IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Action Recommended: Switch to Modern Authentication in Exchange Online Before Basic Authentication Deprecation

DEFEND TODAY, SECURE TOMORROW

June 2022

OVERVIEW

This fact sheet provides guidance on how to determine whether and to what extent your organization is using Basic Authentication ("Basic Auth") in Exchange Online and how to switch to Modern Authentication ("Modern Auth") before Microsoft begins permanently disabling Basic Auth on October 1, 2022.[1] Basic Auth is a legacy authentication method that requires the user's password to be sent with each authentication request. Protocols that can use Basic Auth include Post Office Protocol/Internet Message Access Protocol (POP/IMAP), Exchange Web Services (EWS), ActiveSync, and Remote Procedure Call over HTTP (RPC over HTTP). **Note: Although this guidance is tailored to federal civilian executive branch (FCEB) agencies, all organizations should take urgent steps to switch to Modern Auth before October 1.**

CISA urges all organizations to expedite migration to Modern Auth, as Basic Auth does not support multifactor authentication (MFA), which is required for FCEB agencies per Executive Order 14028, "Improving the Nation's Cybersecurity." Additionally, according to Microsoft,

- *More than 99 percent of password spray attacks use legacy authentication protocols.*
- *More than 97 percent of credential stuffing attacks use legacy authentication.*
- *There are 921 password attacks every second—nearly doubling in frequency over the past 12 months.*[2]
- *Azure AD accounts in organizations that have disabled legacy authentication experience 67 percent fewer compromises than those where legacy authentication is enabled.*[3]

IMMEDIATE ACTION RECOMMENDED

Federal agencies should determine their use of Basic Auth and migrate users and applications to Modern Auth. After completing the migration to Modern Auth, agencies should block Basic Auth. Basic Auth is most likely used by legacy applications or custom-built business applications. Many user-facing applications, such as Outlook Desktop and Outlook Mobile App, have already been moved to Modern Auth by agency implementation of Microsoft security updates.

Determine Usage

First, review Azure Active Directory (AAD) sign-in logs to identify applications and users authenticating with Basic Auth. **Note**: Sign-in logs are retained for 7 days for AAD Free and 30 days for AAD P1/P2 users.[4] M365 G3 licenses include P1 and M365 G5 includes P2.[5]

To review sign-in logs:

- Access AAD sign-in logs.
- Click **Add filters.**
- Select **Client app** in the dropdown.
- Click **Apply.**

[1] "Basic Authentication Deprecation in Exchange Online," Microsoft, May 3, 2022, https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-may-2022/ba-p/3301866.
[2] "This World Password Day consider ditching passwords altogether," Microsoft, May 5, 2022, https://www.microsoft.com/security/blog/2022/05/05/this-world-password-day-consider-ditching-passwords-altogether.
[3] "How to: Block legacy authentication access to Azure AD with Conditional Access," Microsoft, June 2, 2022, https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication.
[4] "How long does Azure AD store reporting data?" Microsoft, February 8, 2022, https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data.
[5] "Product names and service plan identifiers for licensing," Microsoft, May 2, 2022, https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-service-plan-reference.

- Click the new **Client app** bubble.
- Select the following values grouped under **Legacy Authentication Clients:**
    - Autodiscover
    - Exchange ActiveSync
    - Exchange Online PowerShell
    - Exchange Web Services
    - IMAP
    - MAPI Over HTTP
    - Offline Address Book
    - Outlook Anywhere (RPC over HTTP)
    - POP
    - Reporting Web Services
    - SMTP
    - Universal Outlook
- Review the **User sign-ins (interactive)**, **User sign-ins (non-interactive)**, **Service Principal sign-ins,** and **Managed identity sign-ins** tabs.

Note: If searching sign-in logs that have been exported from AAD (i.e., to a Security Information and Event Management [SIEM] system), filter for the above values on the **ClientAppUsed** field.

Review the resulting values, which are applications and users that are using Basic Auth. If there are too many values to review in the browser, download results as a CSV or JSON file to review offline. **Note:** Microsoft also sends monthly Message Center posts to organizations using Basic Auth.

Move to Modern Auth

Create a plan for moving the identified applications and users to Modern Auth by following the protocol recommendation in Microsoft's Deprecation of Basic Authentication in Exchange Online documentation as well as Microsoft's Exchange Team blog post, Basic Authentication Deprecation in Exchange Online.

Block Usage

Agencies can implement either of the two primary methods for blocking usage of Basic Auth in Exchange Online: **1) create an authentication policy in Exchange Online,** or **2) create a Conditional Access policy in AAD**.
Note: Agencies using Basic Auth to authenticate to on-prem Exchange Servers should also move to hybrid modern authentication.

Implement Authentication Policy

Authentication policies block Basic Auth before authentication occurs and are set across an organization. To implement an authentication policy for all Exchange Online mailboxes:

1. Navigate to the M365 Admin Center's Modern Authentication Page: https://admin.microsoft.com/#/homepage/:/Settings/L1/ModernAuthentication.

2. Ensure **Turn on modern authentication for Outlook 2013 for Windows and later** is checked. This is the default setting.

3. Uncheck every protocol under **Allow access to basic authentication protocols.**

4. Click **Save**.

For additional guidance, see Microsoft's Disable Basic Authentication in Exchange Online documentation.

Create Conditional Access Policy

Conditional Access policies block Basic Auth after authentication has occurred, as the policy is applied after the first factor is satisfied. Policies can be targeted to specific applications (e.g., Exchange), users, or groups and can be configured via the AAD Admin Center. For implementation instructions, see Microsoft's Directly blocking legacy authentication documentation. **Note:** Conditional Access policies require an AAD P1 or higher license.

FOR MORE INFORMATION

For complete information, CISA recommends agencies review Microsoft's Deprecation of Basic Authentication in Exchange Online documentation and the associated Exchange Team blog post, Basic Authentication Deprecation in Exchange Online.

REVISIONS

July 22, 2022

- Removed statement that Authentication Policies can be set per mailbox; these can only be set across the organization.
- Added the full list of Client Apps to select in Azure AD sign-in logs.
- Added statement on how to search exported AAD sign-in logs.
- Added note to check all tabs in the Sign-in logs page.