Deprecation of Basic authentication in Exchange Online

For many years, applications have used Basic authentication (also known as Legacy authentication) to connect to servers, services, and API endpoints. Basic authentication simply means the application sends a username and password with every request, and those credentials are also often stored or saved on the device. Traditionally, Basic authentication is enabled by default on most servers or services, and is simple to set up.

Simplicity isn't at all bad, but Basic authentication makes it easier for attackers to capture user credentials (particularly if the credentials are not protected by TLS), which increases the risk of those stolen credentials being reused against other endpoints or services. Furthermore, the enforcement of multifactor authentication (MFA) is not simple or in some cases, possible when Basic authentication remains enabled.

Basic authentication is an outdated industry standard. Threats posed by it have only increased since we originally announced that we were going to turn it off. There are better and more effective user authentication alternatives.

We actively recommend that customers adopt security strategies such as Zero Trust (Never Trust, Always Verify), or apply real-time assessment policies when users and devices access corporate information. These alternatives allow for intelligent decisions about who is trying to access what from where on which device rather than simply trusting an authentication credential that could be a bad actor impersonating a user.

With these threats and risks in mind, we're taking steps to improve data security in Exchange Online.

What we are changing

We're removing the ability to use Basic authentication in Exchange Online for Exchange ActiveSync (EAS), POP, IMAP, Remote PowerShell, Exchange Web Services (EWS), Offline Address Book (OAB), Outlook for Windows, and Mac.

We're also disabling SMTP AUTH in all tenants in which it's not being used.

This decision requires customers to move from apps that use basic authentication to apps that use Modern authentication. Modern authentication (OAuth 2.0 token-based authorization) has many benefits and improvements that help mitigate the issues in basic authentication. For example, OAuth access tokens have a limited usable lifetime, and are specific to the applications and resources for which they are issued, so they cannot be reused. Enabling and enforcing multifactor authentication (MFA) is also simple with Modern authentication.

When will this change take place?

We've already started making this change. New Microsoft 365 tenants are created with Basic authentication already turned off as they have Security defaults enabled.

Beginning in early 2021, we started to disable Basic authentication for existing tenants with no reported usage. We always provide Message Center notifications to any customer prior to Basic authentication being disabled in their tenant.

In September 2021, we announced that effective **October 1, 2022**, we will begin disabling Basic authentication for Outlook, EWS, RPS, POP, IMAP, and EAS protocols in Exchange Online. SMTP Auth will also be disabled if it is not being used.

Apple iOS Mail Client and Modern Authentication

The Apple email client for iOS is a popular email client for both Exchange Server and Exchange Online. Despite being an iPhone user, I prefer Outlook mobile. It's a better mail client for Exchange Online as it supports features like **delegated access**, sensitivity labels, and **shared mailboxes**.

The Apple mail client uses EAS to connect to Exchange, and EAS is one of the protocols that won't support basic authentication after October 2022. Checking **Apple's documentation**, we learn that Apple has made arrangements to upgrade devices running iOS 14 and iPadOS 14 to use modern authentication automatically (Figure 1).

Figure 1: Apple documentation about OAuth support in iOS for Exchange Online

The good thing is that Apple has done the work to make sure that its mail client can use modern authentication to connect to Exchange Online. Everything seems sunny, until you learn that some of the information presented in the documentation is incorrect (Apple has been informed and is apparently in the process of refreshing their content. In a nutshell, the correct position is that if an account for Exchange was created on an iOS or iPadOS email client before **Apple added**

[support for OAuth (iOS 12](#)), the connection uses basic authentication. This is logical because basic authentication was the only connection possible at the time.

To move to modern authentication, users must remove their Exchange account from the mail app configuration and re-add Exchange to the mail app. When the mail app running on iOS 12 or above adds an Exchange account, it detects that modern authentication is available and will use it. It's not enough to upgrade to the latest version of iOS as this action preserves the mail app configuration. Likewise, if you buy a new iOS device and restore your settings on that device from an iCloud backup of the old device, the restore preserves the mail app configuration

Android tablet and phone with Microsoft 365

Office for Android™ (including Outlook for Android) can be installed on tablets and phones running any of the supported versions of Android and have an ARM-based or Intel x86 processor. Starting on July 1, 2019, support will be limited to only the last four major versions of Android.

Information Current as of 11/30/2021

Sources:

MS Depreciation of Basic Authentication.

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

MS Exchange Doc Apple

https://office365itpros.com/2021/10/18/old-apple-mail-clients-exchange-online/

Apple Support Doc.

https://support.apple.com/en-ie/guide/deployment-reference-macos/apd46055de62/web

Microsoft Apple IOS Version supported.

https://support.microsoft.com/en-us/office/what-version-of-ios-does-your-app-support-0cd1b3a8-d8bd-44d8-b874-f4bed8b90eaa