

- [Exchange Online: Basic Auth Depreciation](#)
 - [Prerequisites/Notes:](#)
 - [Background:](#)
 - [Objective:](#)
 - [Make sure Modern Auth is Enabled](#)
 - [Enable Basic Auth \(Not Recommended EOL 2023\)](#)
 - [Disable/Block Basic Auth](#)
 - [Links](#)

Exchange Online: Basic Auth Depreciation

Prerequisites/Notes:

1. Outlook must be versions 2013 or newer to be in compliance.
2. Must use Exchange Online PowerShell V2 Modules to access Exchange remotely via PowerShell going forward.
3. Must be an [Exchange Admin or higher](#) to make these changes.
4. MFA enabled
5. Modern Authentication must be enabled.
6. Conditional Access Policies can take up to 24 hours to take effect.

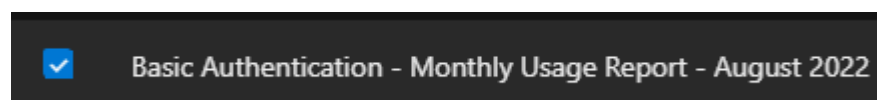
Background:

In early 2019 MS announced retirement for Basic Auth for Legacy protocols. (MAPI, RPC, (OAB) Offline Address Book, (EWS) Exchange Web Services, POP, IMAP, (EAS) Exchange ActiveSync, and Remote PowerShell) but not for SMTPAUTH.

Starting October 1st, 2022 MS will start randomly turning off Basic Auth for the above protocols. They state they will also notify the Tenancy a week ahead as well as on the day via the [ServiceHealth Dashboard](#). MS also stated they will allow post October 1st, 2020 a onetime re-enablement. You also can pre-opt out of having a proto disabled if you do so before October 1st, 2022, but once 2023 rolls around you will no longer be able to re-enable or opt-out again.

If you have already blocked Basic Auth Proto dependencies then you have nothing left to do. If you are not sure, check your "Monthly Usage Reports" in the [Message Center](#).

Search for "Basic Auth"



This section will let you know what you need to change.



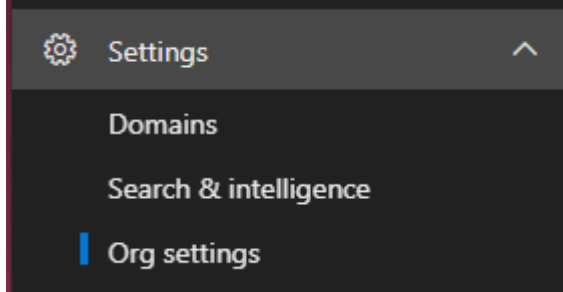
Anything with a number greater than 0 will need addressed.

Objective:

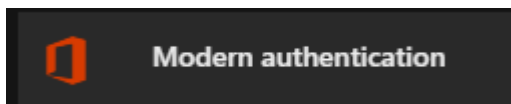
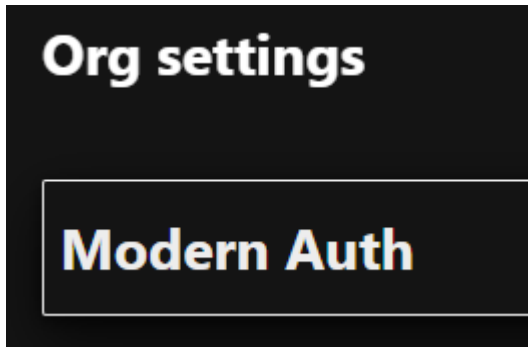
1. Enable MFA, Enabled Modern Auth, and all Basic Auth protocols are disabled/blocked ASAP.

Make sure Modern Auth is Enabled

1. In the [MAC \(Microsoft Admin Center\)](#) go to Settings > Org Settings,




and search for "Modern Auth.



2. Then click on it and make sure "Turn on modern auth" is enabled. You may also have basic auth already disabled. As the tan box states, make sure before disabling Modern Auth on a proto, that it is not being used. Refer to the "Basic Auth Monthly Report" above. These will need turned off sooner than later.

☒ Turn on modern authentication for Outlook 2013 for Windows and later (recommended)

 Before you turn off basic authentication for protocols, view your sign-in reports in the Azure portal to make sure people in your organization aren't using them.

Allow access to basic authentication protocols

☐ Outlook client
Includes Exchange Web Services, MAPI over HTTP, Offline Address Book and Outlook Anywhere protocols

☐ Exchange ActiveSync (EAS)
Used by some email clients on mobile devices.

