MoxiWorks

MoxiEngage Integration Process using Microsoft 365

Overview

MoxiEngage integrates directly with your brokerage's Microsoft 365 (formerly Office 365) account to provide your agents and support staff with consistent and convenient access to their information, while eliminating any need to enter the same information multiple times.

MoxiEngage relies upon Exchange application impersonation access to synchronize data and perform actions on behalf of individual users. Each MoxiEngage user account has an email address that corresponds to a mailbox on your Microsoft 365 account. All integration actions are performed within the context of a single given mailbox. MoxiEngage never requires administrative access to your Microsoft 365 account.

Contacts

MoxiEngage continually synchronizes a user's contacts and contact details with the Microsoft 365 Exchange mailbox. Contacts created in Microsoft 365 will appear in MoxiEngage. Contacts created in MoxiEngage are synchronized back to the Microsoft 365 mailbox.

Calendar

MoxiEngage displays the user's calendar events and appointments. Calendar events and appointments can also be added through MoxiEngage and are synchronized to the Microsoft 365 mailbox.

Email

MoxiEngage sends certain email messages through user's mailbox. These email messages will appear in the Sent mail folder and will be delivered to the recipient from the mailbox just as if the user had sent the email from Microsoft 365 directly. MoxiEngage does not synchronize or inspect incoming email messages.

Service Account Setup

MoxiEngage is designed to utilize service account credentials for organizations that use Microsoft 365 (formerly Office 365) for administration of the company's email functions.

An email administrator in your company organization will need to perform steps to create a service account and obtain the necessary credentials for MoxiEngage to use.

Refer to Microsoft 365 Setup Instructions for Administrators in this document and follow the step-by-step instructions to set up a service account with application impersonation using basic authentication and a password that will not expire.

You will need to provide the service account email address and non-expiring password, along with a regular user email address that we can use for testing.

MoxiWorks

Information Gathering

To enable configuration of the MoxiEngage integration, we will need to gather some key information and credentials from you, including the service account credentials created by following the steps in the Microsoft 365 Setup Instructions for Administrators section of this document.

Next Steps

Verification of Credentials

MoxiWorks staff will begin the next step of the integration process. We will test the credentials you provided to verify that the service account is able to connect to your email service and perform a synchronization for the test email address you supplied.

Outcome: Credentials Cannot be Verified

If your entered credentials cannot be verified, we will contact you. Your email administrator will need to resolve the issue and then you will provide us with the updated information.

Outcome: Credentials are Verified Successfully

If your credentials are verified successfully, we will store the credentials securely. Congratulations! This is a key milestone that enables us to continue the process of getting MoxiEngage enabled for your brokerage.

Security

MoxiWorks requires the use of a single username/mailbox on your Microsoft 365 instance, configured as a service account with the Application Impersonation role. All interactions between the MoxiWorks system and your user's mailboxes happens through this designated impersonation account. MoxiEngage never requires administrative access to your Microsoft 365 instance.

Network Access

MoxiWorks systems communicate directly with Microsoft 365 servers over secure HTTPS/SSL connections.

Managing Shared Secrets and Credentials

For automated access, MoxiWorks makes use of methods native to our configuration management software. Credentials are stored in encrypted objects accessible only to servers with the relevant service role and environment. These credentials are pulled and decrypted during software deployment. Server identity is validated via pre-shared public/private key. Credentials are managed through a commercial password manager and any non-automated access is limited to the MoxiWorks Technical Operations team and, with customer approval, limited support personnel on an as-needed basis. See also:

https://docs.chef.io/secrets.html#encrypt-a-data-bag-item

https://www.lastpass.com/en/enterprise

MoxiWorks

Communications Policy for Security Breaches

In the unlikely event of a security breach where client data such as account credentials for registrar management, impersonation credentials, and the like may have been compromised, MoxiWorks Technical Operations and/or Account Management staff will notify affected clients. If the client is aware of a potential security breach, they should notify MoxiWorks immediately so that we may contain and mitigate potential risk in a timely manner. In either case, a change to Impersonation account credentials will be coordinated between both parties.

Microsoft 365 Setup Instructions for Administrators

The following steps describe the recommended process for creating a service account in Microsoft 365 with the Application Impersonation role for use with your brokerage's MoxiWorks integration. Special consideration must be given to ensure the service account user has a password that never expires. The service account user must also be allowed to connect to Microsoft Web Services and Auto Discovery in your Microsoft 365 instance using basic authentication.

Note

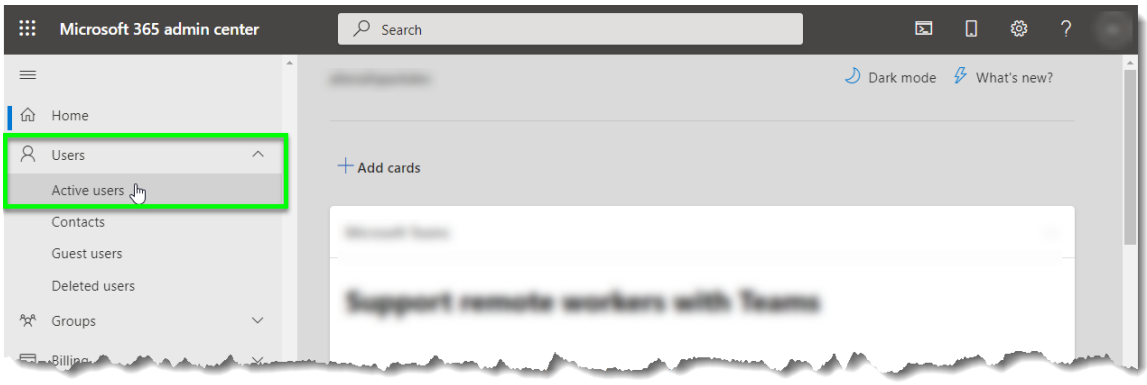
If your Microsoft 365 instance is hosted by a third-party vendor (i.e., GoDaddy, etc.), your Admin user interface may not match the instructions provided here. Please contact your email vendor for assistance. Feel free to provide a copy of this document to your vendor as a guide and explanation of what is required.

Microsoft 365 menu structure and user interface is subject to change. Steps provided in this document were performed from a computer running Windows 10 Pro against a Microsoft 365 instance created in July 2021.

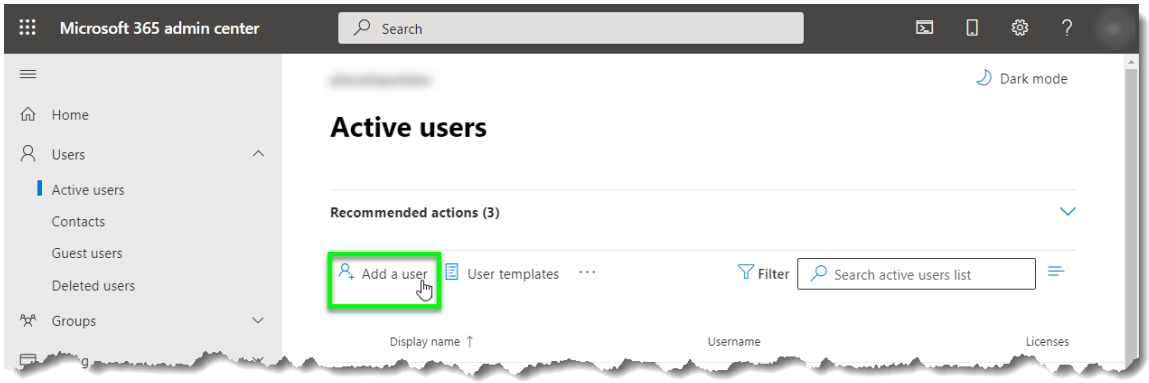
The instructions provided in this guide are not intended to provide security advice for configuring your Microsoft 365 instance. The documented steps represent the most direct approach available at the time of this writing to achieve the necessary access required by MoxiWorks products. Other methods of configuration may be available.

Create a Service Account User

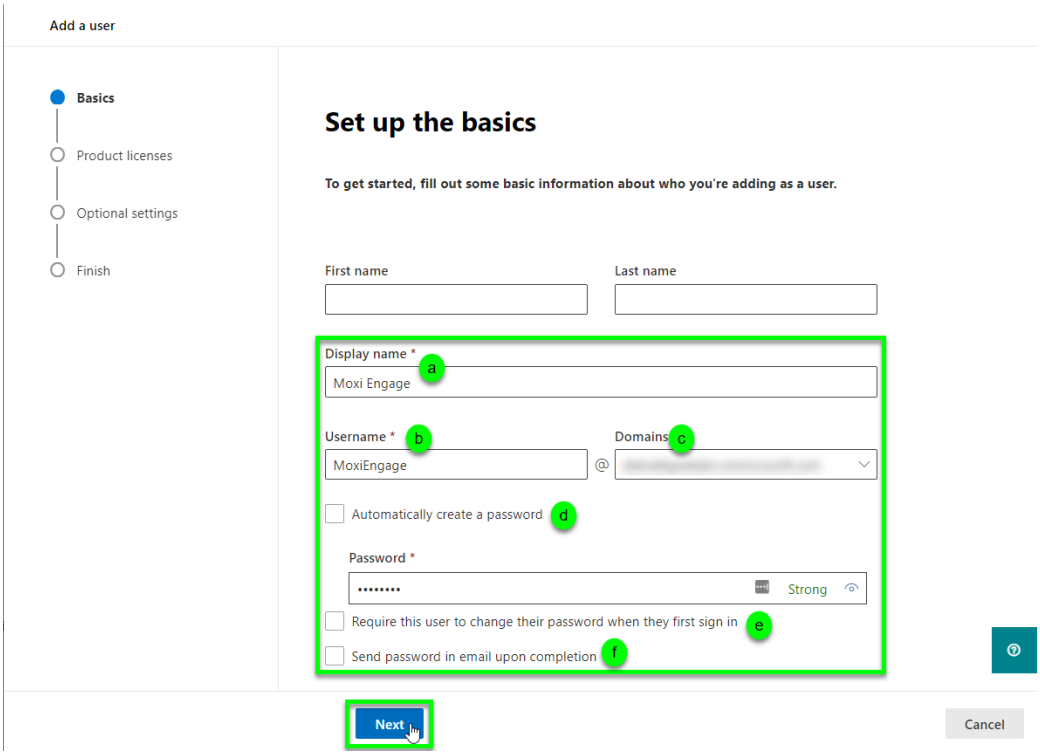
1. Login to your Microsoft 365 Admin Center.
2. Click to expand the "Users" section of the menu, then click on the "Active users" option.



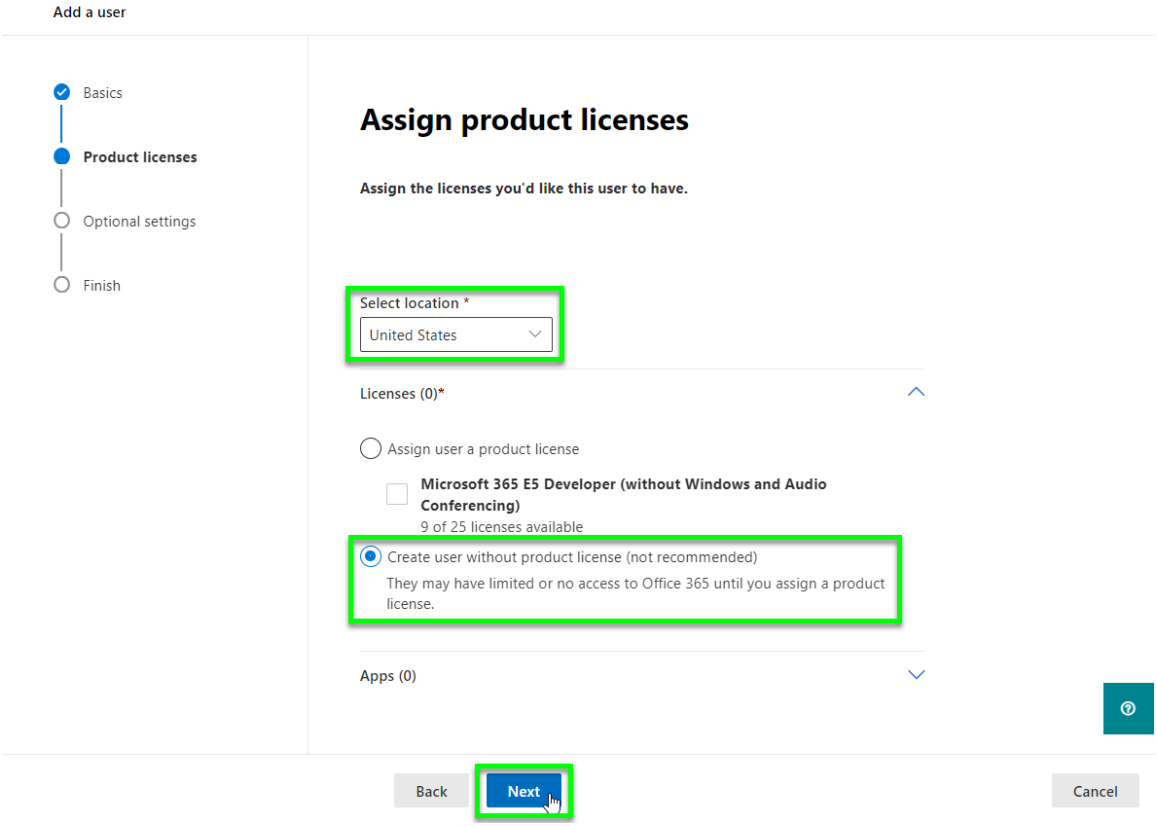
3. Click on the “Add a user” action link.



