requisitos necessários para a configuração do IDP, como configurar o IDP via console de gerenciamento my.anydesk, e como configurar um mapeador de IDP.

Para mais informações sobre tipos de provedores de usuários, consulte Provedores de Usuários.

Pré-requisitos

Antes de configurar o IDP em my.anydesk II, você precisa configurar seu provedor de identidade primeiro. Você pode utilizar qualquer provedor de identidade de terceiros que suporte OpenID Connect, como o Microsoft Azure Active Directory.

Para configurar o IDP em my.anydesk II, você precisará dos seguintes dados:

- **Client Secret.** Copie e cole a URL no campo **Client Secret** ao configurar o **Setup do IDP**.
- **Aplicação (Client ID).** Copie e cole a URL no campo **Client ID**.
- **Endpoint de Autorização.** Copie e cole a URL no campo **URL de Autenticação**.
- **Endpoint de Token.** Copie e cole a URL no campo **URL de Token**.

Configurar IDP

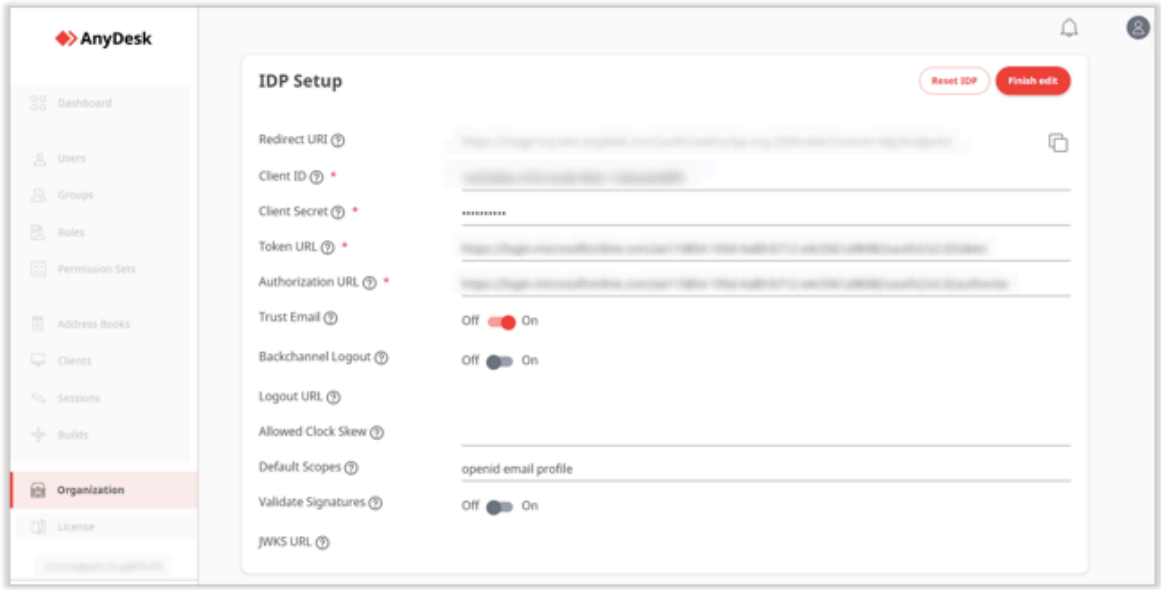
É necessário configurar o IDP para criar uma conexão entre o my.anydesk II e seu provedor de identidade.

❗ Você não poderá editar usuários no my.anydesk II criados por meio do IDP, uma vez que eles estão sincronizados com o provedor de identidade.

Para configurar o IDP em my.anydesk II:

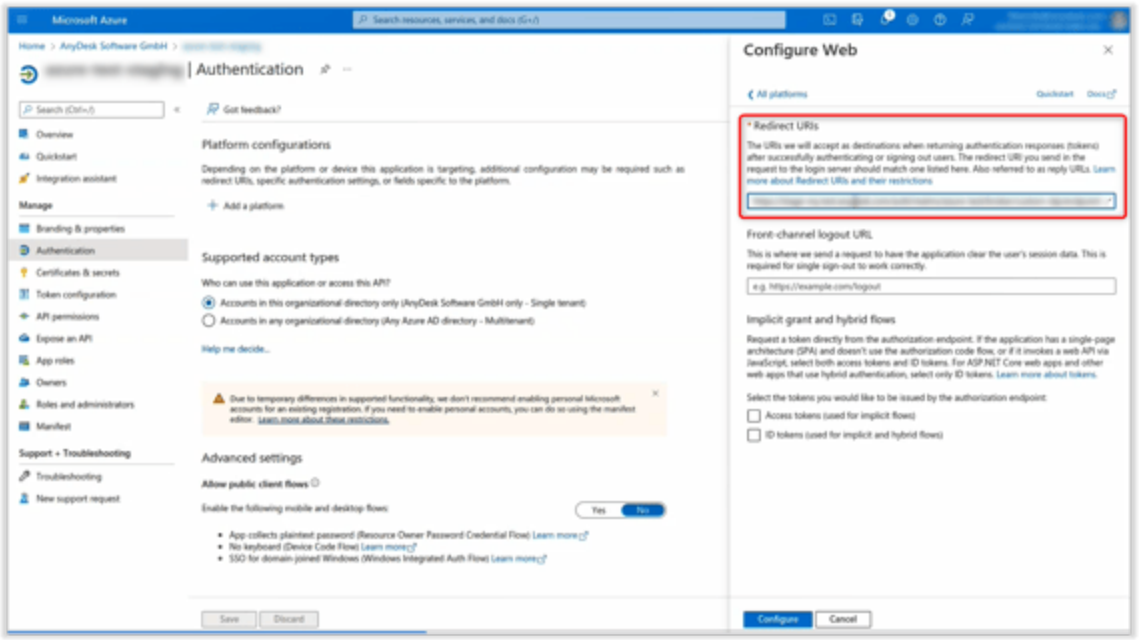
1. Abra o my.anydesk II e vá para **Organização**.
2. Na seção **Geral**, clique em **Editar**. No campo **Provedor de Usuários**, selecione **IDP**.
3. Na janela **Alternar provedor ativo**, selecione **Prosseguir**.
4. Role até a seção **Setup do IDP**, clique em **Editar** e forneça as seguintes informações:
    - **URI de Redirecionamento** - Gerada automaticamente ao finalizar o setup do IDP. Copie o valor da URI de Redirecionamento após finalizar a configuração e cole-a em seu respectivo provedor de identidade.
    - **Client ID** - Copie o valor de **Application (Client ID)** do seu IDP e cole aqui. É utilizado para registrar o my.anydesk como um cliente OIDC no seu provedor.
    - **Client Secret** - Copie o valor de **Client Secret** do seu IDP e cole aqui. É utilizado para registrar o my.anydesk como um cliente OIDC no seu provedor.
    - **URL de Token** - Copie o valor do **Token endpoint** do seu IDP e cole aqui. Ele retorna os tokens de acesso, tokens de ID e tokens de atualização para o cliente (my.anydesk).
    - **URL de Autorização** - Copie o valor do **Authorization endpoint** do seu IDP e cole aqui. Ela é utilizada para autenticação e autorização do cliente my.anydesk.
    - **E-mail de Confiança** - Desative a opção para permitir que os usuários verifiquem seu endereço de e-mail via my.anydesk II. Ative a opção para desabilitar a verificação de e-mail pelo my.anydesk II.
    - **Logoff Backchannel** - Ative a opção para habilitar o suporte ao logoff backchannel pelo IDP configurado. Se habilitado, o campo **URL de Logoff** deve ser fornecido.

- **URL de Logoff** - Forneça o endpoint para fazer logoff dos usuários do IDP externo. **Logoff Backchannel** deve estar habilitado.
- **Margem de Tolerância do Relógio** - Forneça o valor em segundos (o valor padrão é *0*). Determina a margem aceitável ao validar tokens do IDP.
- **Escopos Padrão** - Os escopos incluídos ao solicitar autorização. O padrão é *openid*. Forneça uma lista separada por vírgulas de escopos adicionais que você deseja solicitar.
- **Validar Assinaturas** - Ative a opção para habilitar a validação de assinatura do IDP configurado. Se habilitado, o campo **URL JWKS** deve ser fornecido.
- **URL JWKS** - URL onde my.anydesk II pode recuperar as chaves para o IDP configurado. **Validar Assinaturas** deve estar habilitado.



5. Clique em **Concluir edição**.
6. Após salvar o provedor de identidade, copie o **URI de Redirecionamento** atribuído.
7. Abra seu provedor de identidade e vá para **Autenticação**.

   ❗ O provedor de identidade Microsoft AzureAD é utilizado neste exemplo para demonstrar o procedimento. Você pode utilizar qualquer outro provedor de identidade de terceiros.
8. Clique em **Adicionar plataforma**, selecione **Web** e cole o **URI de Redirecionamento** que você copiou depois de salvar o provedor de identidade em my.anydesk II.



