Splashtop - Microsoft Entra ID (Azure AD) Configuration Changes

Microsoft is rebranding **Azure AD** to **Entra ID**. Likewise, **Office 365** is changing to **Microsoft 365**. Where possible, this document refers to Microsoft services by their recommended name.

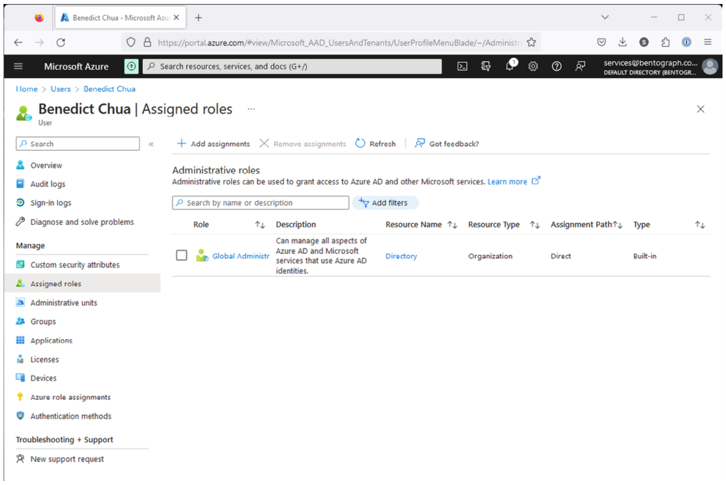
Sync users with Microsoft Entra ID

Entra ID user synchronization requires an admin user with both sufficient permissions and an active Microsoft 365 license to work.

- Admin user must either hold a Global Administrator role or both Cloud Application Administrator and User Administrator roles.

Configure Roles

On Entra ID, navigate to Users and select the account you will use for Foxpass sync. Assign the account sufficient permissions (e.g. Global Administrator) to allow sync.


Benedict Chua - Microsoft Azur
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/Administr
Microsoft Azure
Search resources, services, and docs (G+/)
services@bentograph.co...
DEFAULT DIRECTORY (BENTOGR...
Home > Users > Benedict Chua
Benedict Chua | Assigned roles
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
Troubleshooting + Support
New support request
Add assignments
Remove assignments
Refresh
Got feedback?
Search by name or description
Add filters

Administrative roles

Administrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more

	Role	Description	Resource Name	Resource Type	Assignment Path	Type
□	Global Administr	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.	Directory	Organization	Direct	Built-in

Configure Foxpass sync with Entra ID.

On the Foxpass dashboard, follow Foxpass documentation to authorize Foxpass to sync with Entra ID:

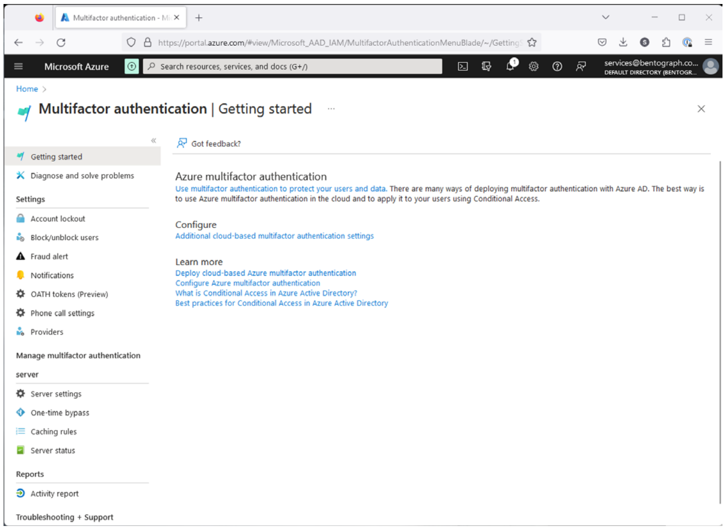
[This describes how to set up Foxpass to sync your directory with Office 365](#).

Leverage Entra ID for user authentication

Configure Entra ID Multifactor authentication trusted IP addresses

Before enabling Foxpass delegated authentication, Entra ID must be configured to trust Foxpass' IP addresses.

Configure trusted IP addresses from Entra ID dashboard by navigating to **Multifactor authentication**. Click the link under **Configure** to set up **Additional cloud-based multifactor authentication settings.**


Multifactor authentication - Mi
https://portal.azure.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationMenuBlade/~/GettingS
Microsoft Azure
Search resources, services, and docs (G+/)
services@bentograph.co...
DEFAULT DIRECTORY (BENTOGR...
Home >
Multifactor authentication | Getting started
Getting started
Diagnose and solve problems
Settings
Account lockout
Block/unblock users
Fraud alert
Notifications
OATH tokens (Preview)
Phone call settings
Providers
Manage multifactor authentication server
Server settings
One-time bypass
Caching rules
Server status
Reports
Activity report
Troubleshooting + Support
Got feedback?

Azure multifactor authentication

Use multifactor authentication to protect your users and data. There are many ways of deploying multifactor authentication with Azure AD. The best way is to use Azure multifactor authentication in the cloud and to apply it to your users using Conditional Access.

Configure

Additional cloud-based multifactor authentication settings

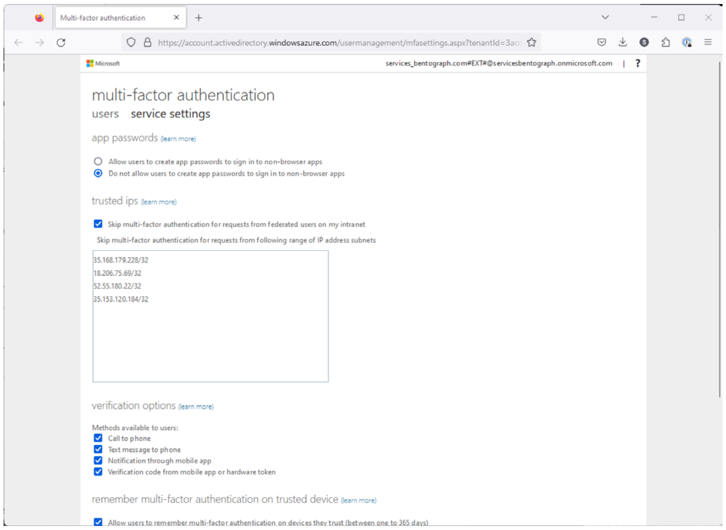
Learn more

Deploy cloud-based Azure multifactor authentication
Configure Azure multifactor authentication
What is Conditional Access in Azure Active Directory?
Best practices for Conditional Access in Azure Active Directory

Enter Foxpass' IP addresses under **Skip multi-factor authentication for requests from following range of IP address subnets.**

[Foxpass' IP Addresses]

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


Multi-factor authentication
https://account.activedirectory.windowsazure.com/usermanagement/mfasettings.aspx?tenantId=3acd
Microsoft
services_bentograph.com#EXT#@servicesbentograph.onmicrosoft.com
users
service settings
(learn more)

multi-factor authentication

app passwords

○ Allow users to create app passwords to sign in to non-browser apps
● Do not allow users to create app passwords to sign in to non-browser apps

trusted ips

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

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

verification options

Methods available to users:
☑ Call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

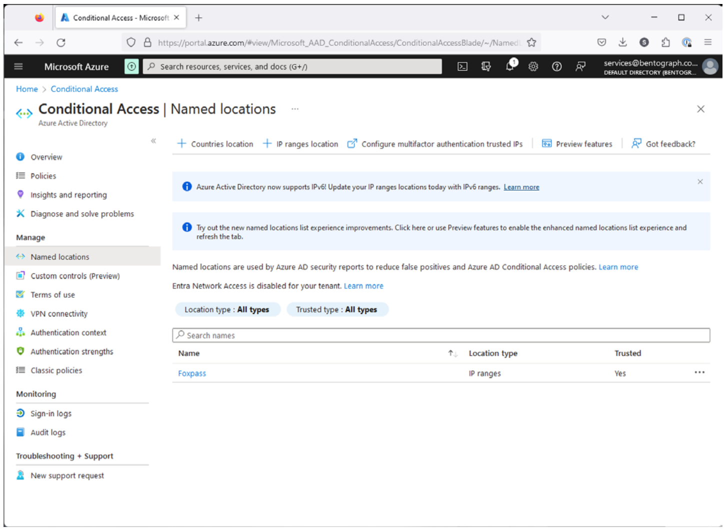
remember multi-factor authentication on trusted device

☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Configure Conditional Access Named locations

> Entra ID enforces strong, multi-factor authentication by default. You must configure a Conditional Access Policy to allow Foxpass to bypass MFA and check user credentials.

In Entra ID, navigate to **Conditional Access | Manage | Named Locations** and define an **IP ranges location**.


Conditional Access - Microsoft
https://portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/NamedL
Microsoft Azure
Search resources, services, and docs (G+/)
services@bentograph.co...
DEFAULT DIRECTORY (BENTOGR...
Home > Conditional Access
Conditional Access | Named locations
Azure Active Directory
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication context
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
+ Countries location
+ IP ranges location
Configure multifactor authentication trusted IPs
Preview features
Got feedback?
Location type : All types
Trusted type : All types
Search names

Azure Active Directory now supports IPv6! Update your IP ranges locations today with IPv6 ranges. Learn more

Try out the new named locations list experience improvements. Click here or use Preview features to enable the enhanced named locations list experience and refresh the tab.

Named locations are used by Azure AD security reports to reduce false positives and Azure AD Conditional Access policies. Learn more

Entra Network Access is disabled for your tenant. Learn more

Name	Location type	Trusted
Foxpass	IP ranges	Yes

Name the location **Foxpass**. Configure location's IP range with the same values used in the trusted IP address pane:

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

Disable Security Defaults

Implementing Conditional Access Policies requires organizations to first disable security defaults. If Security Defaults are active, disable them using the steps found here.

Build a Conditional Access Policy

The **Foxpass** location's IP range defined in the previous step must be used in a policy to have an effect. In this step, we create the policy to allow MFA bypass for requests from the **Foxpass IP range**.

In the same **Conditional Access** section, switch to **Overview** and select **Create new policy**.

Configure the policy with the following values:

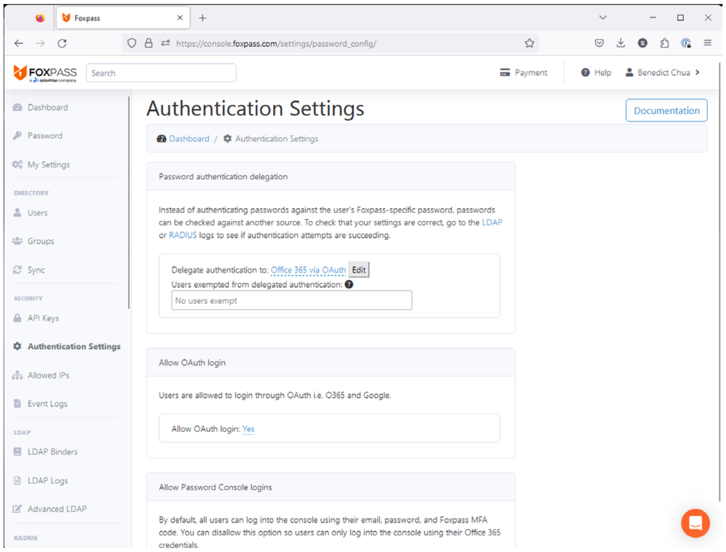
Name: Foxpass
Conditions I Locations:
- Configure: Yes
- Include: Selected locations
- Select: Foxpass
Grant:
- Block/Grant access: Grant access
- Require multifactor authentication: [X] (Check box)
Enable policy: On

Select **Create**

Enable Entra ID / Foxpass password delegation

Complete the process on the **Foxpass dashboard** by settings Foxpass to delegate password verification to **Entra ID**.

Go to the Foxpass Authentication Settings page. Scroll down to "**Password authentication delegation**." Choose **Office 365 via OAuth** from the dropdown menu and click "**Save**."



Authentication Settings

Password authentication delegation

Instead of authenticating passwords against the user's Foxpass-specific password, passwords can be checked against another source. To check that your settings are correct, go to the LDAP or RADIUS logs to see if authentication attempts are succeeding.

Delegate authentication to: Office 365 via OAuth
Users exempted from delegated authentication:
No users exempt

Allow OAuth login

Users are allowed to login through OAuth i.e. O365 and Google.

Allow OAuth login: Yes

Allow Password Console logins

By default, all users can log into the console using their email, password, and Foxpass MFA code. You can disallow this option so users can only log into the console using their Office 365 credentials.

Validate Authentication Flow

Log into your enterprise network (set for Foxpass RADIUS authentication) using any admin or user account defined on **Entra ID** and configured for sync to **Foxpass**.