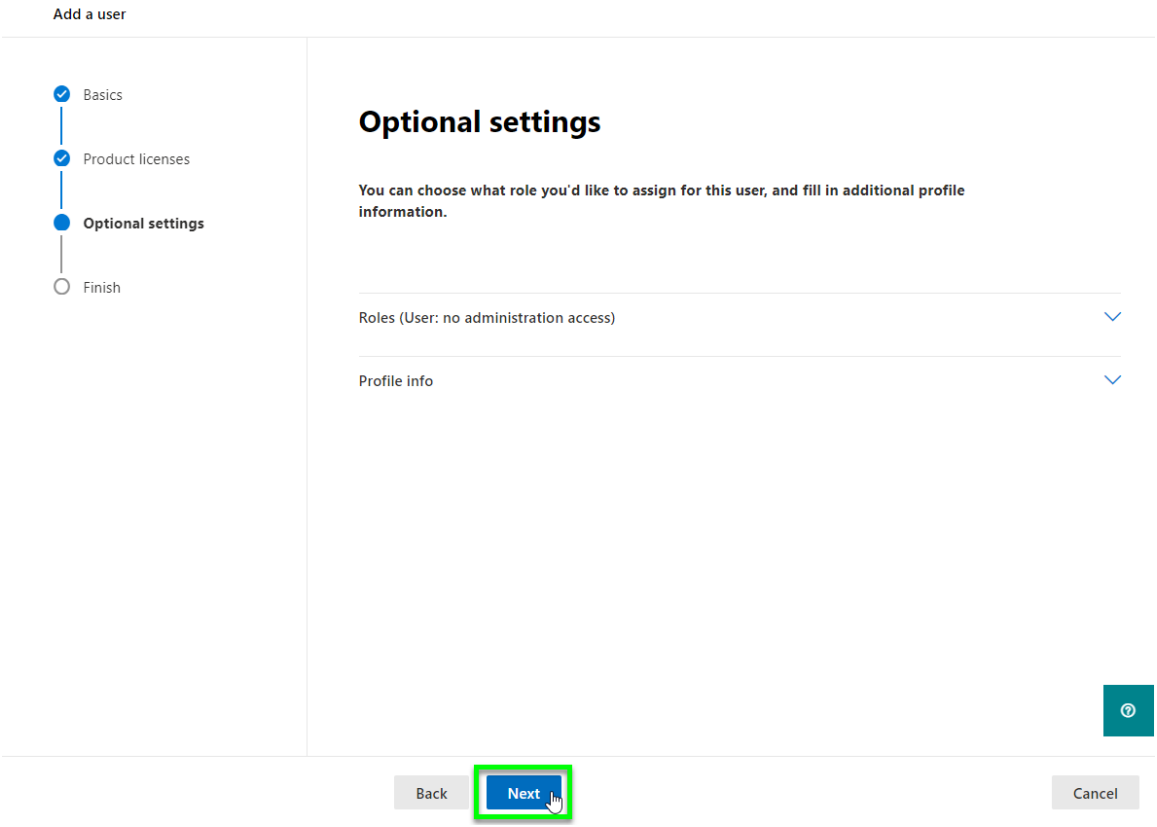
4. Enter the following basic information, then click on the “Next” button:
    a. Display Name (e.g., Moxi Engage)
    b. Username (e.g., MoxiEngage)
    c. Domains (select the domain or use the default)
    d. Ensure the “Automatically create a password” checkbox is cleared (not marked), then enter a Password. (Be sure to make note of the password so you can provide it to us.)
    e. Ensure the “Require this user to change their password when they first sign in” checkbox is cleared (not marked).
    f. Ensure the “Send password in email upon completion” checkbox is cleared (not marked).



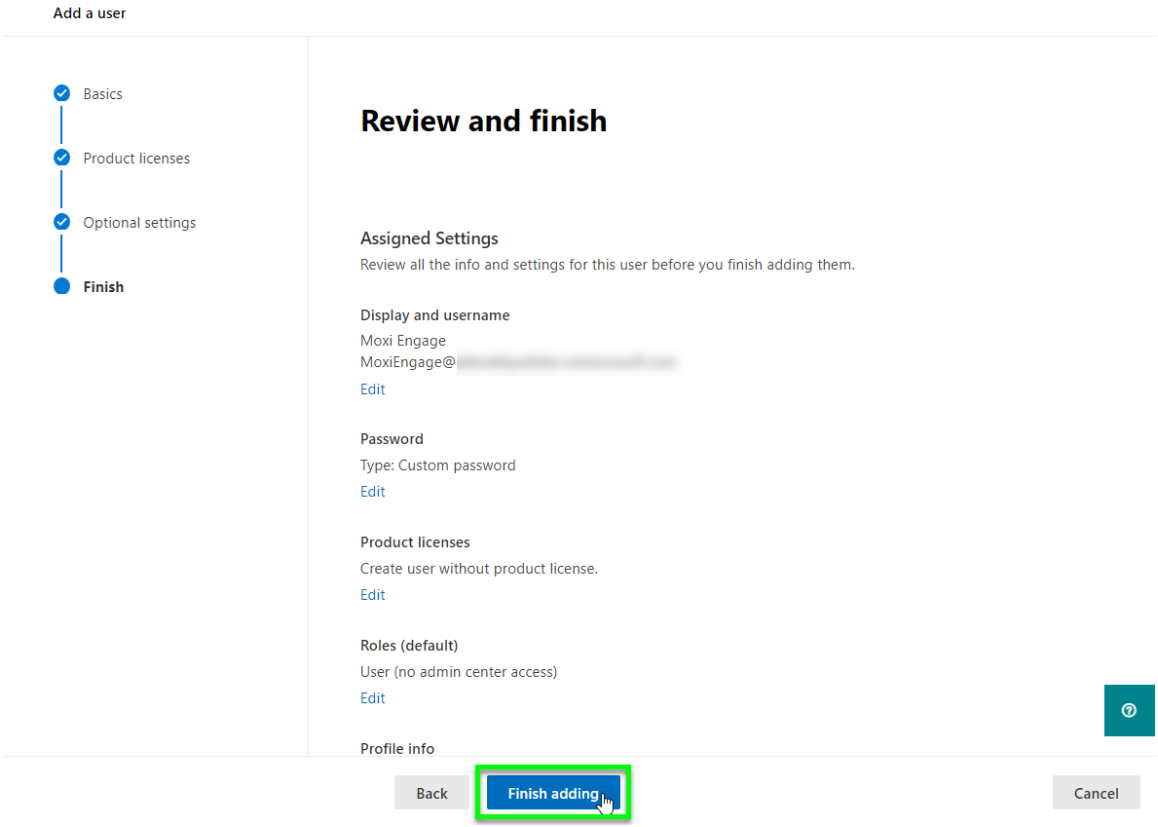
5. Ensure the correct location is selected, then mark the radio button next to the “Create user without product license” option. A service account user does not require a product license. Click on the “Next” button.



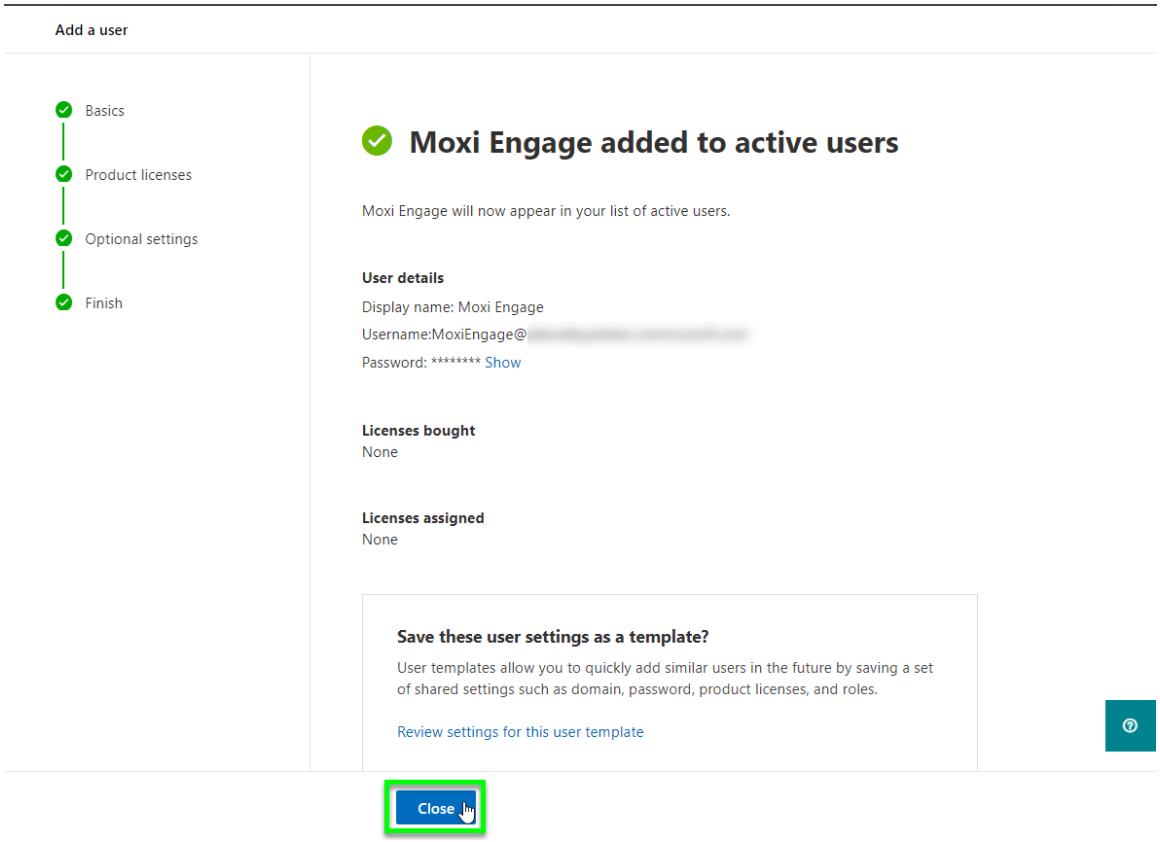
6. No optional settings are required at this time. Click on the “Next” button.



7. Review your changes, then click on the “Finish adding” button.



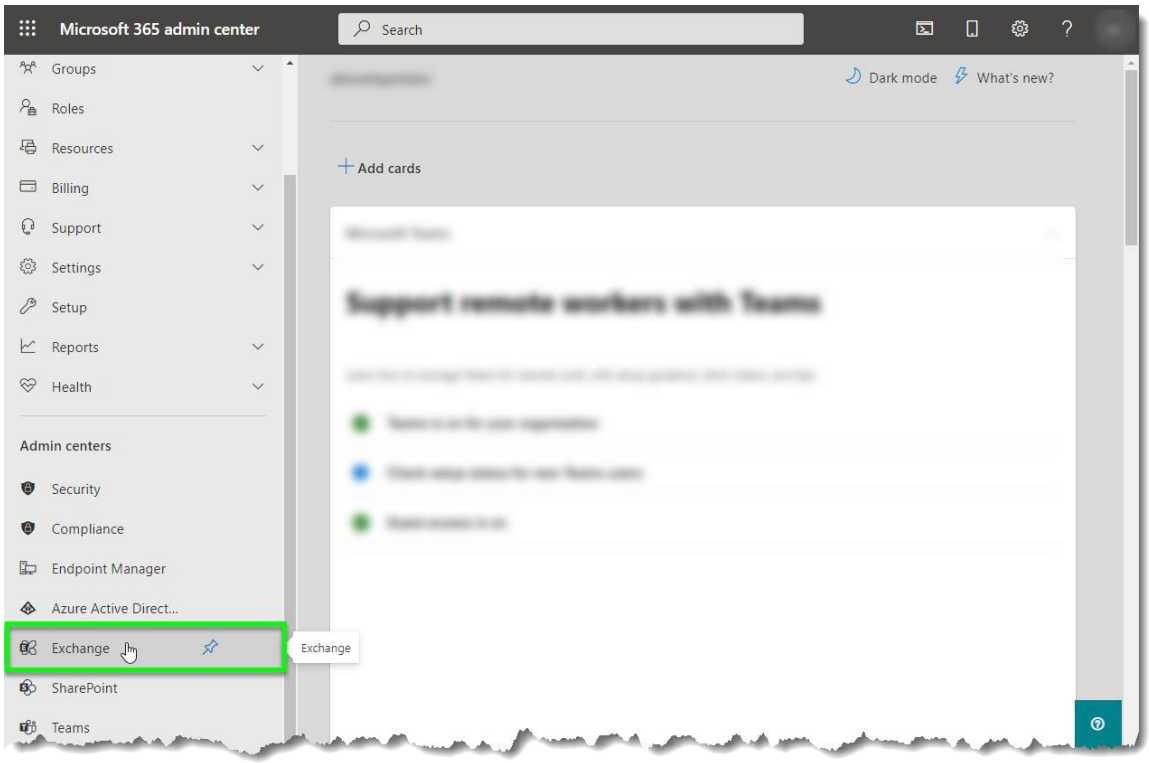
8. View the confirmation that the new user has been added. Click on the “Close” button.



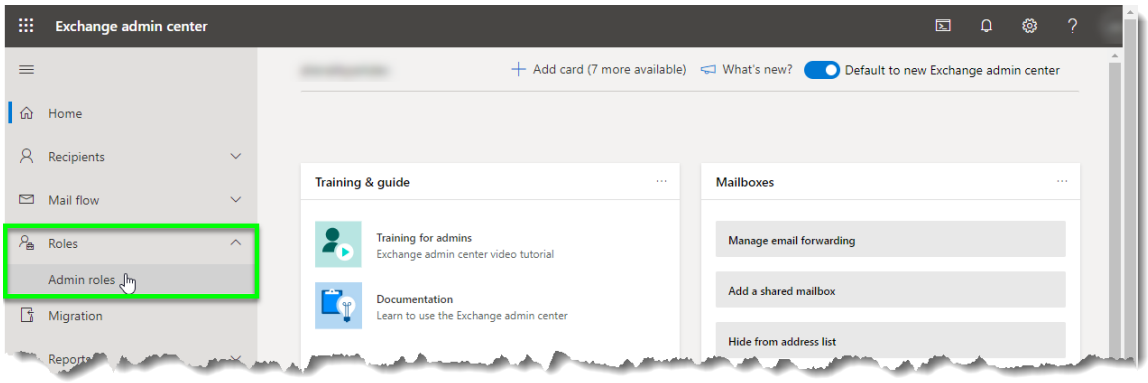
MoxiWorks

Grant Application Impersonation to the Service Account User

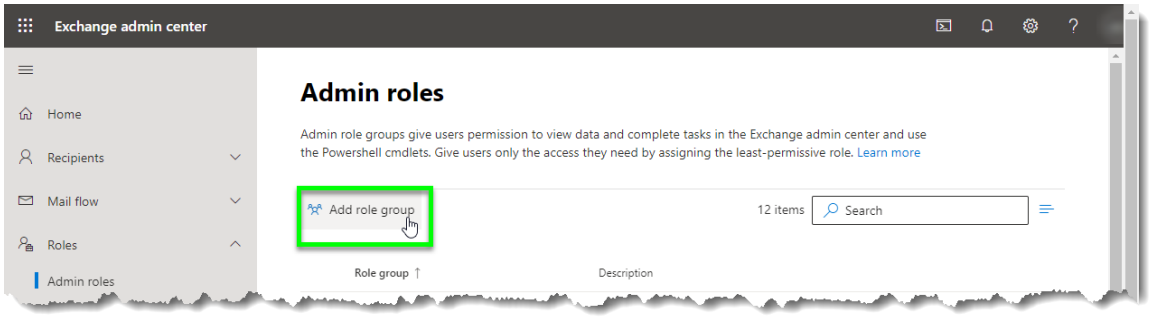
1. Login to your Microsoft 365 Admin Center.
2. Click on the “Exchange” menu option under the “Admin centers” area of the menu. (If this option is not visible, you can click on “Show all” to expand the menu.)