☐ Autodiscover
Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.

☐ IMAP4
Used by IMAP email clients.

☐ POP3
Used by POP email clients.


☐ Authenticated SMTP
Used by POP and IMAP clients to send email messages.

☐ Exchange Online PowerShell
Used to connect to Exchange Online with remote PowerShell. [Learn more](#)

Save

Enable Basic Auth (Not Recommended EOL 2023)

1. In the [MAC \(Microsoft Admin Center\) home page](#), click on "Help and Support" in the lower left.

 Help & support

4. Search for "Basic Auth Enable".

How can we help?

Tell us your problem so we can get you the right help and support.

Enable Basic Auth on EXO



5. Then run the test,

Run diagnostics

We understand you would like to initiate a request to update the Basic authentication settings for protocols.

Let us help by running some tests.

Run Tests

6. Then pick the proto you wish to enable.

Run diagnostics

These are the current Basic authentication settings:

Basic authentication is disabled for the following legacy protocols:

- Post Office Protocol (POP3, used by email clients)
- Internet Message Access Protocol (IMAP, used by email clients)
- Exchange Online Remote PowerShell (used for executing scripts)
- MAPI (used by all versions of Outlook for Windows)
- Offline Address Book (OAB, used by Outlook for Windows)
- RPC (used by older versions of Outlook for Windows)

You can use the drop-down below to indicate which protocols you wish to exclude from being secured. Basic authentication will be disabled for those protocols at a later date.

Protocol to Opt Out *

▼

SMTP

POP

IMAP

Exchange ActiveSync

Exchange Web Services (EWS)

Exchange Online Remote PowerShell

Outlook (includes EWS, MAPI, RPC and OAB)

okie

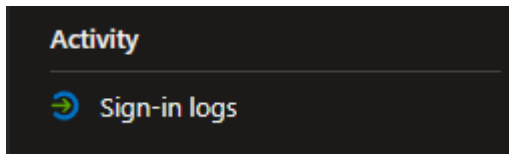
Disable/Block Basic Auth

1. First lets double check to make sure users are not still using some Basic Auth methods. [In Azure A/D](#), go to "All Services",

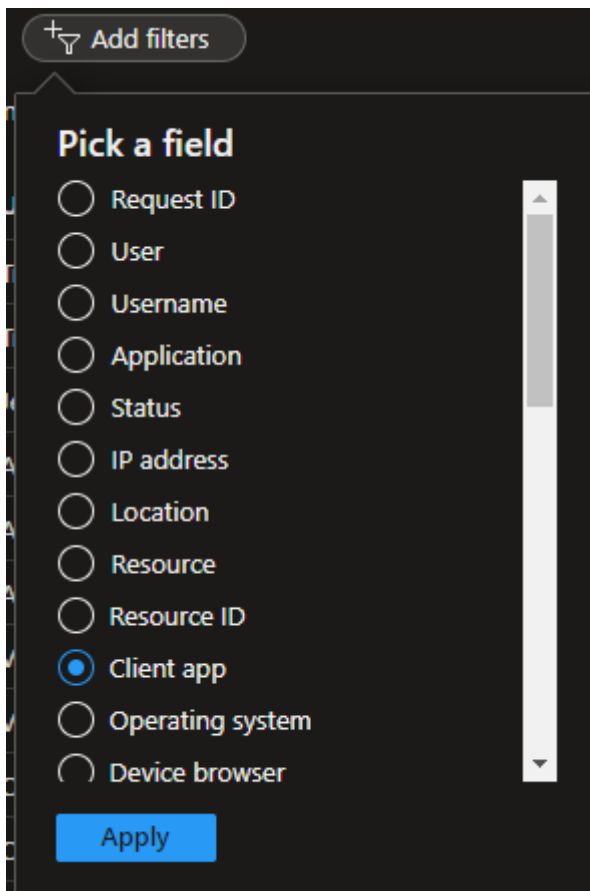
☰ All services

Under the "Identity" section, click "Users"

