

Splashtop – Microsoft Entra ID (Azure AD): alterações de configuração

A Microsoft está renomeando o **Azure AD** para **Entra ID**. Da mesma forma, o **Office 365** passa a se chamar **Microsoft 365**. Sempre que possível, este documento se refere aos serviços da Microsoft pelo nome recomendado.

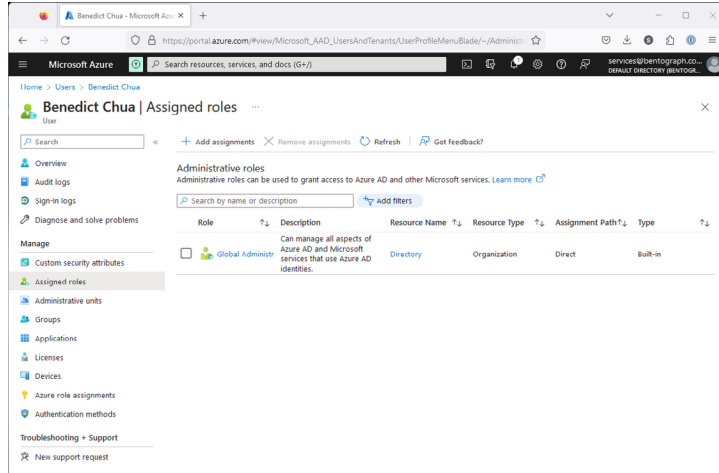
Sincronizar usuários com o Microsoft Entra ID

Para funcionar, a sincronização de usuários do Entra ID requer um usuário administrador com permissões suficientes e uma licença ativa do Microsoft 365.

– O usuário administrador deve ter a função de Administrador Global ou as funções de Administrador de Aplicativos de Nuvem e de Administrador de Usuários.

Configurar funções

No Entra ID, navegue até Usuários e selecione a conta que você usará para a sincronização do Foxpass. Atribua à conta permissões suficientes (por exemplo, Administrador Global) para permitir a sincronização.



Configurar a sincronização do Foxpass com o Entra ID.

No painel do Foxpass, siga a documentação do Foxpass para autorizar o Foxpass a sincronizar com o Entra ID:

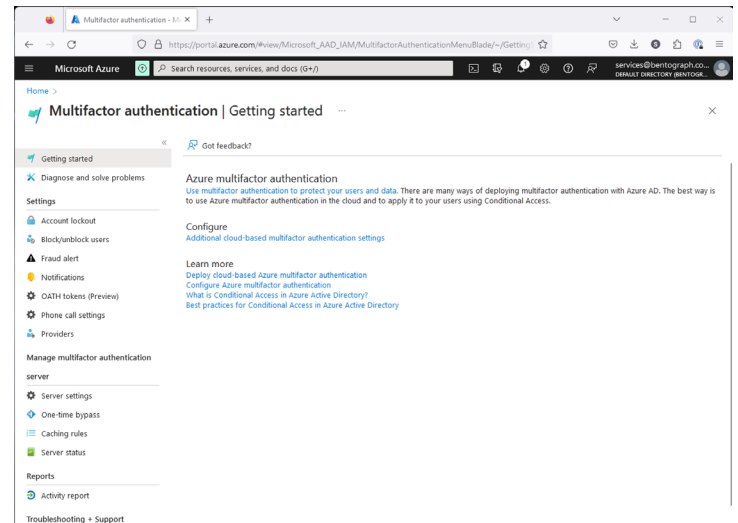
[Aqui você encontra como configurar o Foxpass para sincronizar seu diretório com o Office 365.](#)

Usar o Entra ID para a autenticação de usuários

Configurar endereços IP confiáveis da autenticação multifator do Entra ID

Antes de habilitar a autenticação delegada do Foxpass, o Entra ID deve ser configurado para confiar nos endereços IP do Foxpass.

Configure os endereços IP confiáveis no painel do Entra ID navegando até **Multifactor authentication**. Clique no link em **Configure** para definir as **Additional cloud-based multifactor authentication settings**.



Insira os endereços IP do Foxpass em **Skip multi-factor authentication for requests from following range of IP address subnets**.

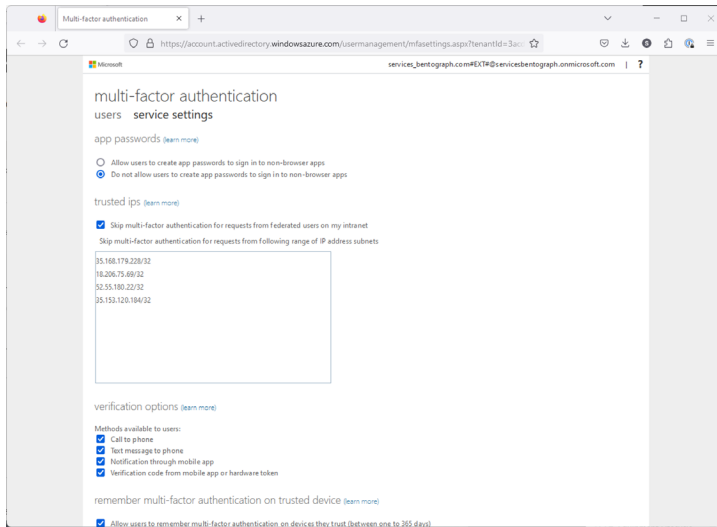
[Endereços IP do Foxpass]