9. Clique em **Configurar**.

Após completar os passos acima, todos os usuários do seu provedor de identidade poderão fazer login no my.anydesk II com SSO utilizando a identidade da organização.

Configurar mapeador IDP

Você pode mapear funções da sua organização para usuários no my.anydesk II. Dessa forma, você não precisa atribuir funções aos usuários manualmente.

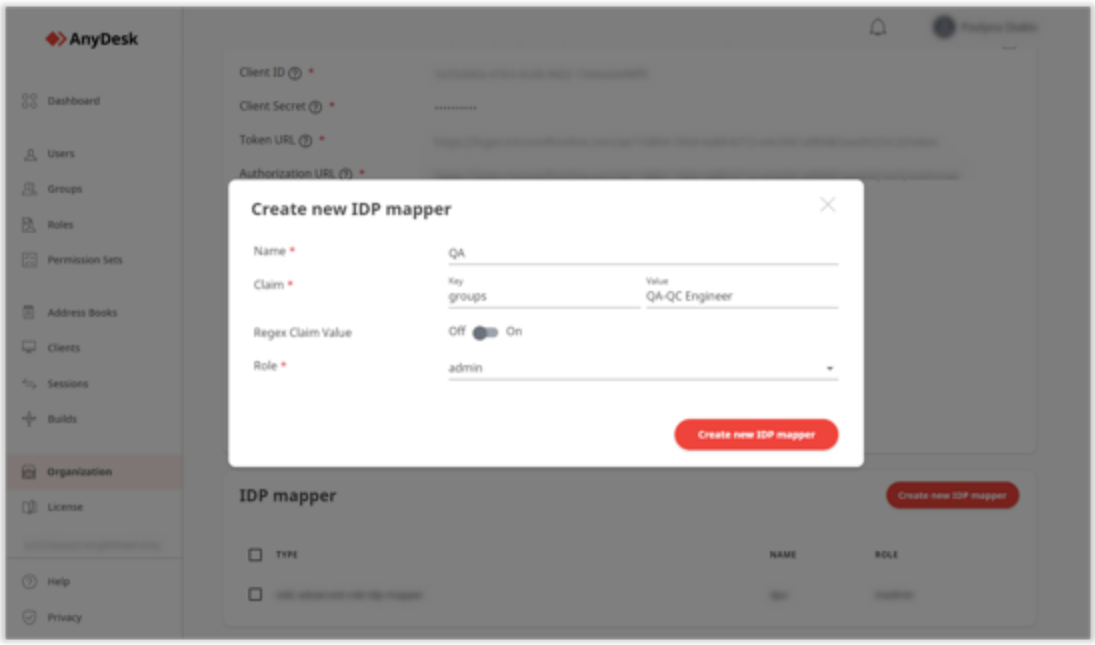
Inicialmente, é necessário configurar um token de grupo em seu provedor de identidade. Então, para configurar o mapeador IDP, é necessário que ao menos uma função já exista no console de gerenciamento my.anydesk II. Essa função poderá então ser mapeada para uma função dentro do provedor de identidade.

Após mapear a(s) função(ões), seu status mudará para *mapeado*. Isso significa que os usuários não poderão mais ser vinculados manualmente a essa função. Deletar o mapeador IDP removerá o status **mapeado**, permitindo que você vincule manualmente usuários a essa função.

Para configurar o mapeador IDP:

1. Abra o my.anydesk II e vá para **Organização**.

2. Role até a seção **Mapeador IDP**, clique em **Criar novo mapeador IDP** e forneça as seguintes informações:
    - **Nome** - Insira o nome para o mapeador IDP.
    - **Reivindicação** - Forneça as seguintes informações:
      * **Chave** - Insira a chave do atributo IDP que você deseja mapear.
      * **Valor** - Insira o valor do atributo IDP que deseja mapear.
    - **Função** - Selecione a função da lista suspensa que você deseja atribuir ao usuário IDP especificado no console de gerenciamento my.anydesk.com.



3. Clique em **Criar novo mapeador IDP**.

Se um usuário com critérios de chave-valor correspondentes fizer login na sua conta [my.anydesk II](), eles terão automaticamente todas as permissões atribuídas à função à qual foram mapeados.

Exemplo

Por exemplo, se você quiser que todo usuário do seu provedor de identidade com o primeiro nome ***John*** receba a função **administrador** do AnyDesk, então no campo **Chave**, insira **Nome** (dependendo da chave do seu IDP), no campo **Valor**, insira **John**, e no campo **Função**, selecione **admin**.