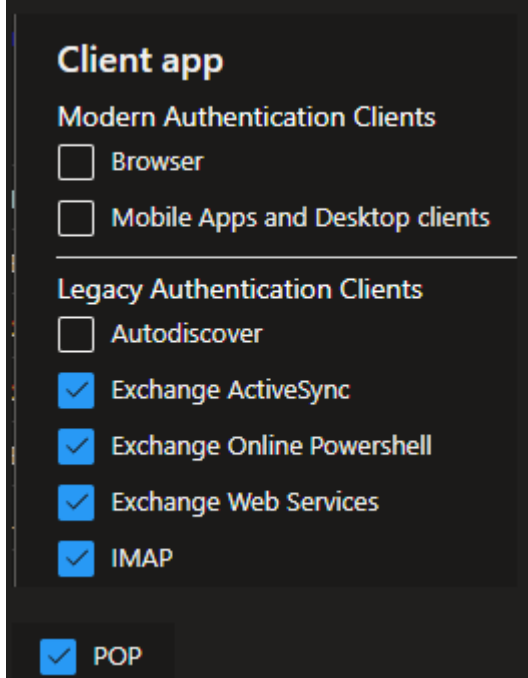
Then under the "Activity" section, click "Sign-in Logs"



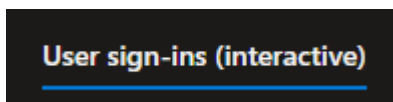
2. On the "Add Filters" button, select "Client App".



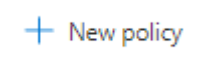
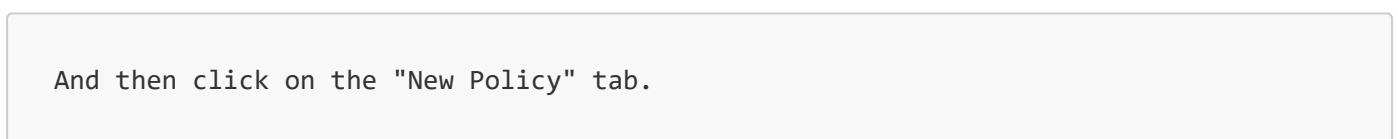
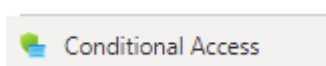
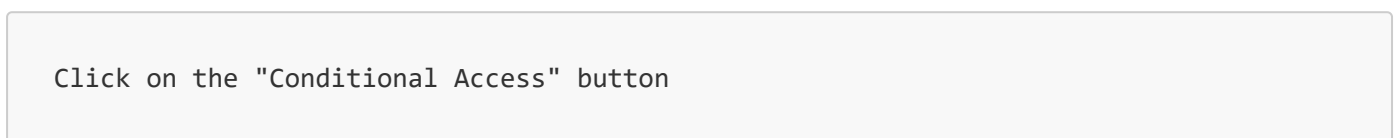
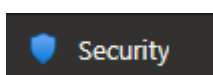
3. Then on the new Column filter check Exchange ActiveSync, Exchange Online PowerShell, Exchange Web Service, IMAP, and POP.



4. Unfortunately you will need to open each Login type and view its protocol. Comb through to make sure no actual users are using Basic Auth.



5. Now that we have double checked ourselves, lets create a Conditional Access Policy to block Basic Auth methods for Cloud apps. On the [Azure A/D homepage](#), go to the "Security" button.



6. Under the "Name" pulldown let's call it "Basic Auth Block".

Name *

Basic Auth Block



7. On the "Assignment" pulldown, select "Users and Groups", then pick "All Users".

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

What does this policy apply to?

Users and groups



Include Exclude



None



All users



Select users and groups



Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

8. Then on the "Cloud Apps or Actions" pulldown, pick Cloud apps.

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps



Include Exclude



None



All cloud apps



Select apps



Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

9. Under the "Conditions" pull down, select "Client Apps". We have two ways of setting this up. Indirectly blocking Basic Auth or Directly blocking Basic Auth.

Directly blocking Basic Auth: This is if you know you don't have anything using Basic Auth, that you should have confirmed above. A side note when checking "Other Clients", this blocks "Exchange Online PowerShell" and "Dynamics 365" using Basic Auth as well as older devices that do not support MFA.

Slide the "Configure" button to "Yes" and make sure "Exchange Active Sync Clients" and "Other Clients" are the only ones checked.

