# https://upload.wikimedia.org/wikipedia/commons/7/74/Office_365_logo.png

# Baseline policy Block legacy authentication (preview) - Azure Active Directory

**In this article**

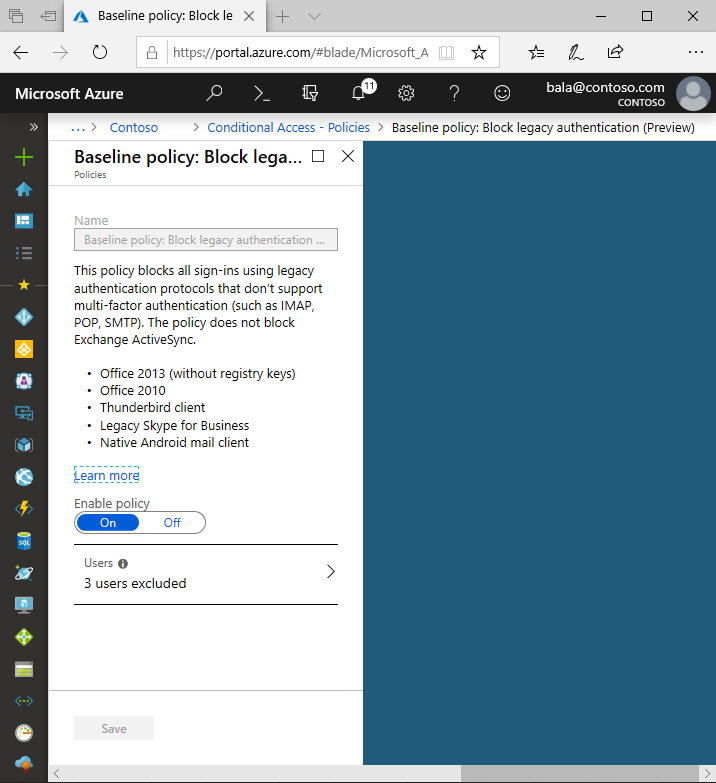
1. [Identify legacy authentication use](about:reader?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Fconditional-access%2Fhowto-baseline-protect-legacy-auth#identify-legacy-authentication-use)
2. [Moving away from legacy authentication](about:reader?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Fconditional-access%2Fhowto-baseline-protect-legacy-auth#moving-away-from-legacy-authentication)
3. [Enable the baseline policy](about:reader?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Fconditional-access%2Fhowto-baseline-protect-legacy-auth#enable-the-baseline-policy)
4. [Next steps](about:reader?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Fconditional-access%2Fhowto-baseline-protect-legacy-auth#next-steps)

To give your users easy access to your cloud apps, Azure Active Directory (Azure AD) supports a broad variety of authentication protocols including legacy authentication. Legacy authentication is a term that refers to an authentication request made by:

* Older Office clients that do not use modern authentication (for example, Office 2010 client)
* Any client that uses legacy mail protocols such as IMAP/SMTP/POP3

Today, majority of all compromising sign-in attempts come from legacy authentication. Legacy authentication does not support multi-factor authentication (MFA). Even if you have an MFA policy enabled on your directory, a bad actor can authenticate using a legacy protocol and bypass MFA.

The best way to protect your account from malicious authentication requests made by legacy protocols is to block these attempts all together. To make it easier for you to block all login requests made by legacy protocols, we created a baseline policy that does just that.



**Block legacy authentication** is [baseline policy](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-baseline-protection) that blocks all authentication requests made from legacy protocols. Modern authentication must be used to successfully sign in for all users. Used in conjunction with the other baseline policies, all requests coming from legacy protocols will be blocked and all users will be required to MFA whenever required. This policy does not block Exchange ActiveSync.

**Identify legacy authentication use**

Before you can block legacy authentication in your directory, you need to first understand if your users have apps that use legacy authentication and how it affects your overall directory. Azure AD sign-in logs can be used to understand if you’re using legacy authentication.

1. Navigate to the **Azure portal** > **Azure Active Directory** > **Sign-ins**.
2. Add the Client App column if it is not shown by clicking on **Columns** > **Client App**.
3. Filter by **Client App** > **Other Clients** and click **Apply**.

Filtering will only show you sign-in attempts that were made by legacy authentication protocols. Clicking on each individual sign-in attempt will show you additional details. The **Client App** field under the **Basic Info** tab will indicate which legacy authentication protocol was used.

These logs will indicate which users are still depending on legacy authentication and which applications are using legacy protocols to make authentication requests. For users that do not appear in these logs and are confirmed to not be using legacy authentication, implement a conditional access policy or enable the **Baseline policy: block legacy authentication** for these users only.

**Moving away from legacy authentication**

Once you have a better idea of who is using legacy authentication in your directory and which applications depend on it, the next step is upgrading your users to use modern authentication. Modern authentication is a method of identity management that offers more secure user authentication and authorization. If you have an MFA policy in place on your directory, modern authentication ensures that the user is prompted for MFA when required. It is the more secure alternative to legacy authentication protocols.

This section gives a step-by-step overview on how to update your environment to modern authentication. Read through the steps below before enabling a legacy authentication blocking policy in your organization.

**Step 1: Enable modern authentication in your directory**

The first step in enabling modern authentication is making sure your directory supports modern authentication. Modern authentication is enabled by default for directories created on or after August 1, 2017. If your directory was created prior to this date, you’ll need to manually enable modern authentication for your directory using the following steps:

1. Check to see if your directory already supports modern authentication by running Get-CsOAuthConfiguration from the [Skype for Business Online PowerShell module](https://docs.microsoft.com/office365/enterprise/powershell/manage-skype-for-business-online-with-office-365-powershell).
2. If your command returns an empty OAuthServers property, then Modern Authentication is disabled. Update the setting to enable modern authentication using Set-CsOAuthConfiguration. If your OAuthServers property contains an entry, you’re good to go.

Be sure to complete this step before moving forward. It’s critical that your directory configurations are changed first because they dictate which protocol will be used by all Office clients. Even if you’re using Office clients that support modern authentication, they will default to using legacy protocols if modern authentication is disabled on your directory.

**Step 2: Office applications**

Once you have enabled modern authentication in your directory, you can start updating applications by enabling modern authentication for Office clients. Office 2016 or later clients support modern authentication by default. No extra steps are required.

If you are using Office 2013 Windows clients or older, we recommend upgrading to Office 2016 or later. Even after completing the prior step of enabling modern authentication in your directory, the older Office applications will continue to use legacy authentication protocols. If you are using Office 2013 clients and are unable to immediately upgrade to Office 2016 or later, follow the steps in the following article to [Enable Modern Authentication for Office 2013 on Windows devices](https://docs.microsoft.com/office365/admin/security-and-compliance/enable-modern-authentication). To help protect your account while you’re using legacy authentication, we recommend using strong passwords across your directory. Check out [Azure AD password protection](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad) to ban weak passwords across your directory.

Office 2010 does not support modern authentication. You will need to upgrade any users with Office 2010 to a more recent version of Office. We recommend upgrading to Office 2016 or later, as it blocks legacy authentication by default.

If you are using MacOS, we recommend upgrading to Office for Mac 2016 or later. If you are using the native mail client, you will need to have MacOS version 10.14 or later on all devices.

For Windows-based Outlook clients to use modern authentication, Exchange Online must be modern authentication enabled as well. If modern authentication is disabled for Exchange Online, Windows-based Outlook clients that support modern authentication (Outlook 2013 or later) will use basic authentication to connect to Exchange Online mailboxes.

SharePoint Online is enabled for modern authentication default. For directories created after August 1, 2017, modern authentication is enabled by default in Exchange Online. However, if you had previously disabled modern authentication or are you using a directory created prior to this date, follow the steps in the following article to [Enable modern authentication in Exchange Online](https://docs.microsoft.com/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online).

**Step 4: Skype for Business**

To prevent legacy authentication requests made by Skype for Business, it is necessary to enable modern authentication for Skype for Business Online. For directories created after August 1, 2017, modern authentication for Skype for Business is enabled by default.

To enable modern authentication in Skype for Business, we suggest you transition to Microsoft Teams, which supports modern authentication by default. However, if you are unable to tr at this time, you will need to enable modern authentication for Skype for Business Online so that Skype for Business clients starts using modern authentication. Follow these steps in the article [Skype for Business topologies supported with Modern Authentication](https://docs.microsoft.com/skypeforbusiness/plan-your-deployment/modern-authentication/topologies-supported), for steps to enable Modern Authentication for Skype for Business.

In addition to enabling modern authentication for Skype for Business Online, we recommend modern authentication be enabled for Exchange Online when enabling modern authentication for Skype for Business. This process will help synchronize the state of modern authentication in Exchange Online and Skype for Business online and will prevent multiple sign-in prompts for Skype for Business clients.

**Step 5: Using mobile devices**

Applications on your mobile device need to block legacy authentication as well. We recommend using Outlook for Mobile. Outlook Mobile supports modern authentication by default and will satisfy other MFA baseline protection policies.

In order to use the native iOS mail client, you will need to be running iOS version 11.0 or later to ensure the mail client has been updated to block legacy authentication.

**Step 6: On-premises clients**

If you are a hybrid customer using Exchange Server on-premises and Skype for Business on-premises, both services will need to be updated to enable modern authentication. When using modern authentication in a hybrid environment, you’re still authenticating users on-premises. The story of authorizing their access to resources (files or emails) changes.

Before you can begin enabling modern authentication on-premises, be sure you meet theIf you meet the requirements, you’re now ready to enable modern authentication on-premises.

Steps for enabling modern authentication be found in the following articles:

* [How to configure Exchange Server on-premises to use Hybrid Modern Authentication](https://docs.microsoft.com/office365/enterprise/configure-exchange-server-for-hybrid-modern-authentication)
* [How to use Modern Authentication (ADAL) with Skype for Business](https://docs.microsoft.com/skypeforbusiness/manage/authentication/use-adal)

**Enable the baseline policy**

The policy **Baseline policy: Block legacy authentication (preview)** comes pre-configured and will show up at the top when you navigate to the Conditional Access blade in Azure portal.

To enable this policy and protect your organization:

1. Sign in to the **Azure portal** as global administrator, security administrator, or conditional access administrator.
2. Browse to **Azure Active Directory** > **Conditional Access**.
3. In the list of policies, select **Baseline policy: Block legacy authentication (preview)**.
4. Set **Enable policy** to **Use policy immediately**.
5. Add any user exclusions by clicking on **Users** > **Select excluded users** and choosing the users that need to be excluded. Click **Select** then **Done**.
6. Click **Save**.