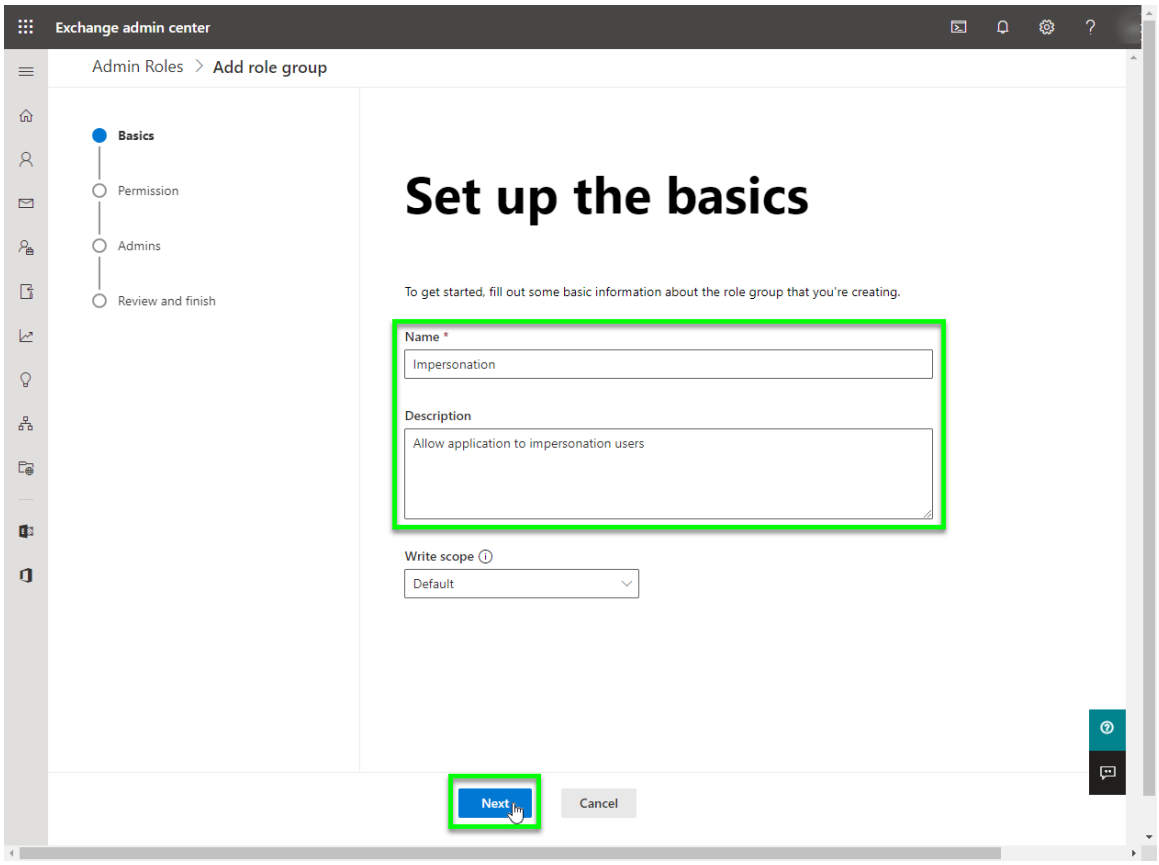
3. In the Exchange Admin Center, expand the “Roles” area of the menu and click on the “Admin roles” option.



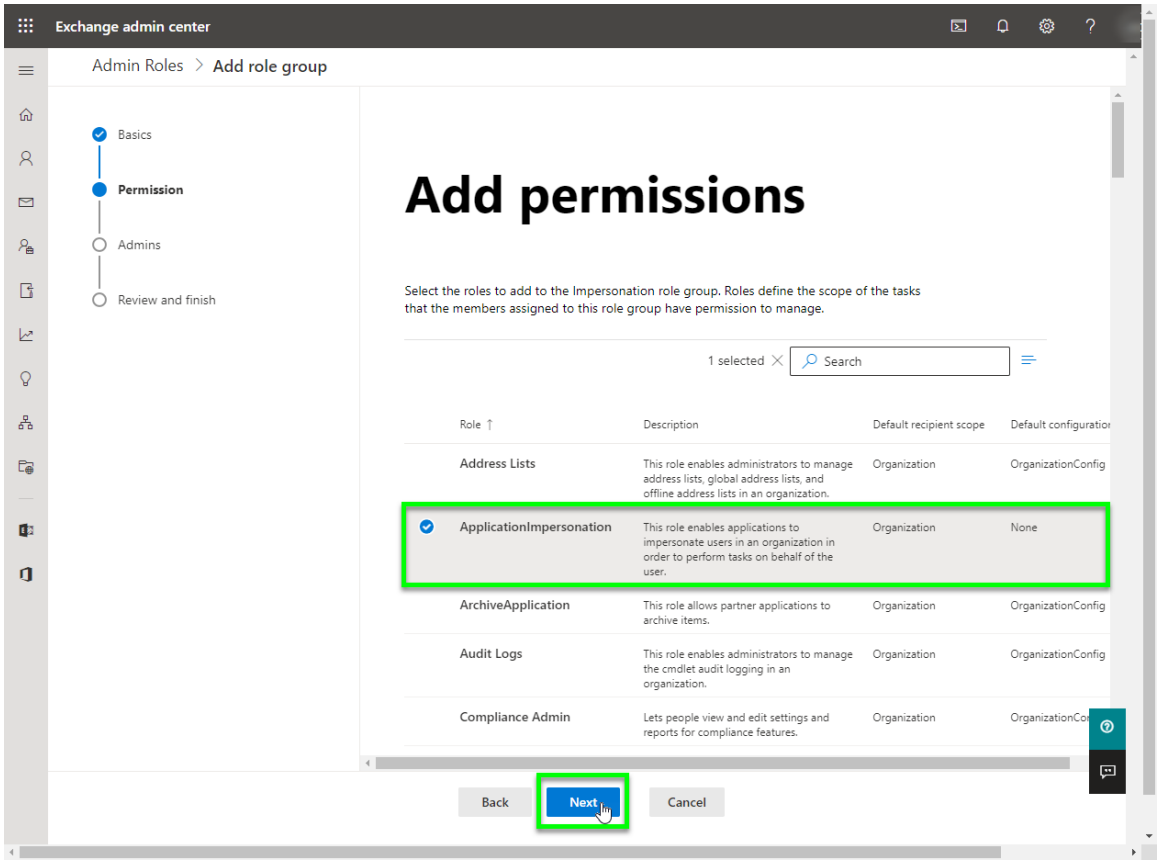
4. Click on the “Add role group” option button.