Client apps ✕

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

Yes No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

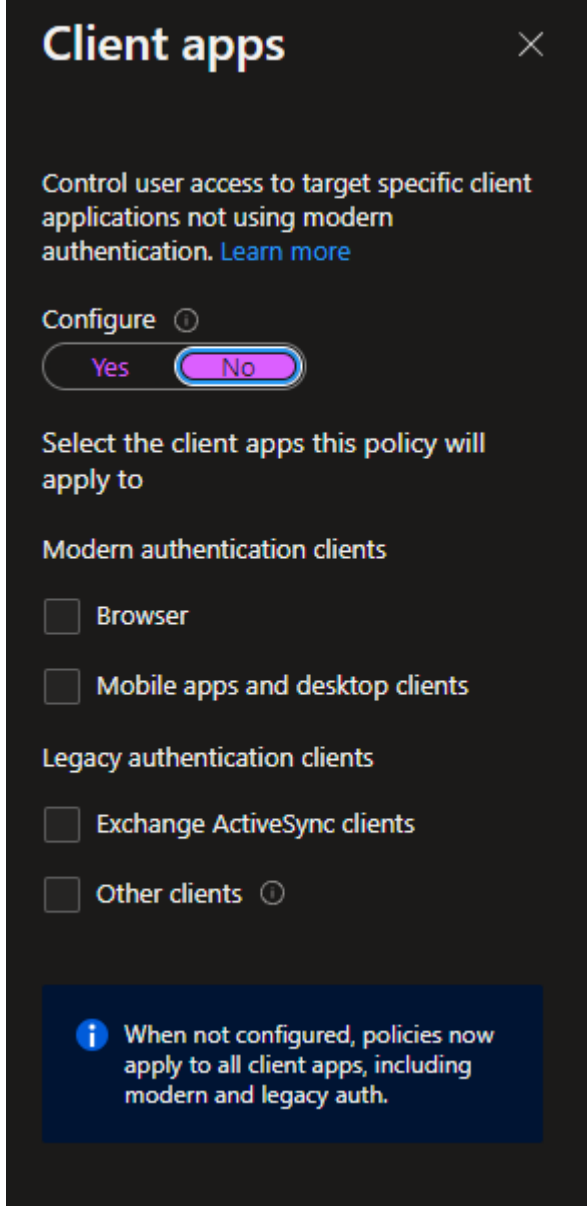
☐ Mobile apps and desktop clients

Legacy authentication clients

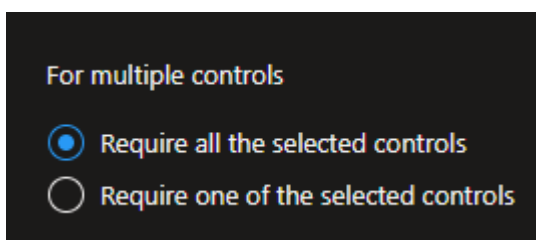
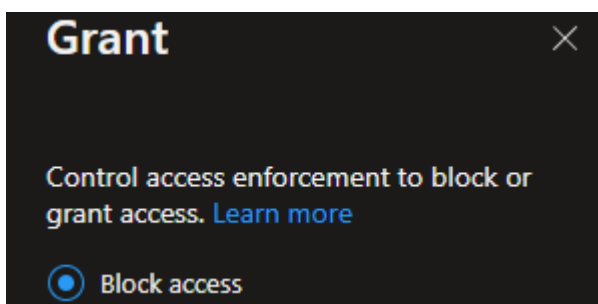
☒ Exchange ActiveSync clients

☒ Other clients ⓘ

Indirectly blocking Basic Auth: This is if you know you have legacy devices that still require Basic Auth aka don't support MFA and you want to not block it. Not shaming here but this is considered "Technical Debt" and should be addressed sooner than later. Keep the Slider set to "No".

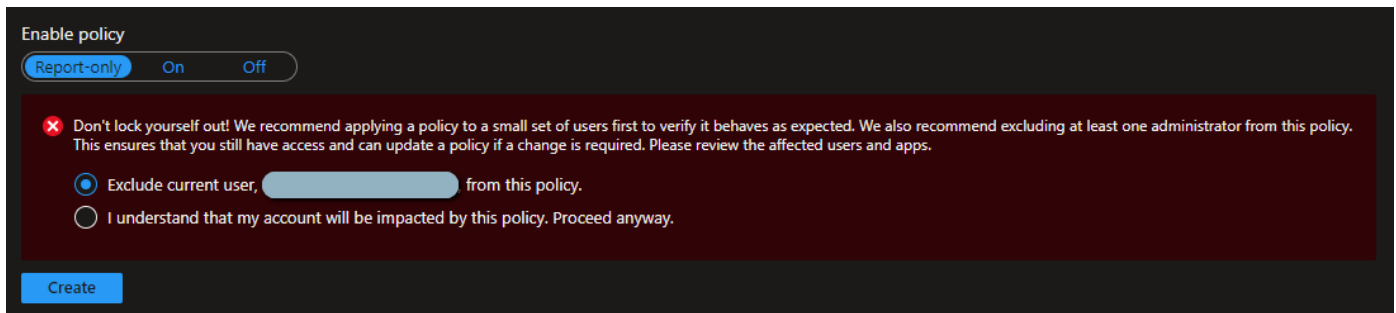


10. On "Access Control" select "Block Access" as we are trying to block Basic Auth and leave "Require all the selected Controls" as default.