35.168.179.228/32

18.206.75.69/32

52.55.180.22/32

35.153.120.184/32

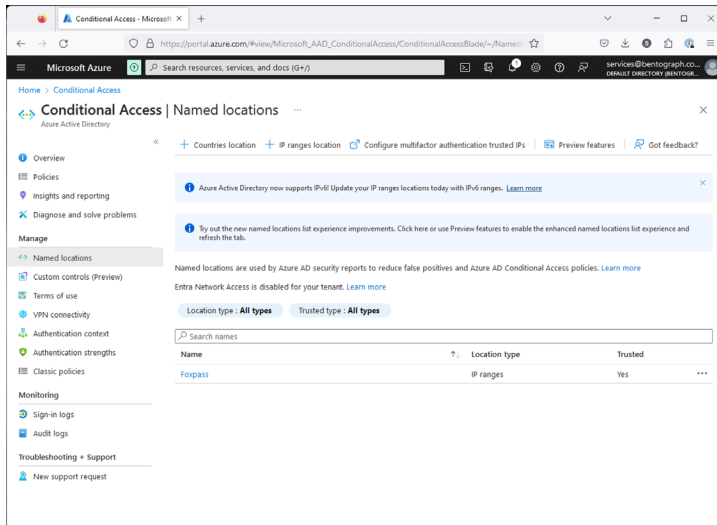


Configurar locais nomeados do Acesso Condicional



Por padrão, o Entra ID impõe uma autenticação multifator forte. Você deve configurar uma política de Acesso Condicional para permitir que o Foxpass ignore a MFA e verifique as credenciais dos usuários.

No Entra ID, navegue até **Conditional Access | Manage | Named Locations** e defina um local do tipo **IP ranges location**.



Dê ao local o nome **Foxpass**. Configure o intervalo de IP do local com os mesmos valores usados no painel de endereços IP confiáveis:

35.168.179.228/32
18.206.75.69/32
52.55.180.22/32
35.153.120.184/32

Desabilitar os padrões de segurança

Para implementar políticas de Acesso Condicional, as organizações precisam primeiro desabilitar os padrões de segurança. Se eles estiverem ativos, [desabilite-os seguindo as etapas descritas aqui](#).

Criar uma política de Acesso Condicional

O intervalo de IP do local **Foxpass** definido na etapa anterior precisa ser usado em uma política para ter efeito. Nesta etapa, criamos a política que permite ignorar a MFA para solicitações vindas do **intervalo de IP do Foxpass**.

Na mesma seção **Conditional Access**, alterne para **Overview** e selecione **Create new policy**.

Configure a política com os seguintes valores:

Name: Foxpass

Conditions | Locations:

- Configure: **Yes**

- Include: **Selected locations**

- Select: **Foxpass**

Grant:

- Block/Grant access: **Grant access**

- Require multifactor authentication: **[X]** (caixa de seleção)

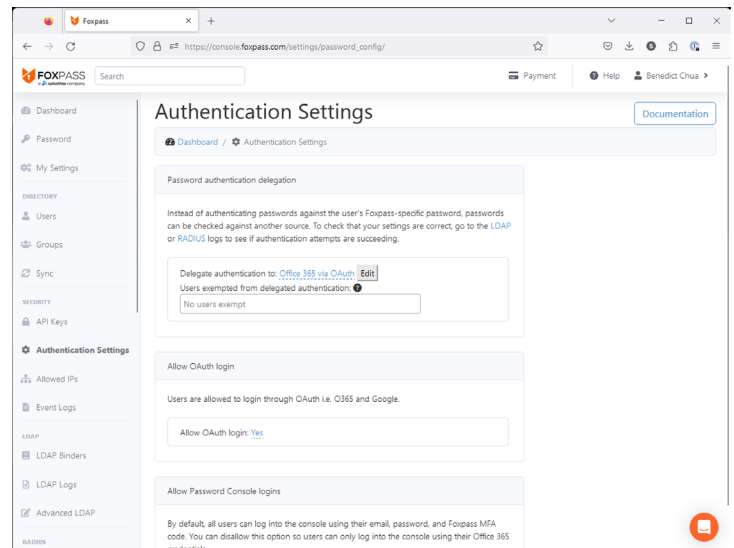
Enable policy: **On**

Selecione **Create**

Habilitar a delegação de senhas Entra ID / Foxpass

Conclua o processo no **painel do Foxpass**, configurando o Foxpass para delegar a verificação de senhas ao **Entra ID**.

Acesse a página [Authentication Settings](#) do Foxpass. Role até **"Password authentication delegation"**. Escolha **Office 365 via OAuth** no menu suspenso e clique em **"Save"**.



Validar o fluxo de autenticação

Faça login na rede corporativa (configurada para a autenticação RADIUS do Foxpass) com qualquer conta de administrador ou de usuário definida no **Entra ID** e configurada para sincronização com o **Foxpass**.