5. Enter a Name and Description for the new role group, then click on the “Next” button.

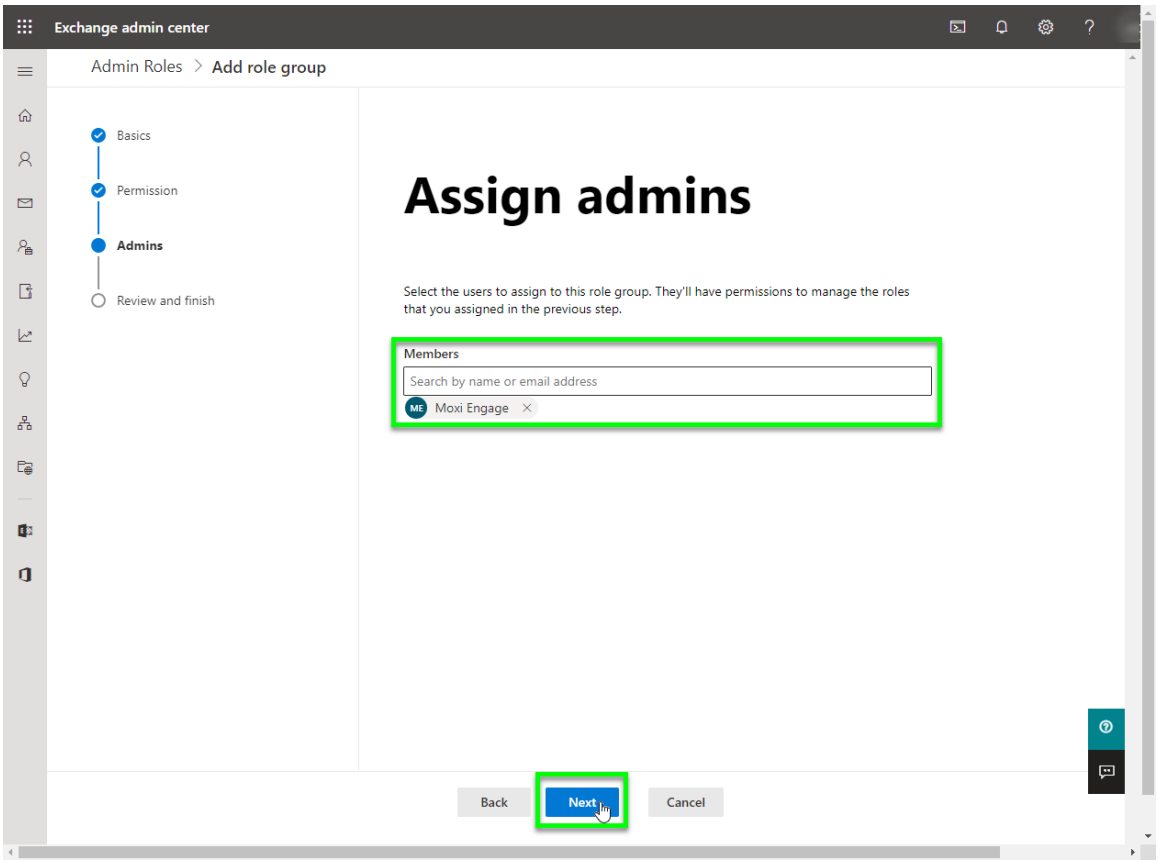


6. Select the “ApplicationImpersonation” role, then click on the “Next” button.

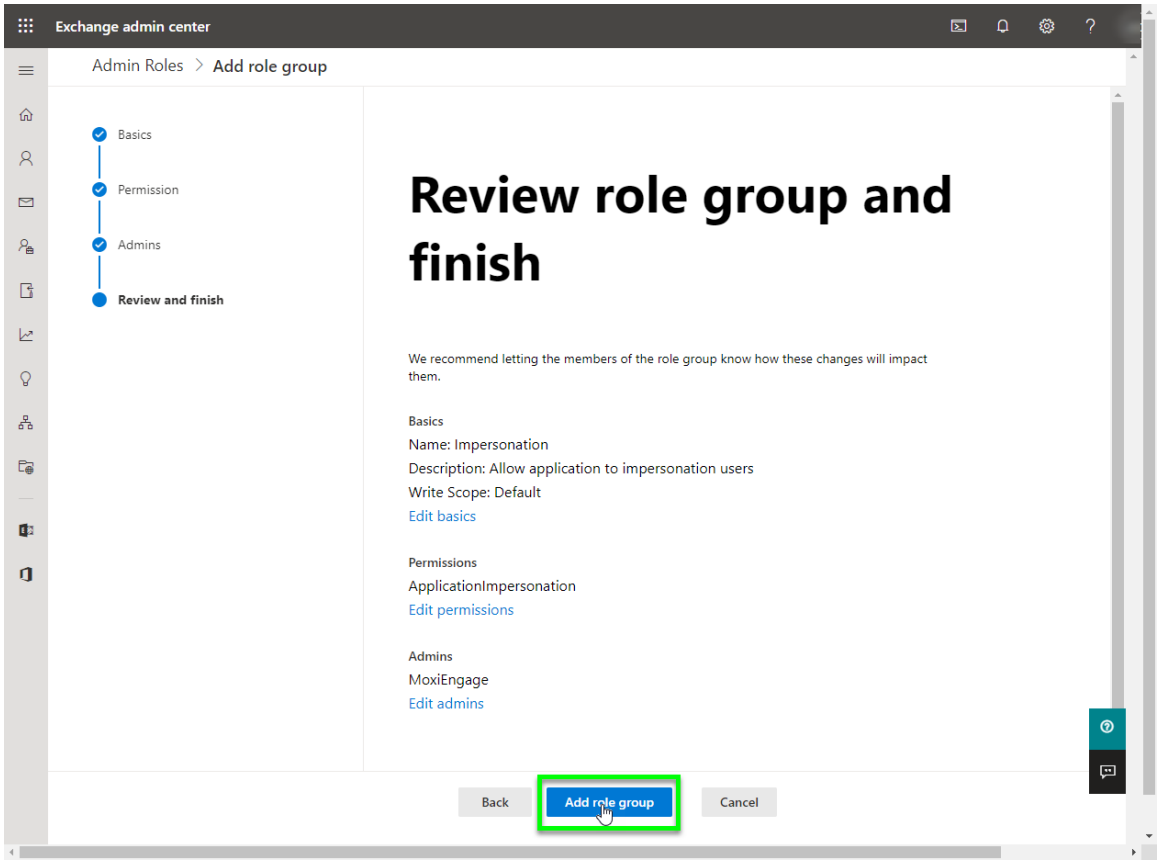


MoxiWorks

7. Search for and add the MoxiEngage service account, then click on the “Next” button.

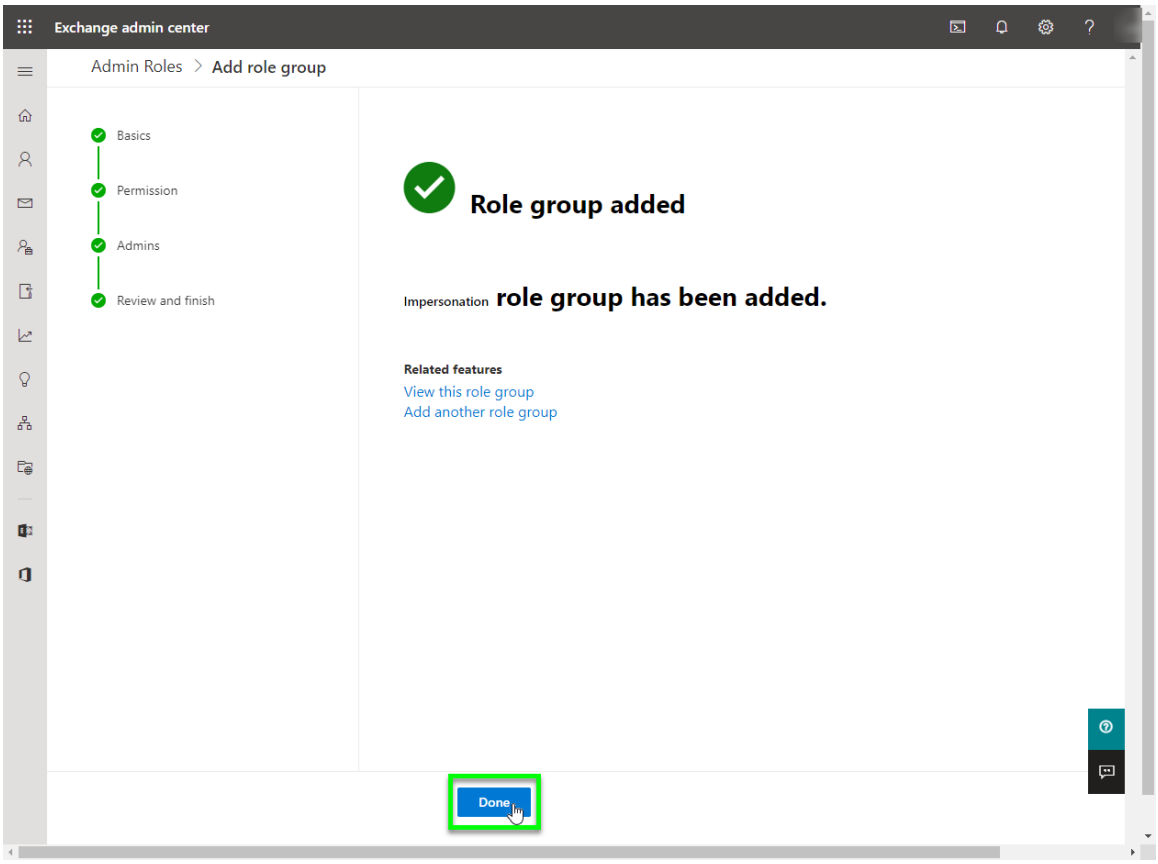


8. Review your changes, then click on the “Add role group” button.



MoxiWorks

9. View the confirmation that the role group has been added, then click on the “Done” button.



MoxiWorks

Ensure Service Account User has a Password that Never Expires

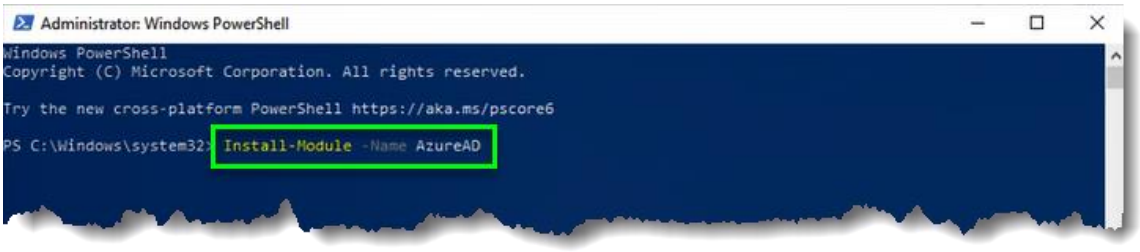
Connectivity to your Microsoft 365 instance depends on having the correct credentials stored and available for use when synchronizing your agents' contact data. When the service account password expires, synchronization will be interrupted until the password has been reset, provided to MoxiWorks, and stored securely for MoxiEngage to authenticate against your account.

Unlike the classic Active Directory interface, Azure Active Directory does not provide a simple method to set a password to never expire for a single user. Instead, setting a user's password to never expire must be done using the AzureAD module in PowerShell.

1. Run Windows PowerShell as an administrator. (From your Windows Start menu, right click over the Windows PowerShell shortcut, select More => Run as administrator.)
2. At the PowerShell prompt, type

   ```
   Install-Module -Name AzureAD
   ```

   and press Enter on your keyboard to begin installation of the Azure AD module.



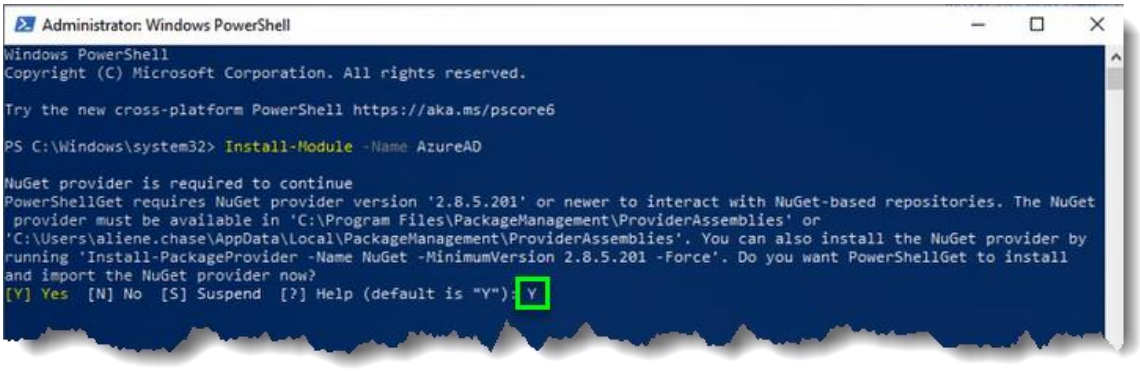
Note

If the AzureAD module is already installed, the message prompts shown in steps 3-5 will not be displayed.

3. Type

   ```
   Y
   ```

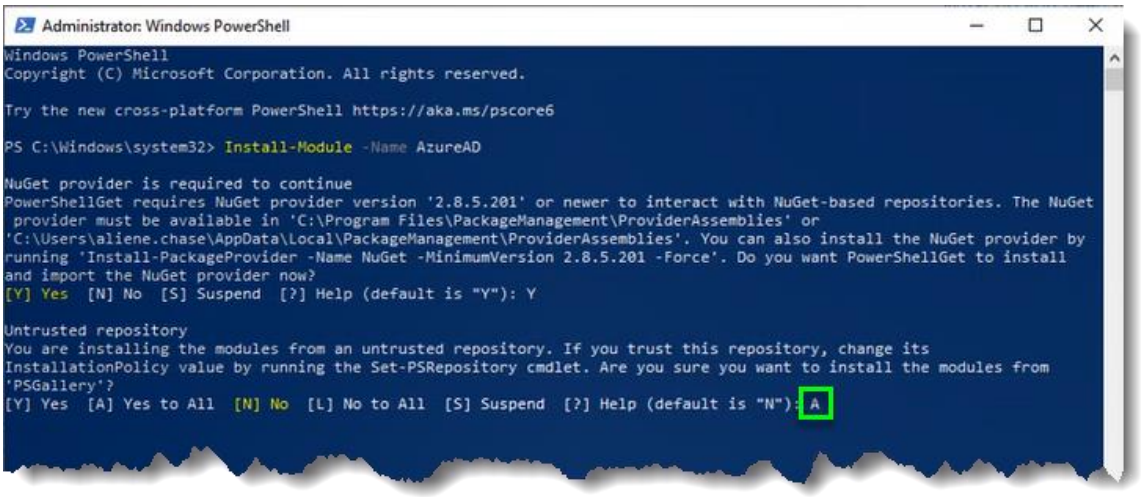
   and press Enter on your keyboard to accept installation of the NuGet provider.



4. Wait for the next prompt.
5. The AzureAD module is part of the PowerShell Gallery (PSGallery), which is not by default configured as a trusted repository for PowerShell. If a message is displayed about an untrusted repository, review the warning. If you wish to continue the installation, type

   `A`

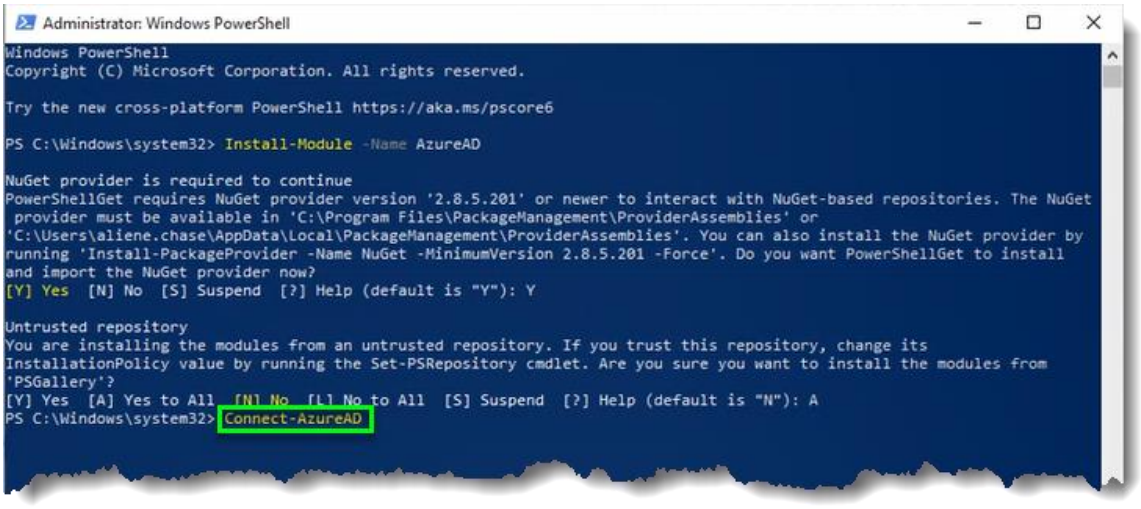
   and press Enter on your keyboard.



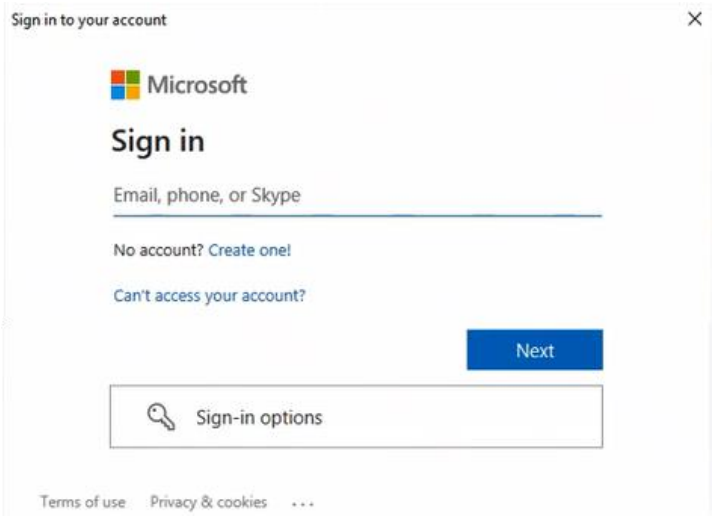
6. Wait for the next prompt. It may take a few minutes to complete the installation.
7. At the prompt, type

   `Connect-AzureAD`

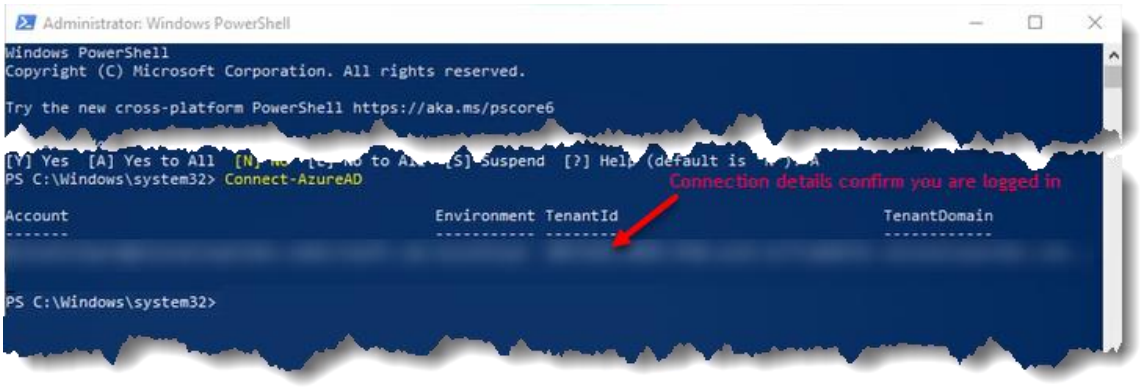
   and press Enter on your keyboard.



8. Follow the on-screen instructions to log into your Microsoft 365 account using a login with administrative rights. The login screen that may appear as a pop-up over your PowerShell window supports multi-factor authentication (MFA).



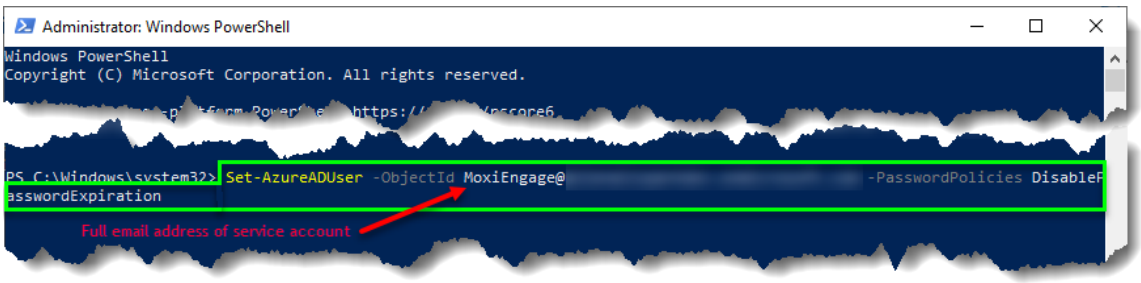
9. When you have logged in successfully, connection information including your login account, environment, and domain will be displayed.