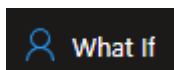
11. Then don't select anything for "Session Control".
12. Now make sure you create your Conditional Access Policy as a "Report only" and review it with the What if Tool" before turning it on. There is also a new feature on

excluding the person who created the "Conditional Access Policy" Keep in mind what option you make. Report only will not take effect until its changed to "On".

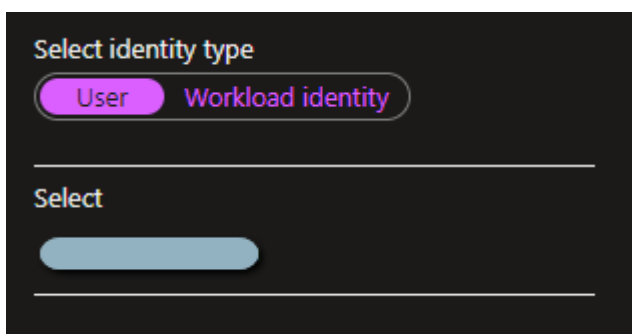


"What If" tool to test a Conditional Access Policy

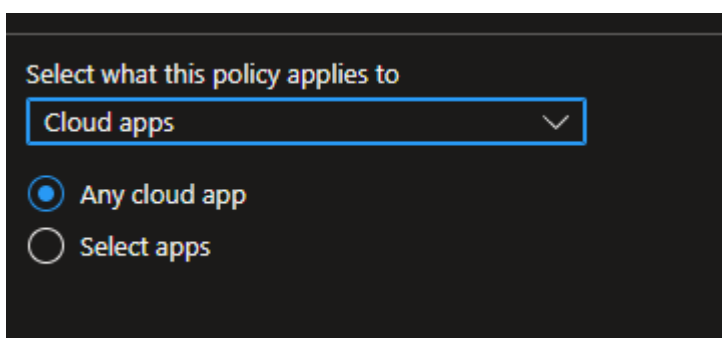
1. Now that our "Block Basic Auth Conditional Access Policy" is in read only mode, let see how it effects a user. First click on the "What If" button. (Azure A/D Home > Security > Conditional Access > What If)



2. Then under the "Users and Workload Identities" section select "Users" and pick a user you know will be effected in your Org.



3. On the "Cloud Apps, Actions, or Authentication Context" section, make sure the pull down is set to "Cloud Apps" and select "Any Cloud App" and leave the other sections blank.



Depending on how you blocked Basic Auth you can also check one or multiple Apps specifically.

Select what this policy applies to

Cloud apps

☐ Any cloud app

☒ Select apps

Select

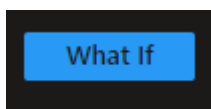
Office 365 Exchange Online and 2 more

ON OneDrive ...

Microsoft Teams ...

Office 365 Exchange Online ...

4. Now press the "What If" button,



You should now see our Conditional Access Policy blocking Basic Auth.

Policies that will apply

Search

Policy Name ↑↓

Basic Auth Block

If your Policy is showing under "Policies that don't Apply" go back over the Disable/Block Basic Auth section again.

If you are new to Conditional Access or What If, I encourage you to create a fake Org User and External User to test signing in to Apps in various ways when the Policy is turned on post What If testing to see how things act by signing in as them.

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
[Learn more](#)

Name *

Basic Auth Org Test User Test

Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select

1 user

TO

Test Org User

Links

1. Basic Auth depreciation: <https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437>

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online?WT.mc_id=365AdminCSH_SupportCentral

2. MAC Home Page:

<https://admin.microsoft.com/#/homepage>

3. MAC Service Health Dashboard:

<https://admin.microsoft.com/AdminPortal/home#/servicehealth>

4. MAC Message Center :

<https://admin.microsoft.com/AdminPortal/home#/MessageCenter>

5. Disable/Enable Basic Auth in Exchange Online : <https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online>

<https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

6. PowerShell Remoting V2 Module: <https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps>

7. MAC Admin Roles: <https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

8. Azure A/D Portal:

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview