Modern Authentication in Microsoft 365 Key to Improved Security

In February 2021, Microsoft announced an updated schedule for removing support for basic authentication. That is, in the second half of 2021 modern authentication will become the access method for Office apps. While Microsoft has granted customers additional time to implement modern authentication, organizations need to prepare now.

The process of implementing modern authentication methods and disabling basic authentication can prove complex. Various versions of Office handle modern authentication differently. Additionally, while challenges with application and protocol support have eased, mobile apps still give some trouble. And organizations need to avoid a key security risk.

Modern Authentication vs. Basic Authentication

First, users must understand the difference between modern authentication and basic authentication. Basic authentication requires a username and password to authenticate each user. This means that the application must store those credentials somewhere. It also means that a hacker who gains that information can easily wreak havoc within the system.

On the other hand, modern authentication methods provide much greater security without the use of risky passwords. These methods include options such as multi-factor authentication (MFA), certificate-based authentication (CBA) and smart cards. In addition to improved security, modern authentication in Microsoft 365 also allows for conditional access policies.

End of Support for Basic Authentication in Microsoft 365

Since August 2017, Microsoft has supported both modern authentication and basic authentication. However, in 2019, the company announced that it planned to discontinue support for basic authentication in autumn 2020. With the onset of the pandemic, that date has shifted to the latter half of 2021. This has significant implications for Microsoft customers.

Every application or service that connects to Microsoft 365 must authenticate. As soon as basic authentication is disabled, any services that depend on Microsoft 365 will no longer work. While Microsoft plans to warn customers several months before completely disabling basic authentication, organizations need to act sooner rather than later.

Implications for Older Versions of Office and Windows Server

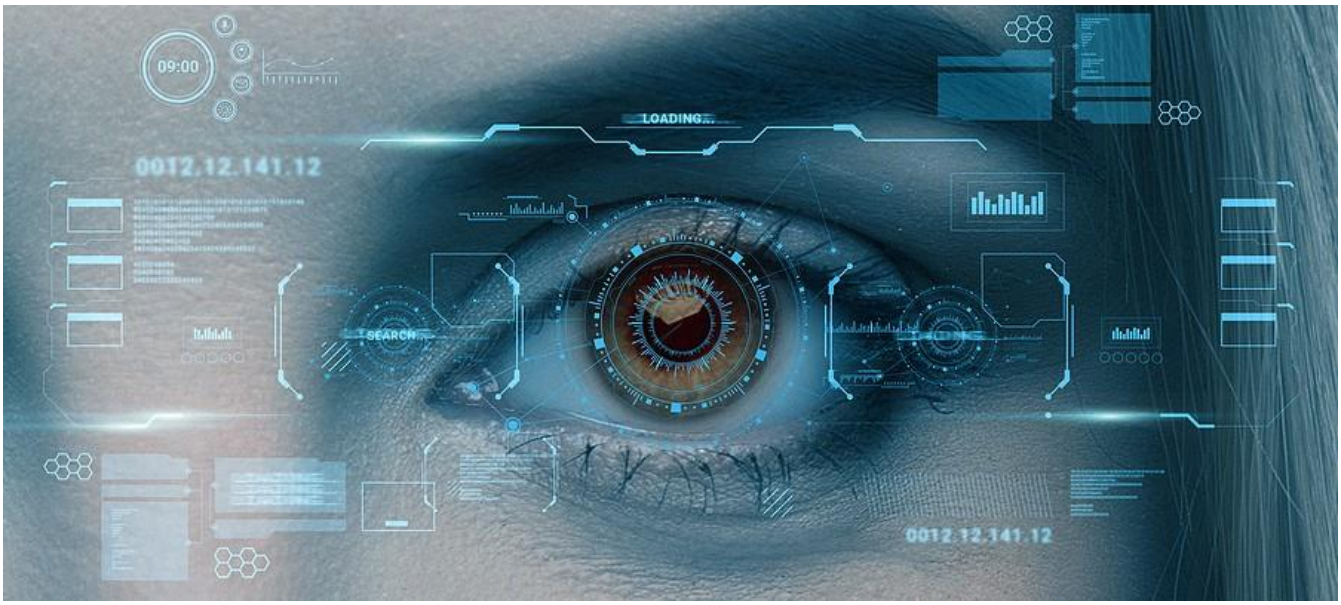
Organizations preparing to implement modern authentication should know that not all versions of Office support it. Office 2016 and higher include modern authentication by default. However, organizations using Office 2013 will have to set registry keys for each device that will use modern authentication. And older versions of Office do not support modern authentication.

Further, versions of Windows Server earlier than 2012 R2 do not support modern authentication. And email clients other than Outlook offer mixed support. Consequently, moving to modern authentication may require upgrades or additional steps in some cases.

Modern Authentication for Mobile Users

Experience shows that moving to modern authentication can prove somewhat tricky for mobile users. The current versions of IOS and Android support modern authentication nicely, as does Outlook mobile.

However, native email clients can get messy, even when they technically support modern authentication. For a clean implementation, consider forcing users to use the Outlook app instead of native email clients.



Close a Critical Security Loophole

Basic authentication presents a significant data security risk. In fact, Verizon's 2021 Data Breach Investigations Report indicates that stolen credentials account for 61 percent of security breaches. Thus, any device or service in the organization that still uses basic authentication represents a backdoor for hackers.

As you implement modern authentication, be sure to locate and disable all instances of basic authentication within the system. This will ensure that hackers cannot bypass passwordless authentication with stolen credentials. The Azure AD Sign-In log can help highlight holes that need to be closed.

Ensure a Smooth Transition

As with any change, moving from basic authentication to modern authentication can involve some hiccups along the way. Organizations can ease the way with proper preparation. Check existing systems and devices for compatibility with modern authentication. Locate all instances of basic authentication. And communicate the change effectively with end users.

The consultants at eMazzanti can assist. With deep experience in Microsoft and data security, we can help you plan effectively and catch any potential gotchas in advance.