10. At the prompt, type

`Set-AzureADUser -ObjectId` {email address} `-PasswordPolicies DisablePasswordExpiration`

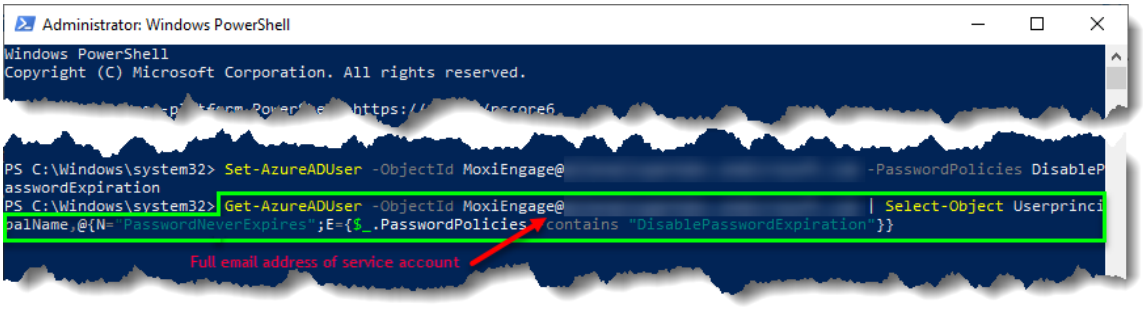
replacing "{email address}" with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard.



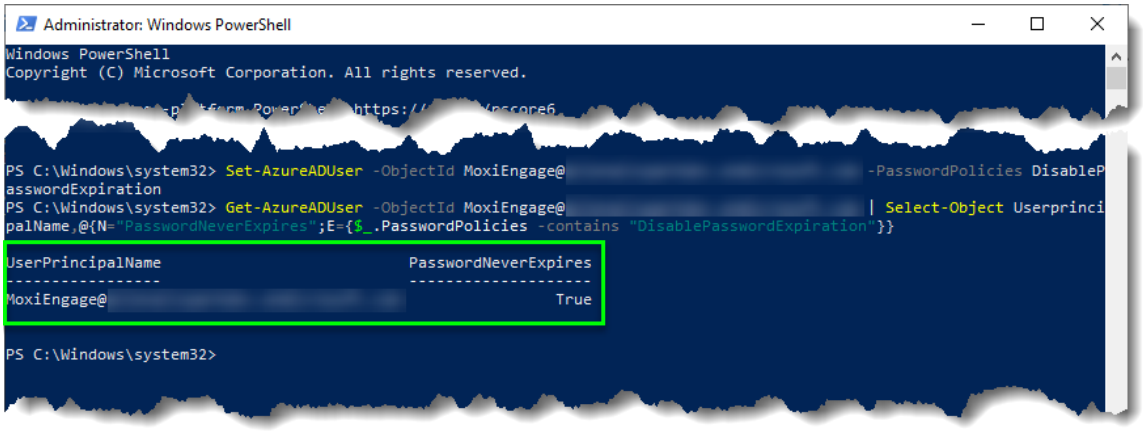
11. To verify the service account's password is set to never expire, type

```
Get-AzureADUser -ObjectId {email address} | Select-Object
UserprincipalName,@{N="PasswordNeverExpires";E={$_.Password
Policies -contains "DisablePasswordExpiration"}}
```

replacing "{email address}" with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard.



12. Observe the displayed confirmation that the password never expires.

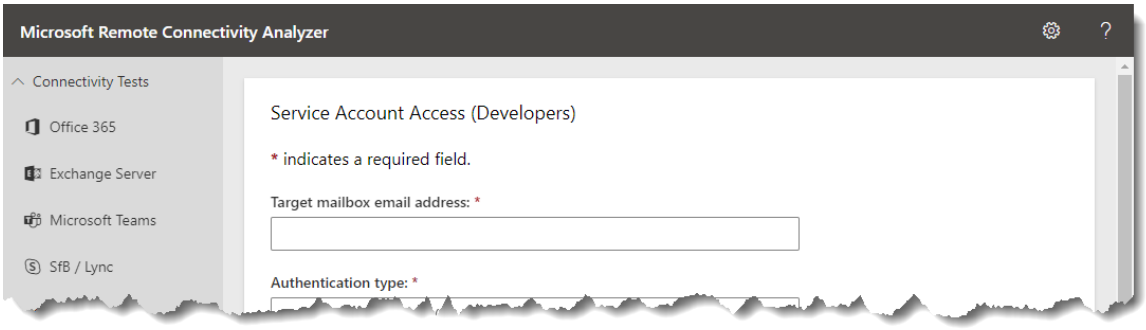


MoxiWorks

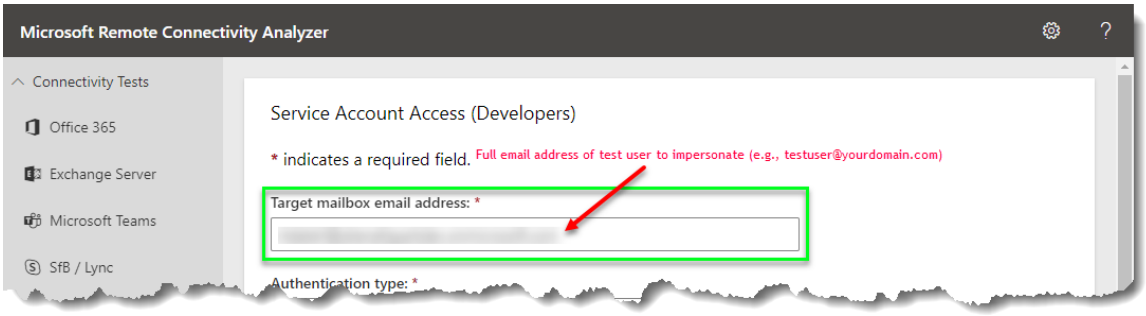
Test Service Account Impersonation for MoxiEngage

It is best practice to test the impersonation role of your MoxiEngage service account before you provide the service account credentials to MoxiWorks. This will prevent delays in your onboarding process. If the impersonation testing fails, additional configuration steps may be required.

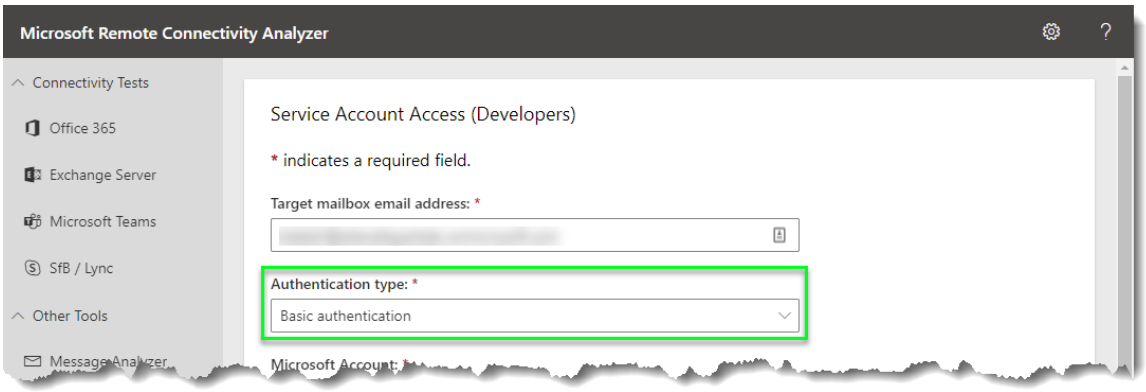
1. Identify a regular (non-administrator) email address in your Microsoft 365 instance. The test will attempt to use the service account to impersonate this user. Be sure that the selected user has logged into Microsoft 365 and accessed Outlook at least one time.
2. In your web browser, navigate to the Microsoft Remote Connectivity Analyzer.



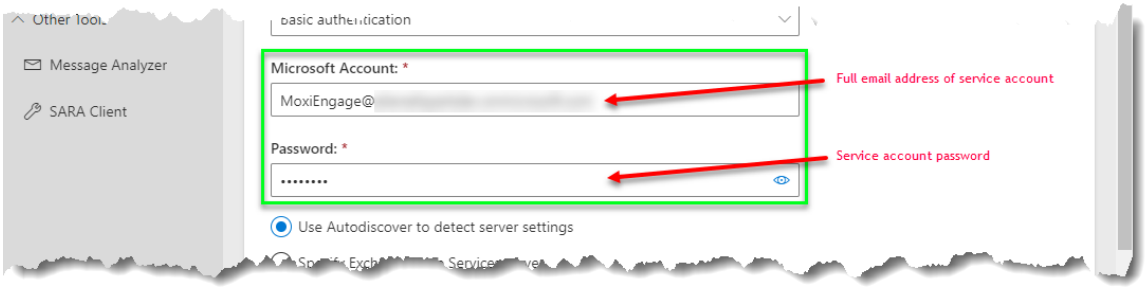
3. Enter the test email address in the “Target mailbox email address” box of the form.



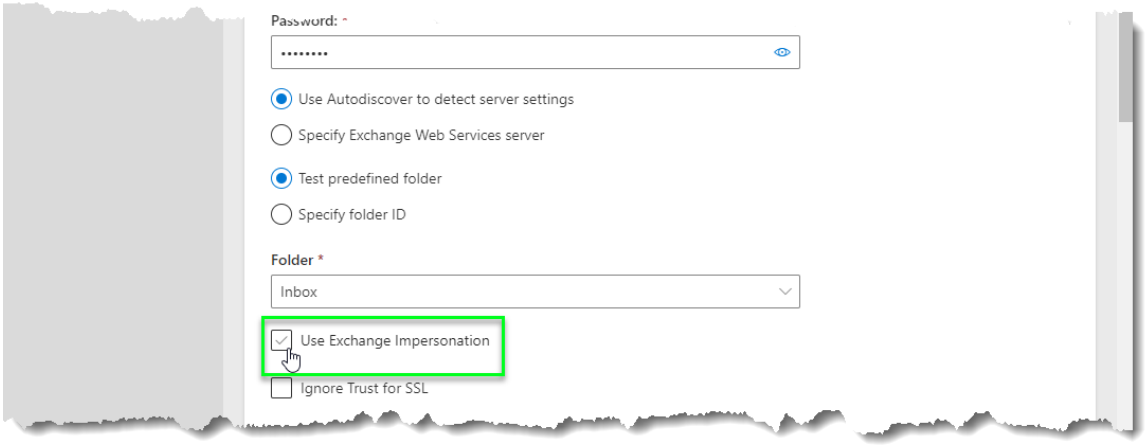
4. Select “Basic authentication” from the “Authentication type” dropdown list.



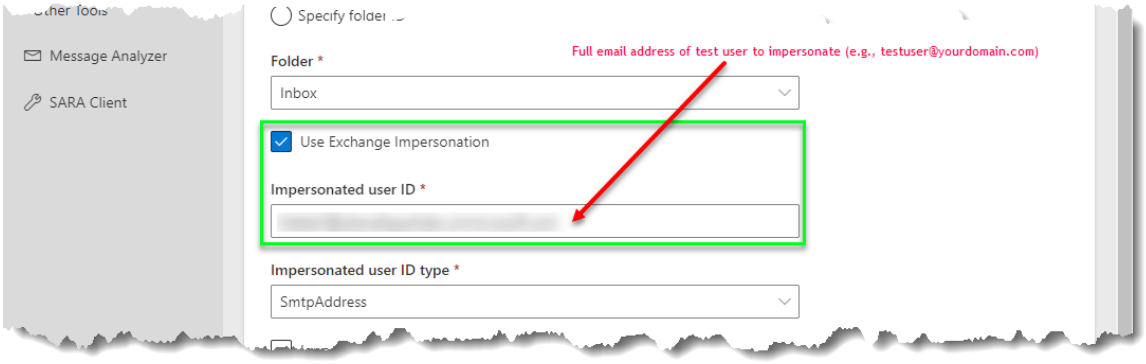
5. Enter the email address of the service account you created for MoxiEngage in the “Microsoft Account” box of the form, then enter the associated password in the “Password” box.



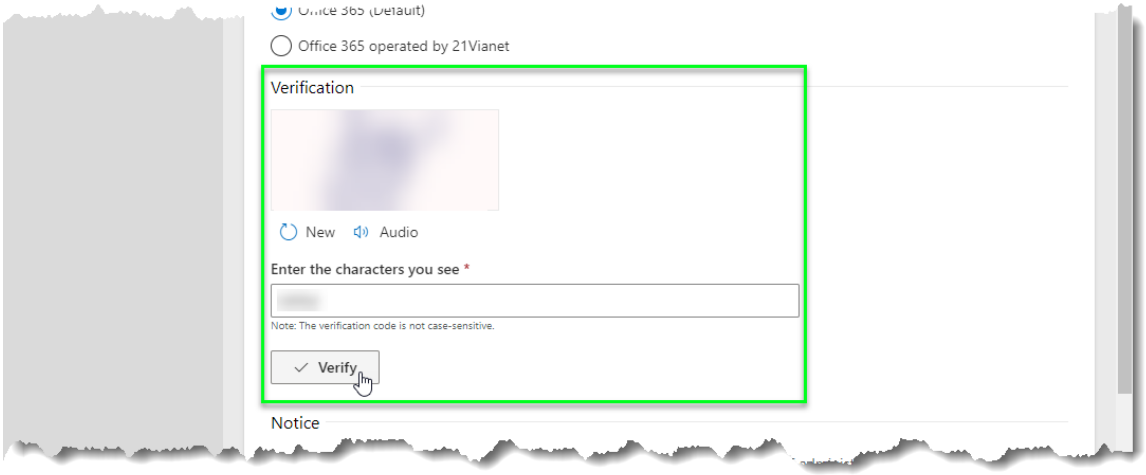
6. Mark the checkbox next to the “Use Exchange Impersonation” label.



