CONFIGURING PASSWORD-LESS AUTHENTICATION FOR AZURE ACTIVE DIRECTORY

By Achilleas Eleftheriou – Team Leader – Support Services

Active Directory (AD) consists of on-premises features included in a Windows Server. These are the **Active Directory Domain Services**, and the **On-premises Active Directory** service in which identities, groups, and other objects are stored.

Microsoft Authenticator can be used to sign into any **Azure Active Directory** account without using a password. This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries. To vastly improve the user experience, I would absolutely make the effort to enable Passwordless authentication for Azure AD.

HOW TO ENABLE PASSWORDLESS AZURE AD

Today we're going to cover exactly how to enable Passwordless authentication so you can answer the age-old question of how to, login to Microsoft Authentication app. This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.

Requirements:

To get Passwordless authentication setup and configured in your environment, there are a couple of items that need to be setup beforehand. Don't worry, we'll walk through the entire process to ensure you're at least beta testing this feature. Here's an overview.

- The user must have Microsoft Authenticator installed on their device.
- Microsoft Authenticator must be the default MFA method.
    - If a user has TOTP as their default method, Passwordless authentication will not work.
- A device can only be registered to 1 account.
    - To Confirm Device Registration: **Open Authenticator → Settings → Device Registration**
- The user will need to be scoped to the authentication method policy.
- The app must be a cloud app. Applications hosted in ADFS may not work since it's a different IdP.

Configuring Administrative settings for Passwordless authentication:

Let's follow the below steps:

- Navigate to the **Azure Active Directory -> Security -> Authentication Methods -> Microsoft Authenticator**
- Set the policy to **Enable.**
- Set the target to **All Users** or specify a pilot user/group.
- As a bonus, enable location rich context For MFA Push Notifications and number matching for icing on the cake.

Then let's see the client setup and user experience:

Assuming the user is in scope of the policy, let's review the setup that's needed as the end-user. It is relatively straight forward, and setup is only needed once per device.

- On the user's mobile device, click the entry for the account.
- Click **Enable phone sign-in**
- Select continue the next screen and you'll be prompted to authenticate to approve MFA.
- If successful, click back into your account and you should see **Passwordless enabled.**

In this way we have successfully enabled Passwordless authentication for Azure AD, to sum up I think this is one of the great features that you should have rolled out to your organization. Most important it is a user friendly and secure.

Azure AD comes in four editions: Free, Office 365 apps, Azure AD Premium P1, and Azure AD Premium P2. IBSCY, as a Microsoft Gold Partner in Cyprus, can help you choose the right edition for your business as we are certified to sell, install, configure, and maintain all Microsoft Cloud products such as Microsoft Azure.

Achilleas Eleftheriou is working for IBSCY for more than 9 years. He is the Team Leader – Support Services with a lot of experience in Microsoft Products (MS365 and AZURE), and on premises infrastructure.