

Splashtop – Microsoft Entra ID (Azure AD): Konfigurationsänderungen

Microsoft benennt **Azure AD** in **Entra ID** um. Ebenso wird aus **Office 365** nun **Microsoft 365**. Wo möglich, verwendet dieses Dokument die empfohlenen Namen der Microsoft-Dienste.

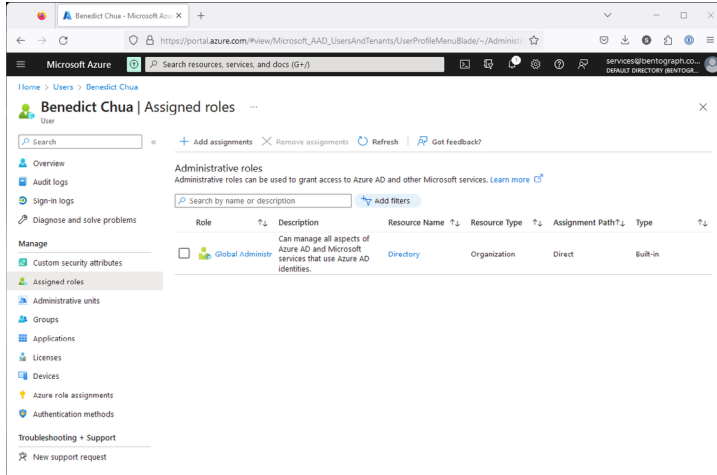
Benutzer mit Microsoft Entra ID synchronisieren

Für die Benutzersynchronisierung mit Entra ID ist ein Administratorkonto erforderlich, das sowohl über ausreichende Berechtigungen als auch über eine aktive Microsoft 365-Lizenz verfügt.

– Das Administratorkonto muss entweder die Rolle „Globaler Administrator“ oder die beiden Rollen „Cloudanwendungsadministrator“ und „Benutzeradministrator“ innehaben.

Rollen konfigurieren

Navigieren Sie in Entra ID zu „Benutzer“ und wählen Sie das Konto aus, das Sie für die Foxpass-Synchronisierung verwenden. Weisen Sie dem Konto ausreichende Berechtigungen zu (z. B. „Globaler Administrator“), um die Synchronisierung zu ermöglichen.



Foxpass-Synchronisierung mit Entra ID konfigurieren.

Folgen Sie im Foxpass-Dashboard der Foxpass-Dokumentation, um Foxpass für die Synchronisierung mit Entra ID zu autorisieren:

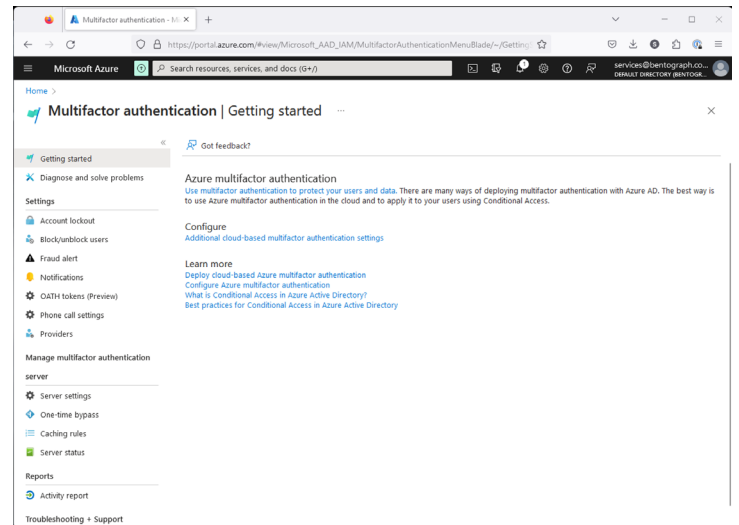
[Hier wird beschrieben, wie Sie Foxpass für die Synchronisierung Ihres Verzeichnisses mit Office 365 einrichten.](#)

Entra ID für die Benutzerauthentifizierung nutzen

Vertrauenswürdige IP-Adressen für die Multi-Faktor-Authentifizierung in Entra ID konfigurieren

Bevor Sie die delegierte Authentifizierung von Foxpass aktivieren, muss Entra ID so konfiguriert werden, dass es den IP-Adressen von Foxpass vertraut.

Konfigurieren Sie vertrauenswürdige IP-Adressen im Entra ID-Dashboard unter **Multifactor authentication**. Klicken Sie auf den Link unter **Configure**, um die **Additional cloud-based multifactor authentication settings** einzurichten.



Geben Sie die IP-Adressen von Foxpass unter **Skip multifactor authentication for requests from following range of IP address subnets** ein.

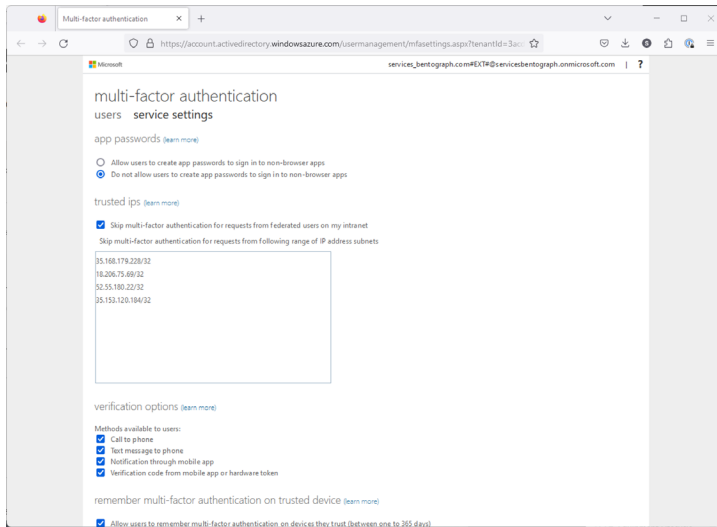
[IP-Adressen von Foxpass]