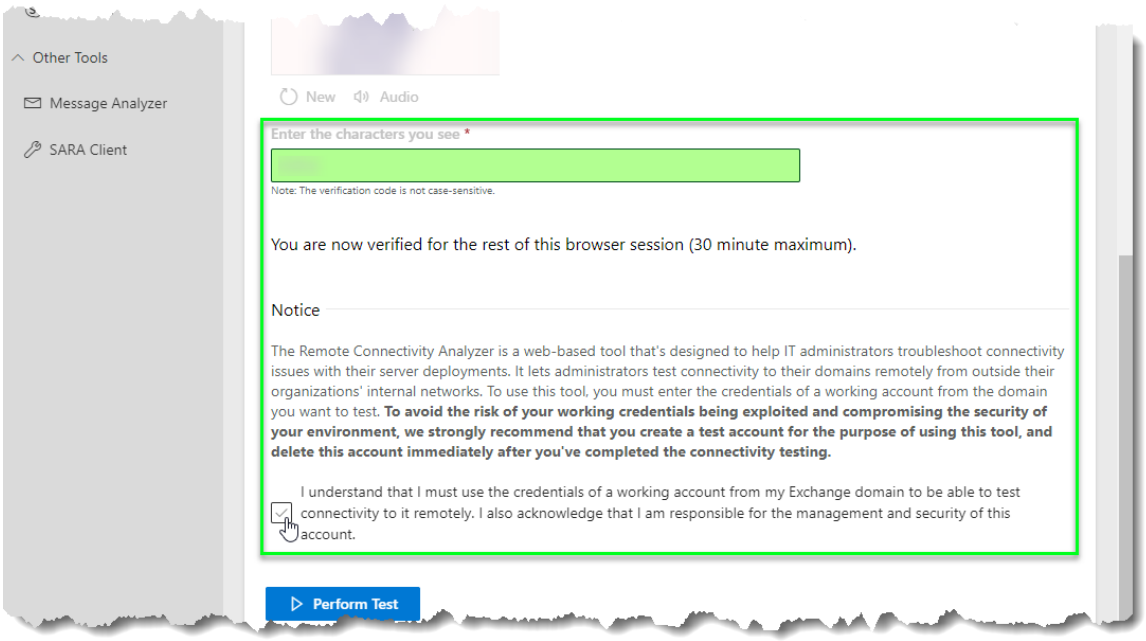
7. Enter the test email address in the “Target mailbox email address” box of the form. (This should be the same email address entered in the “Target mailbox email address” box.)



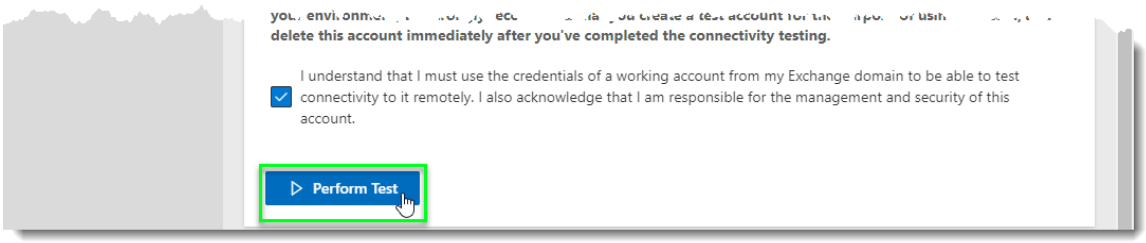
8. Enter the displayed Verification code in the “Enter the characters you see” box of the form, then click on the “Verify” button.



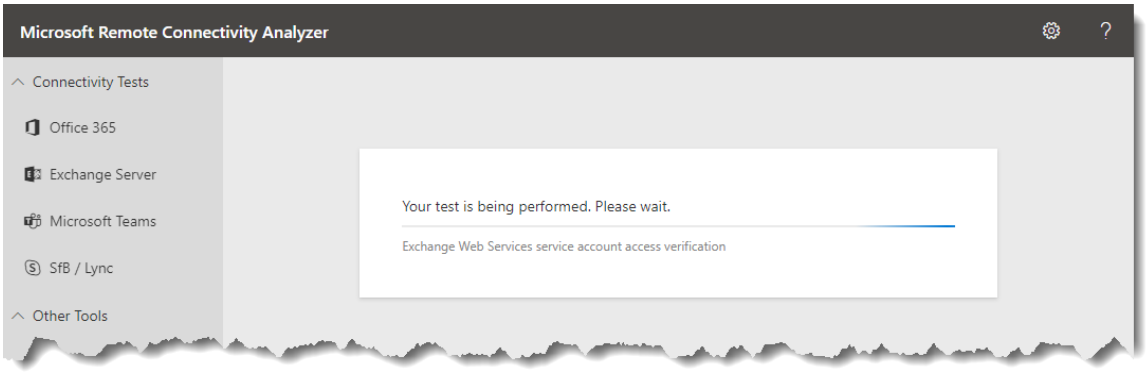
9. Observe that your verification code was accepted for the browser session, then mark the checkbox next to the acknowledgement statement.



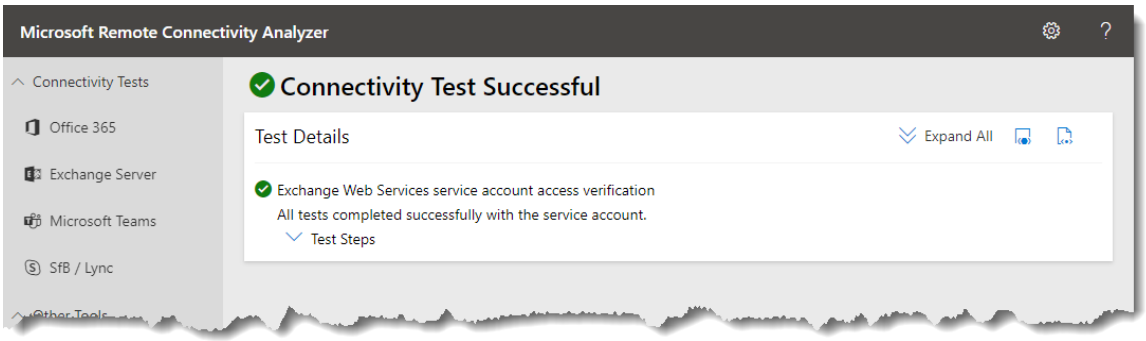
10. Click on the “Perform Test” button.



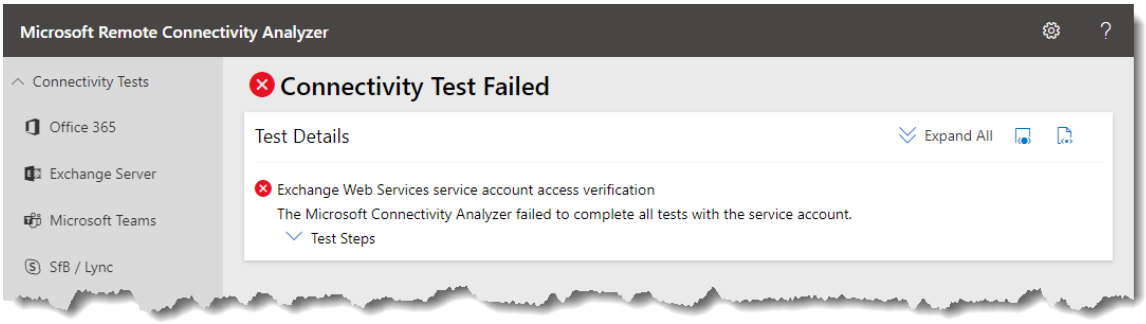
11. Wait while the test is performed.



12. Observe the results of the test.
    a. If the test was successful, no further configuration of the service account is required. Provide the service account email address and password in the secure online form.



    b. If the test failed, review the error messages. Refer to Troubleshoot Service Account Impersonation for MoxiEngage in this document for guidance in resolving the most commonly encountered issues.

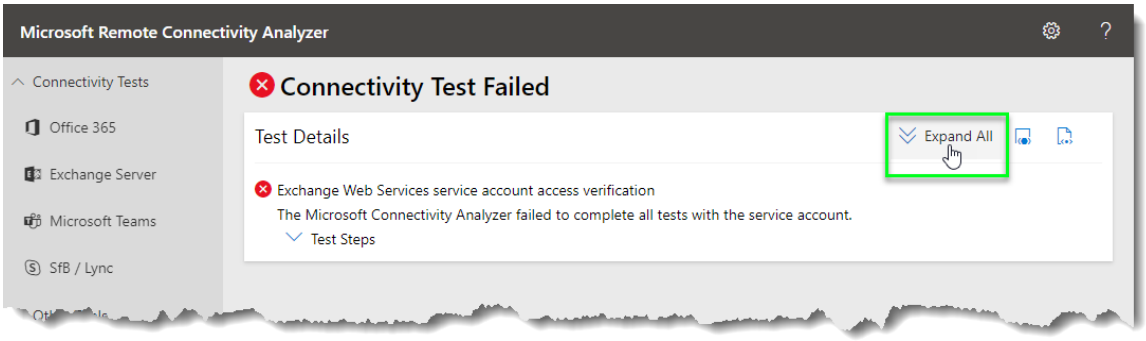


MoxiWorks

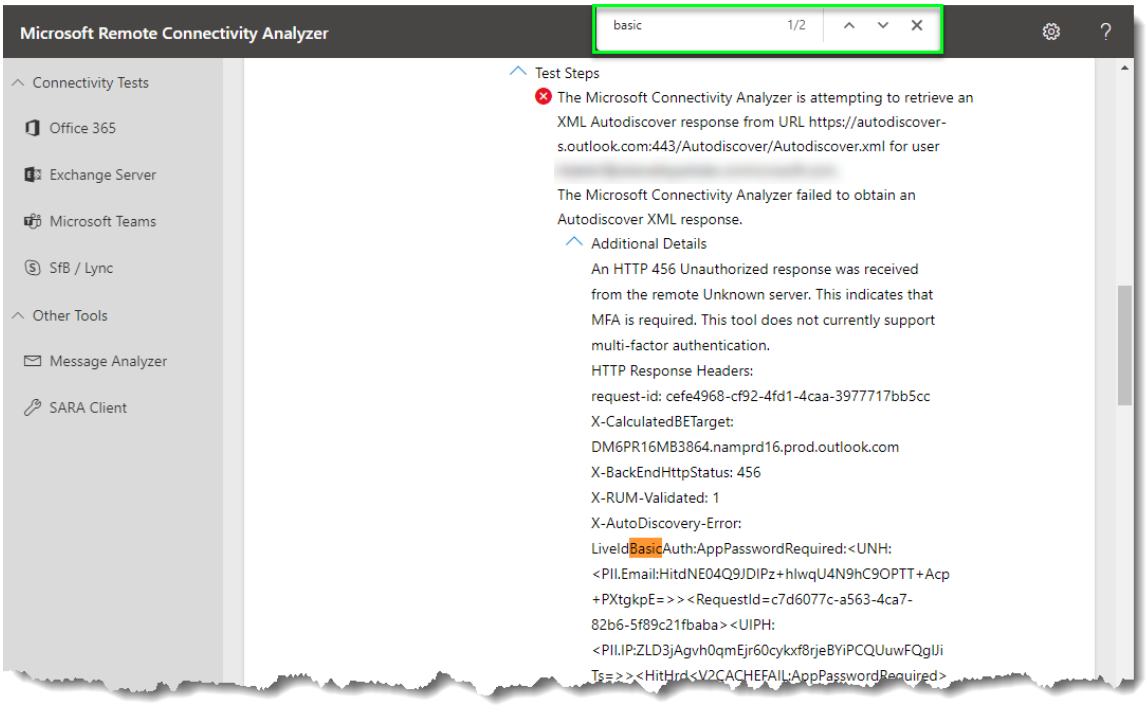
Troubleshoot Service Account Impersonation for MoxiEngage

The Microsoft Remote Connectivity Analyzer provides detailed error logging. Use this section to review the results of a failed connectivity test. This troubleshooting guide is intended to address typical authentication issues that may occur. If the error you are encountering is not addressed in this document, please refer to Microsoft Help for the Remote Connectivity Analyzer Tool.

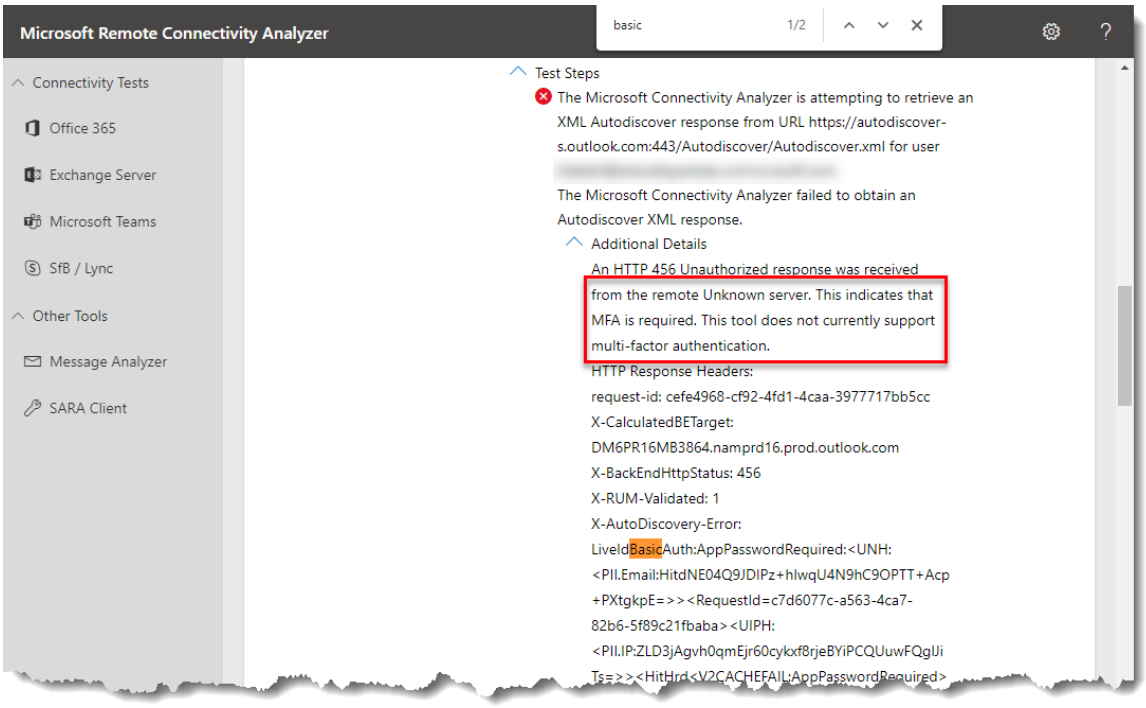
1. Click on the icon next to the “Expand All” label to expand the log messages.

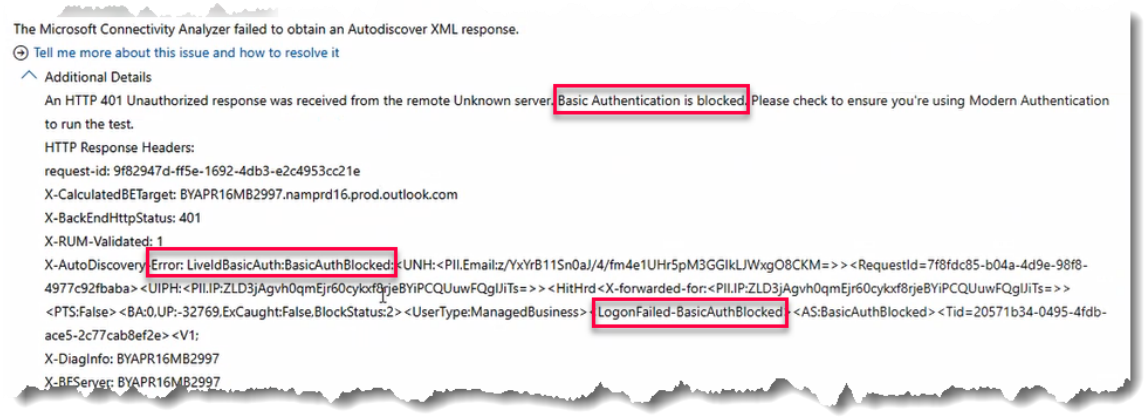


2. Once the entire log is expanded, the text becomes searchable. Search the webpage for “basic” by using the search tool in your browser or typing Ctrl-F on your Windows keyboard.

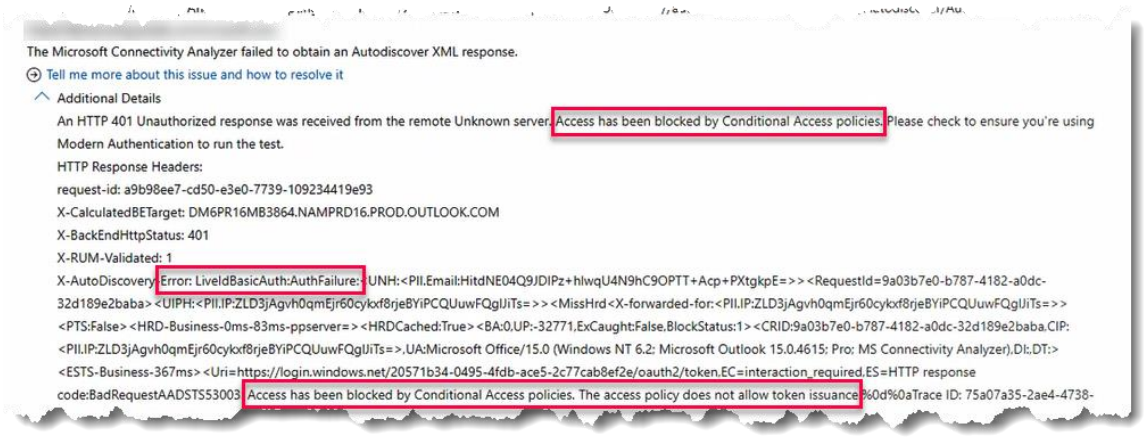


3. Review the log text in the vicinity of the first occurrence of the “basic” word. If you see text that says “MFA is required” or “basic authentication is blocked” or is not accepted, this likely indicates that you need to follow the steps to allow basic authentication for the service account.





4. Review the log text in the vicinity of the first occurrence of the “basic” word. If you see text that says “Access has been blocked by Conditional Access policies” or “access policy does not allow token issuance” or similar, this likely indicates that you need to follow the steps to adjust your conditional access policy for the service account.



Allow Basic Authentication for Service Account

MoxiWorks does not currently support modern authentication for Microsoft 365. The service account that MoxiEngage requires to synchronize agent data will connect to Microsoft Web Services and Auto Discovery using basic authentication. Default security settings in newer instances of Microsoft 365 automatically disable basic authentication. Basic authentication must be enabled for the MoxiEngage service account.

1. Run Windows PowerShell as an administrator. (From your Windows Start menu, right click over the Windows PowerShell shortcut, select More => Run as administrator.)

Note

To clear the PowerShell window, type `cls` at the PowerShell prompt and press Enter on your keyboard.

2. At the PowerShell prompt, type

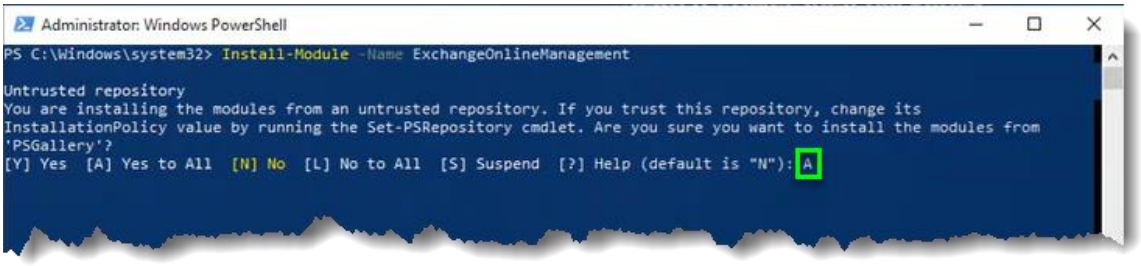
```
Install-Module -Name ExchangeOnlineManagement
```

and press Enter on your keyboard.

3. The ExchangeOnlineManagement module is part of the PowerShell Gallery (PSGallery), which is not by default configured as a trusted repository for PowerShell. If a message is displayed about an untrusted repository, review the warning. If you wish to continue the installation, type

   `A`

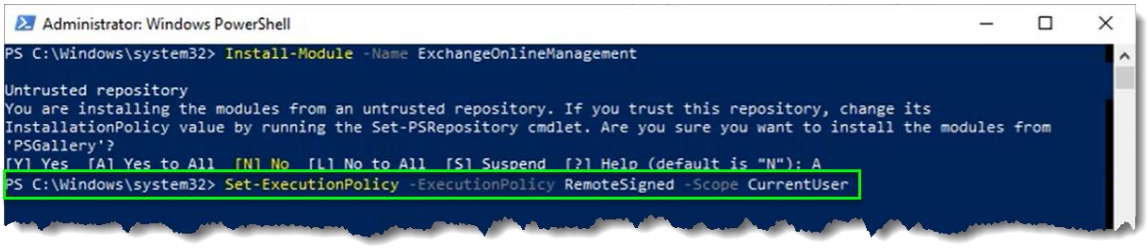
   and press Enter on your keyboard.



4. Wait for the prompt. It may take a moment to complete the installation.
5. Type

   `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser`

   and press Enter on your keyboard.



6. Confirm the change to your PowerShell execution policy. Type

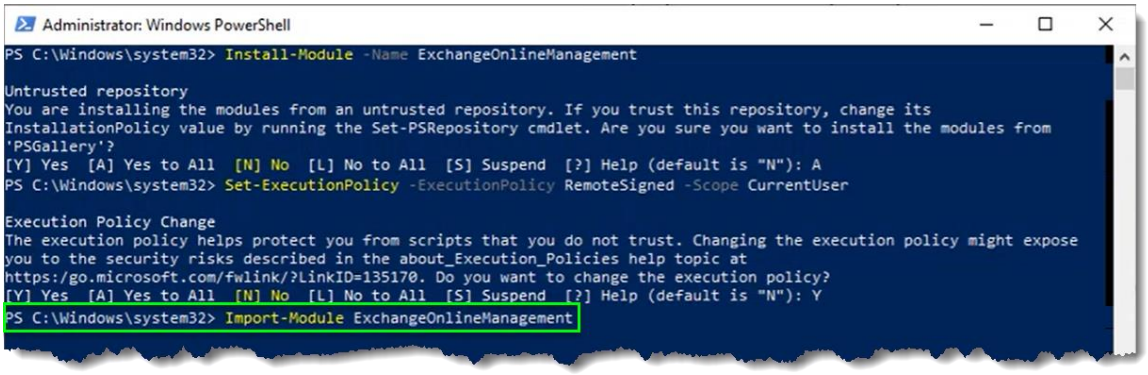
   `Y`

   and press Enter on your keyboard.

7. Type

   `Import-Module ExchangeOnlineManagement`

   and press Enter on your keyboard.

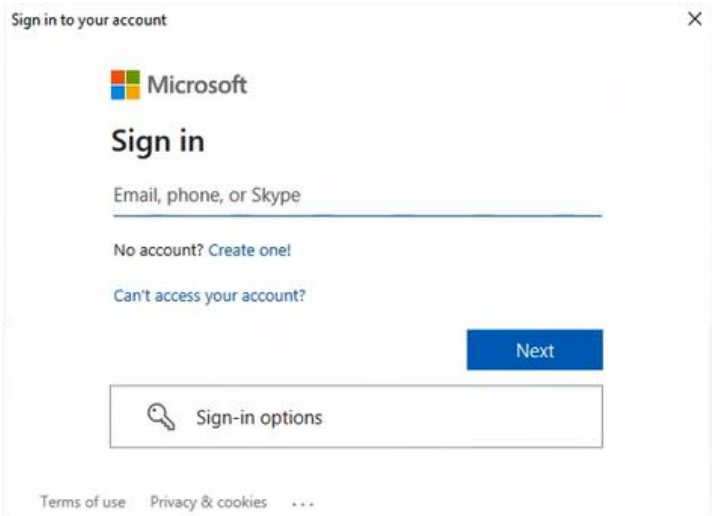


8. Type

   `Connect-ExchangeOnline`

   and press Enter on your keyboard.

9. Follow the on-screen instructions to log into your Microsoft 365 account using a login with administrative rights. The login screen that may appear as a pop-up over your PowerShell window supports multi-factor authentication (MFA).

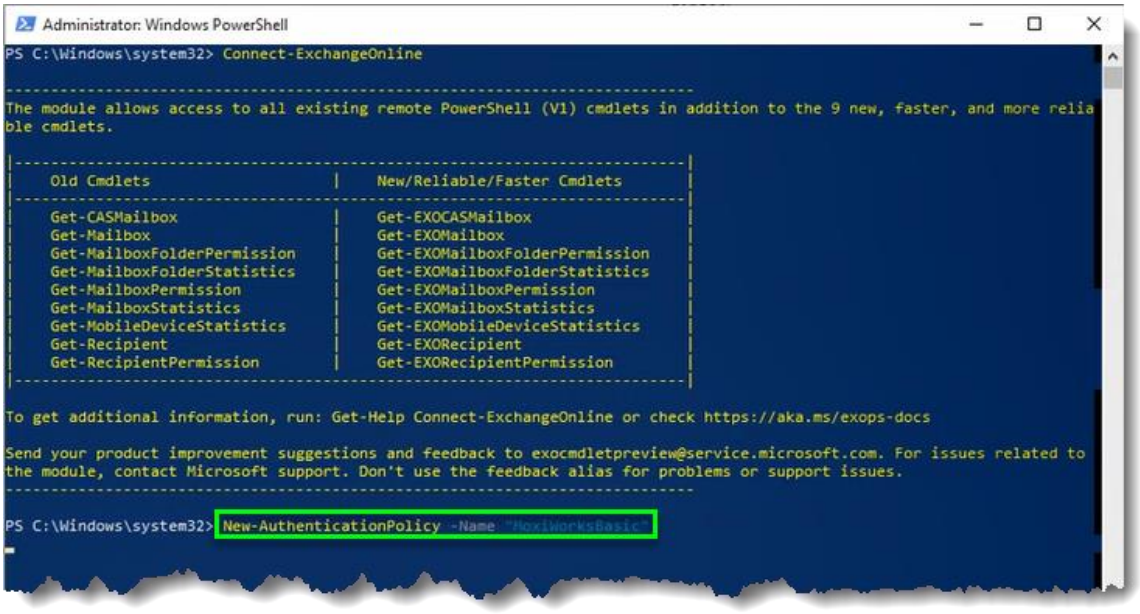


10. Wait for the prompt to appear after the login process completes.

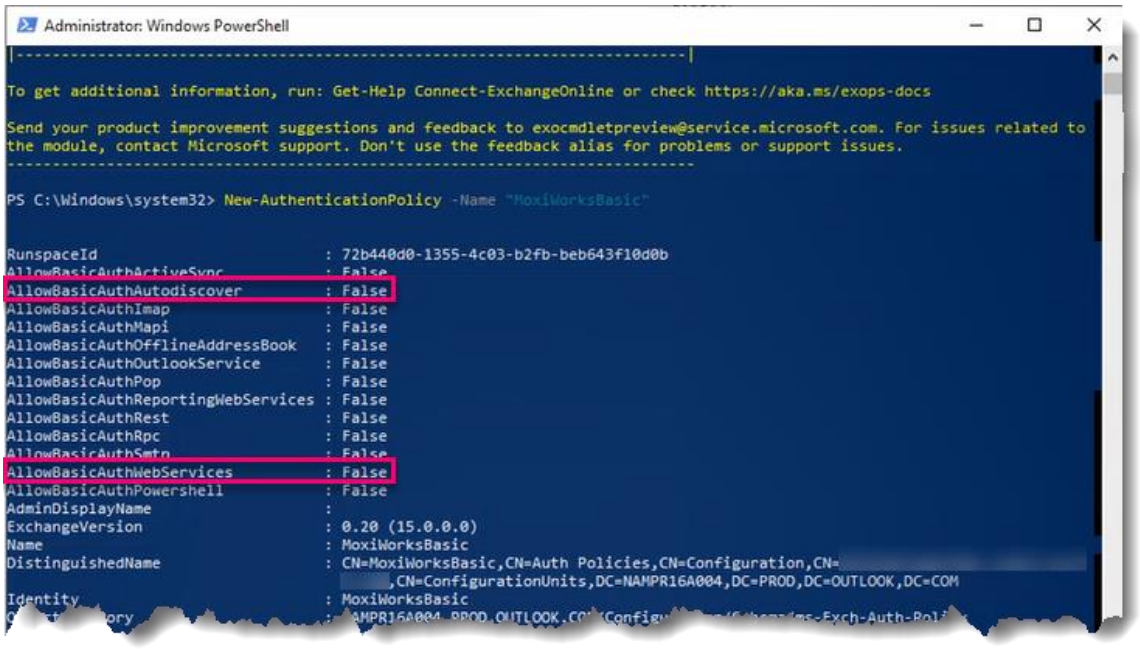
11. Type

```
New-AuthenticationPolicy -Name "MoxiWorksBasic"
```

and press Enter on your keyboard.



