

Advisory: Upcoming Cloud Service Authentication Changes

Sharing Guideline: TLP:WHITE

The [REN-ISAC Technical Advisory Group](#) would like to call attention to announced changes of authentication services from widely-used cloud providers.

Executive Summary

Microsoft and Google have both published plans to disable the ability to use “legacy” logins for several services. This is because these legacy authentication mechanisms do not support many of today’s security standards, notably Multi-Factor Authentication (MFA).

Further Details

[Microsoft Legacy Login](#)

Terminology: Microsoft calls legacy authentication “Basic Authentication” (Basic Auth) as opposed to “Modern Authentication” (Modern Auth or OAuth).

What this affects and specific [user impacts](#)?

- Exchange Web Services (EWS)
- Exchange ActiveSync (EAS)
- Post Office Protocol (POP)
- Internet Message Access Protocol (IMAP)
- Remote PowerShell
- Remote Procedure Call (RPC)
- Offline Address Book (OAB)

What this excludes?

- Basic Auth for Simple Mail Transfer Protocol Authentication (SMTP AUTH) – Currently, there is [no plan](#) to disable Basic Auth for SMTP AUTH. While Exchange Online [SMTP AUTH now supports OAuth](#), many devices do not include the necessary client functionality. Manually [disabling SMTP AUTH](#) is recommended across your organization. [Re-enables should be limited to only specifically required mailboxes](#) such as scan-to-email multi-function devices.

What services may break?

- Exchange Online Remote PowerShell using *New-PSSession* rather than the newer *Connect-ExchangeOnline* cmdlet
- Mobile devices checking email configured with Exchange ActiveSync
- Outlook 2010 or older, which do not support Modern Auth

When this may impact services?

- Q2 2022: Sometime during this period, Microsoft will selectively pick tenants and disable Basic Auth for all affected protocols for a period of 12-48 hours. After this duration, Basic Auth for these protocols will be re-enabled if the tenant admin has not already done so.
- October 1, 2022: Microsoft will begin to permanently disable Basic Auth for all affected protocols in all tenants regardless of usage.

How to identify potentially affected clients and block Basic Auth sooner?

- Microsoft has a [guide for using Azure AD to find legacy authentication](#) sign-ins, as well as a matrix summarizing [proactively disabling Basic Auth](#).

Additional Resources:

- A [Guide to Shift Away from Legacy Authentication Protocols](#) in Microsoft 365

[Google Legacy Login](#)

Terminology: Google calls legacy authentication “Less secure app access.”

What this affects?

- IMAP
- Calendar Distributed Authoring and Versioning (CalDAV)
- vCard Distributed Authoring and Versioning (CardDAV)
- Exchange ActiveSync (Google Sync)
- Mobile Device Management (MDM) configuration of the above

What this excludes?

- SMTP Auth

When this may impact services?

- Google originally intended to disable Less Secure Apps for all G Suite accounts on February 15, 2021. However, once the pandemic hit, Google [suspended this effort until further notice](#). Their announcements do imply an intent to resume this endeavor at some point, though they promise a 12-month notice before any future cutoff date. REN-ISAC will continue to monitor and summarize information as it’s released by Google.