# Cyber Snapshot

*Exploring and Assessing Current Topics*

MICHIGAN CYBER COMMAND CENTER (MC3)

December 18, 2020
CS-09-2020

## Legacy Authentication – Bypassing 2FA/MFA

**OVERVIEW:**

Microsoft legacy authentication is a basic authentication service used when connecting to cloud-based services. Legacy authentication uses protocols such as POP, SMTP, IMAP and MAPI. The problem with allowing legacy authentication is it does not enforce the use of two-factor authentication (2FA) or multi-factor authentication (MFA), which increases the risk of a possible compromise. Even if MFA/2FA policy is enabled, a bad actor can authenticate using legacy authentication protocols. This makes legacy authentication a primary target of password spray and/or credential stuffing attacks.

**ADDRESSING THE ISSUE:**

To protect yourself from falling victim to malicious actors, the MC3 recommends disabling legacy authentication and using modern authentication instead. Prior to doing this, it is best to identify any applications or devices which use legacy authentication and how blocking it may affect these. To do this, administrators can review the organization's Azure Active Directory sign-in page and then filter the logins using client apps to see which applications use legacy authentication.


Another way to see how this will affect users is to create an access policy to block legacy authentication in report-only mode, which will block client applications not using modern authentication. This will allow you to monitor the real time side effects of blocking legacy authentication without disrupting the users. After letting this run for a few days, use the conditional access insights workbook to see which users would have been blocked by the policy. Once you have an idea of what users and applications are still using legacy authentication, the next step is blocking it. To directly block legacy authentication, change the conditional access policy from report only mode to on. In the event you have users who you are unable to block legacy authentication for, create a separate access policy for the users who still require legacy authentication versus the ones who do not. This will provide time to shift the applications/users who require legacy authentication over to modern authentication.

It is possible to indirectly block legacy authentication on the service side by ensuring applications using legacy authentication are not bypassing MFA/2FA. To do this, apply policies with grant controls so applications using legacy authentication will not satisfy the grant control. The only problem with this is you may block protocols like EWS and MAPI which support both legacy and modern authentication.

**ADDITIONAL INFORMATION:**

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-block-legacy-authentication
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/new-tools-to-block-legacy-authentication-in-your-organization/ba-p/1225302