35.168.179.228/32

18.206.75.69/32

52.55.180.22/32

35.153.120.184/32

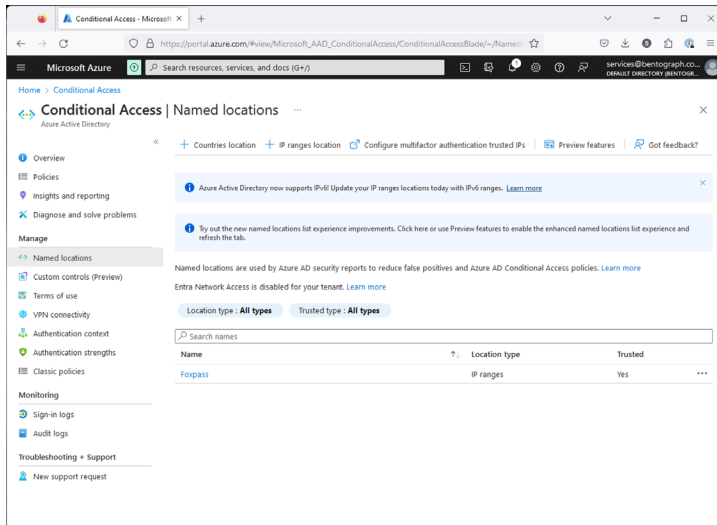


Benannte Standorte für bedingten Zugriff konfigurieren



Entra ID erzwingt standardmäßig eine starke Multi-Faktor-Authentifizierung. Sie müssen eine Richtlinie für bedingten Zugriff konfigurieren, damit Foxpass die MFA umgehen und Benutzeranmeldedaten prüfen kann.

Navigieren Sie in Entra ID zu **Conditional Access | Manage | Named Locations** und definieren Sie einen Standort vom Typ **IP ranges location**.



Benennen Sie den Standort **Foxpass**. Konfigurieren Sie den IP-Bereich des Standorts mit denselben Werten wie im Bereich für vertrauenswürdige IP-Adressen:

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

Sicherheitsstandards deaktivieren

Um Richtlinien für bedingten Zugriff einzusetzen, müssen Organisationen zunächst die Sicherheitsstandards deaktivieren. Wenn die Sicherheitsstandards aktiv sind, [deaktivieren Sie sie anhand der hier beschriebenen Schritte](#).

Richtlinie für bedingten Zugriff erstellen

Der im vorherigen Schritt definierte IP-Bereich des Standorts **Foxpass** muss in einer Richtlinie verwendet werden, damit er wirksam wird. In diesem Schritt erstellen wir die Richtlinie, die das Umgehen der MFA für Anfragen aus dem **Foxpass-IP-Bereich** erlaubt.

Wechseln Sie im selben Abschnitt **Conditional Access** zu **Overview** und wählen Sie **Create new policy** aus.

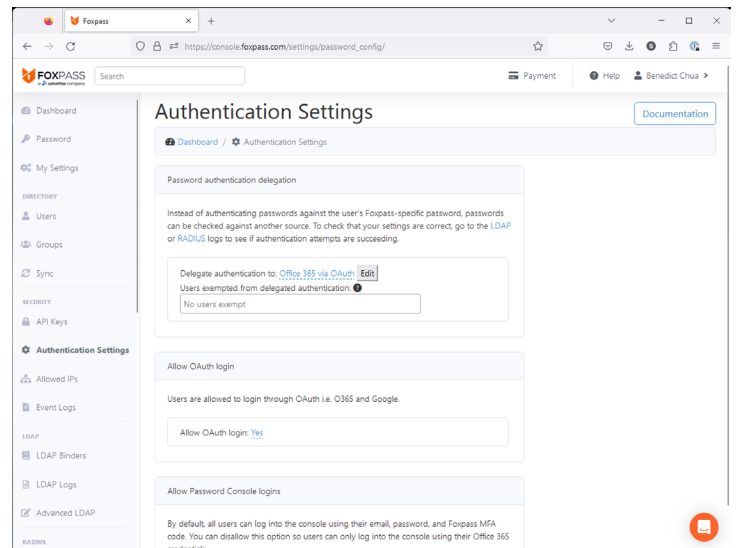
Konfigurieren Sie die Richtlinie mit den folgenden Werten:

Name: Foxpass
Conditions | Locations:
- Configure: **Yes**
- Include: **Selected locations**
- Select: **Foxpass**
Grant:
- Block/Grant access: **Grant access**
- Require multifactor authentication: **[x] (Kontrollkästchen)**
Enable policy: **On**
Create auswählen

Kennwortdelegierung Entra ID / Foxpass aktivieren

Schließen Sie den Vorgang im **Foxpass-Dashboard** ab, indem Sie Foxpass so einstellen, dass die Kennwortüberprüfung an **Entra ID** delegiert wird.

Rufen Sie in Foxpass die Seite [Authentication Settings](#) auf. Scrollen Sie nach unten zu „**Password authentication delegation**“. Wählen Sie im Dropdown-Menü **Office 365 via OAuth** und klicken Sie auf „**Save**“.



Authentifizierungsablauf überprüfen

Melden Sie sich mit einem beliebigen Administrator- oder Benutzerkonto, das in **Entra ID** definiert und für die Synchronisierung mit **Foxpass** konfiguriert ist, bei Ihrem Unternehmensnetzwerk an (eingerrichtet für die Foxpass-RADIUS-Authentifizierung).