Authlogics MFA for Microsoft Azure and Office 365

Secure access to Microsoft Cloud and On-Premises from anywhere

Cloud-based services give organisations greater functionality at a lower cost, albeit with increased risk. Sensitive corporate information could now be available to anyone, therefore, securing access to these services is critical. Authlogics MFA protects businesses by providing a flexible and highly-secure authentication layer both inside and outside the network.

Office 365 and Active Directory

Out-of-the-box, when a user logs into Office 365 they are authenticated by Azure AD. This is the account used for accessing Exchange Online, SharePoint Online, Skype for Business etc. When you first setup Office 365, user accounts can be created manually or, more typically, they are synchronised from an on-premises Active Directory with Microsoft's Azure AD Connect tool, known as **same sign-on**

A better approach would be to let Azure / Office 365 delegate the responsibility of authenticating users to the on-premises Active Directory by using federation via Microsoft ADFS, generally known as **single sign-on**. However, both these approaches are highly vulnerable as they rely on a password-only approach. A more robust solution is required.

By requiring multiple factors of authentication, with or without a password, you can greatly reduce the chances that an attacker will be able to impersonate a user in a way that would have been simple when using the out-of-the-box username and password security. Authlogics is uniquely positioned to provide cost-effective, flexible and secure options for multi-factor authentication for Office 365 and other cloud-based services.

Modern Authentication

The client-side of Office 365 authentication is often overlooked but is vitally important. When enabling multi-factor authentication with Office 365, by definition, you make a username and password only combination redundant. As such, any client application that asks for and remembers a password will no longer work. Microsoft has addressed this issue by adding "Modern Authentication" support to Microsoft Office since 2013.

Modern Authentication is already built into many Microsoft applications including Outlook, Teams, Active Sync and Workplace Join. When required, the Office app, e.g. Outlook, will present a mini web browser view of a login page allowing for a new login process. Any kind of authentication can then reasonably be presented to the user, and this is where the flexibility of Authlogics' multiple authentication types really shines. Be it device-less 1.5-factor authentication using PINgrid, an oath-compliant 2FA soft token using PINpass, or even a hardware-based one time code generated by a YubiKey device, Authlogics has it covered. Furthermore, these authentication types are available anywhere a user logs in, including their Windows PC and on-premises apps, creating a consistent, simplified authentication experience for users.

Features and highlights

- MFA for Azure and Office 365
- Azure administrator access, Mobile device sync, Outlook client connectivity and browser access to OWA or SharePoint
- Security and flexibility benefits over Microsoft MFA
- Integrate with other cloud app providers via SAML 2.0
- Seamless integration with Modern Authentication
- True single step, Single Sign-On
- Patented 1.5, 2 and 3 Factor Authentication
- Self Service portal for device management and AD password reset
- SDK and Web API automation capability

Authlogics

Authlogics MFA for Microsoft Azure and Office 365

Single Sign-On and Multi-Factor Authentication for the cloud

Authlogics MFA provides seamless integration with all Web browsers, desktop and mobile operating systems capable of working with Azure and Office 365.

Benefits of Authlogics MFA

The Authlogics MFA solution for Azure and Office 365 integrates directly with Microsoft ADFS, providing the greatest level of control and a track-proven implementation of the protocols needed to authenticate users securely. It covers the most use case scenarios for strong authentication. Not only do you reap the benefits of single sign-on to Azure, Office 365, and any other cloud provider which supports SAML 2.0, you can also decide which applications must use strong authentication and from which location.

Authlogics goes beyond simply adding two-factor authentication to Azure and Office 365. It also provides multiple authentication technologies and can be delivered via the web, soft token, email, SMS/TEXT, or YubiKey devices.

PINgrid is our unique device-less 1.5-factor authentication technology that allows users to generate a one time code without a separate physical device. It is quicker and less costly to deploy, more convenient to use, whilst mitigating the security concerns associated with traditional password-based security.

The primary method for delivering strong two-factor authentication is the Authlogics Authenticator soft token which is available on all major App stores. The soft token works 100% offline and has no dependency on 3G or Wi-Fi to function, which is critical for people on the move. All these options can be configured on a per-user basis for control and flexibility.

Authlogics MFA has native integration with YubiKey hardware tokens for when strong security is required, but soft tokens are not the desired option.

Authlogics vs Microsoft MFA

Microsoft includes a limited version of their own MFA solution (Multi-factor Authentication for Office 365) with all Office 365 SKUs which covers some basic scenarios. Furthermore, Microsoft offers a more feature-rich version of their MFA solution (Azure Multi-factor Authentication) which is available as part of the more expensive Azure AD Premium and Enterprise Mobility Suite services.

However, Multi-factor Authentication for Office 365 is limited to Office 365 applications only and is administered via the Office 365 portal. If you require MFA or single sign-on to other cloud providers or on-premises applications, then this is not an option. For those features, you will need to upgrade, for a fee, to Azure Multi-factor Authentication which allows you to install an on-premises server. The downside to this is that you need to administer the on-premises and cloud offerings separately as there is no cross-platform integration.

While the built-in Microsoft MFA solution may initially appear free or appealing, its shortcomings are quickly realised. Authlogics MFA provides better security, more flexibility and consistency across the enterprise and wider cloud network.

Authlogics MFA vs Microsoft MFA feature comparison

Feature \ Solution	Authlogics	Azure MFA	MFA for O365
Multiple authentication technologies	✓		
1.5 Factor Authentication	✓		
Mobile App token	✓	✓	✓
3rd Party Cloud support	✓	✓	
Self Service AD password reset	✓	✓	
Web API & SDK (100% automation)	✓		

Further detailed table available at https://authlogics.com/solutions/azureoffice365/

Authlogics

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866