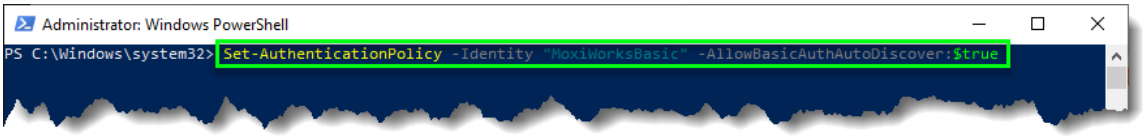
12. Review the default settings of the new authentication policy. Note that the value is “False” for “AllowBasicAuthAutoDiscover” and “AllowBasicAuthWebServices” in the list of properties. MoxiEngage needs the “True” value to be set for these properties.



13. Type

```
Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -
AllowBasicAuthAutoDiscover:$true
```

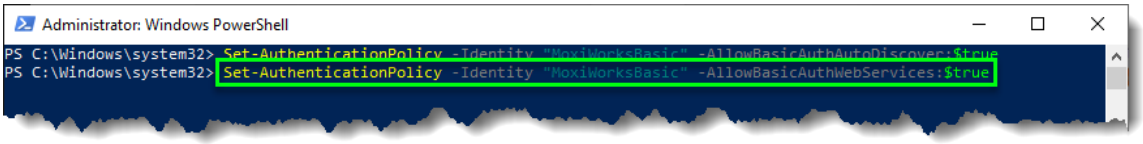
and press Enter on your keyboard.



14. Type

```
Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -
AllowBasicAuthWebServices:$true
```

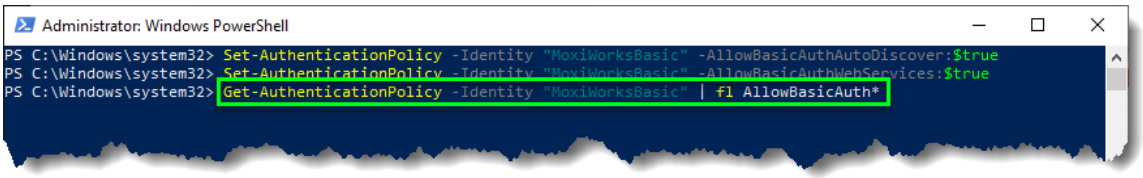
and press Enter on your keyboard.



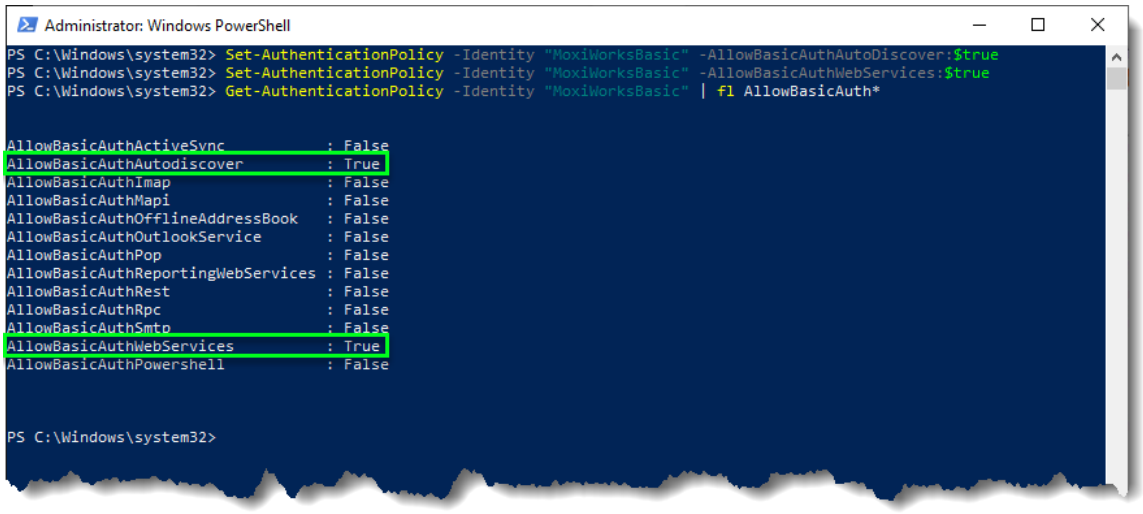
15. To verify the settings, type

```
Get-AuthenticationPolicy -Identity “MoxiWorksBasic” | fl
AllowBasicAuth*
```

and press Enter on your keyboard.



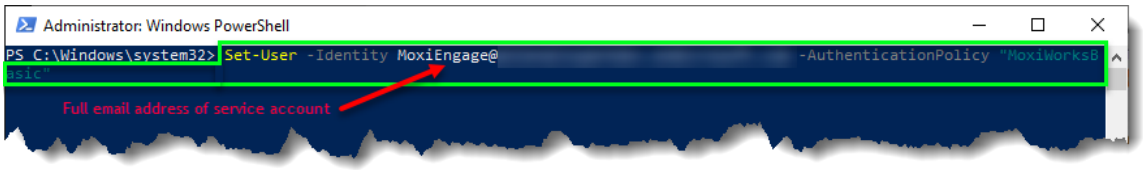
16. Note the “True” value displayed for the “AllowBasicAuthAutoDiscover” and “AllowBasicAuthWebServices” properties.



17. Type

`Set-User -Identity` {email address} `-AuthenticationPolicy "MoxiWorksBasic"`

replacing “{email address}” with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard to apply the authentication policy to the service account user.

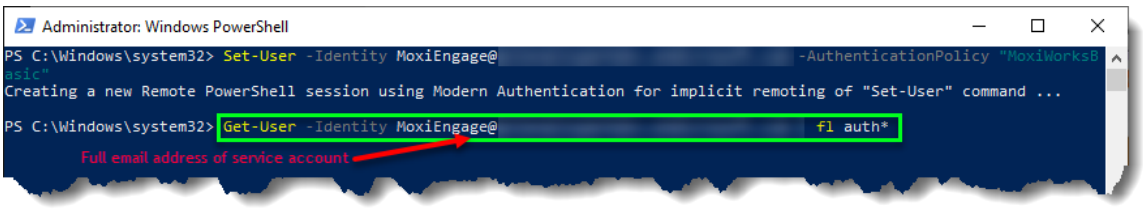


18. Wait for the prompt. You may notice a message saying that a new remote PowerShell session is being created. This is normal behavior.

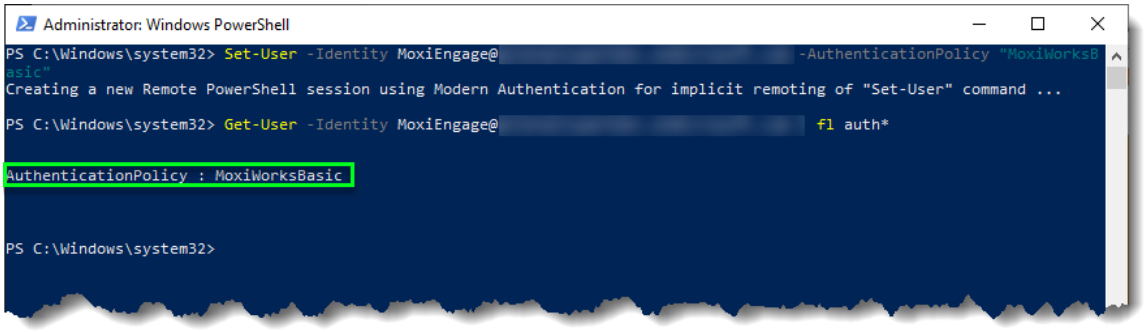
19. Type

`Get-User -Identity` {email address} `| fl auth*`

replacing “{email address}” with the email address of the service account you created for MoxiEngage, and press enter on your keyboard to verify the authentication policy set for the service account user.



20. Observe the response indicating the applied authentication policy.



21. Return to Test Service Account Impersonation for MoxiEngage to verify that impersonation using the service account is successful.

MoxiWorks

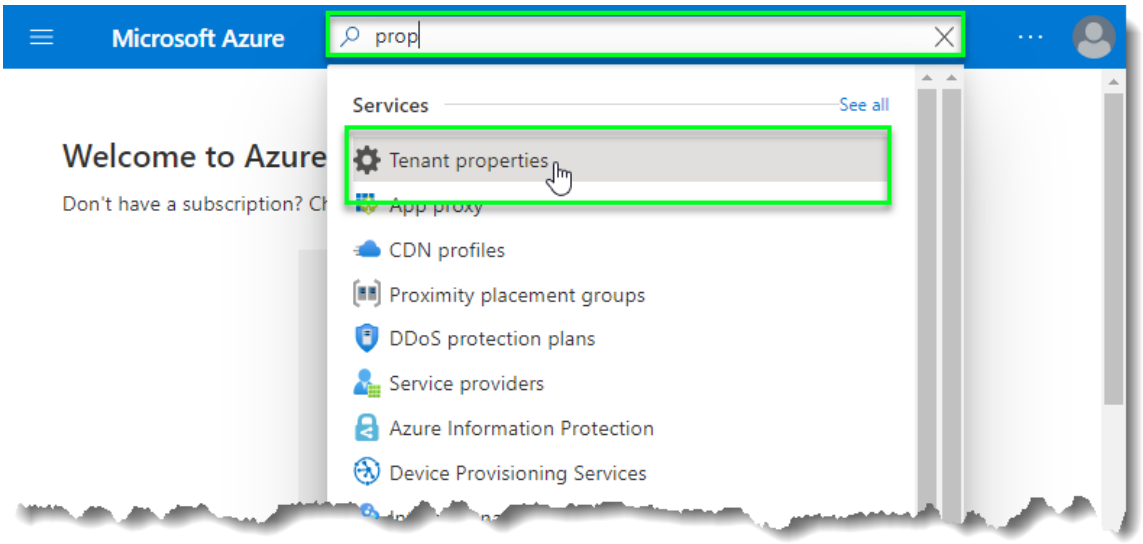
Adjust Conditional Access Policy for Service Account

Microsoft's "Security Defaults" implements a Conditional Access Policy that blocks connections made using basic authentication. This policy is applied automatically to new instances of Microsoft 365, and the policy cannot be modified. To change the conditional access settings, a new Conditional Access policy must be created. It is possible to set up a Conditional Access policy that reflects most of the settings in the default policy. However, instructions for doing so are outside the scope of this document.

The instructions provided here will assist you in disabling the "Security Defaults" Conditional Access Policy and creating a new Conditional Access Policy that requires multi-factor authentication (MFA) for all users except the MoxiEngage service account. Any additional security considerations and/or policy settings may be managed separately.

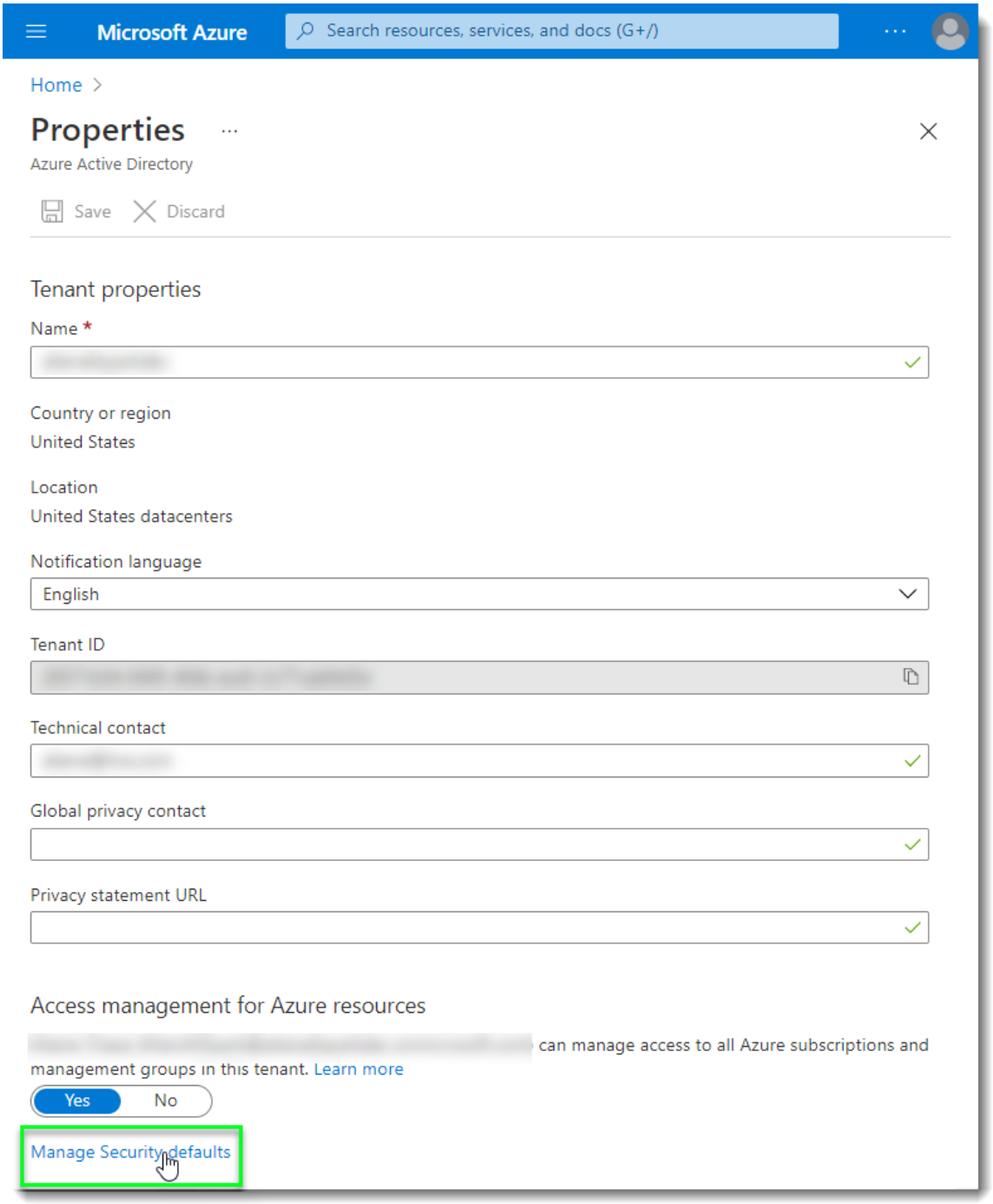
This document is not intended to provide advice regarding your security policies or protocols for Microsoft 365.

1. Login to your Microsoft Azure Portal as a Global Administrator.
2. Enter "prop" in the search box, then click on the "Tenant properties" option in the resulting list of services.

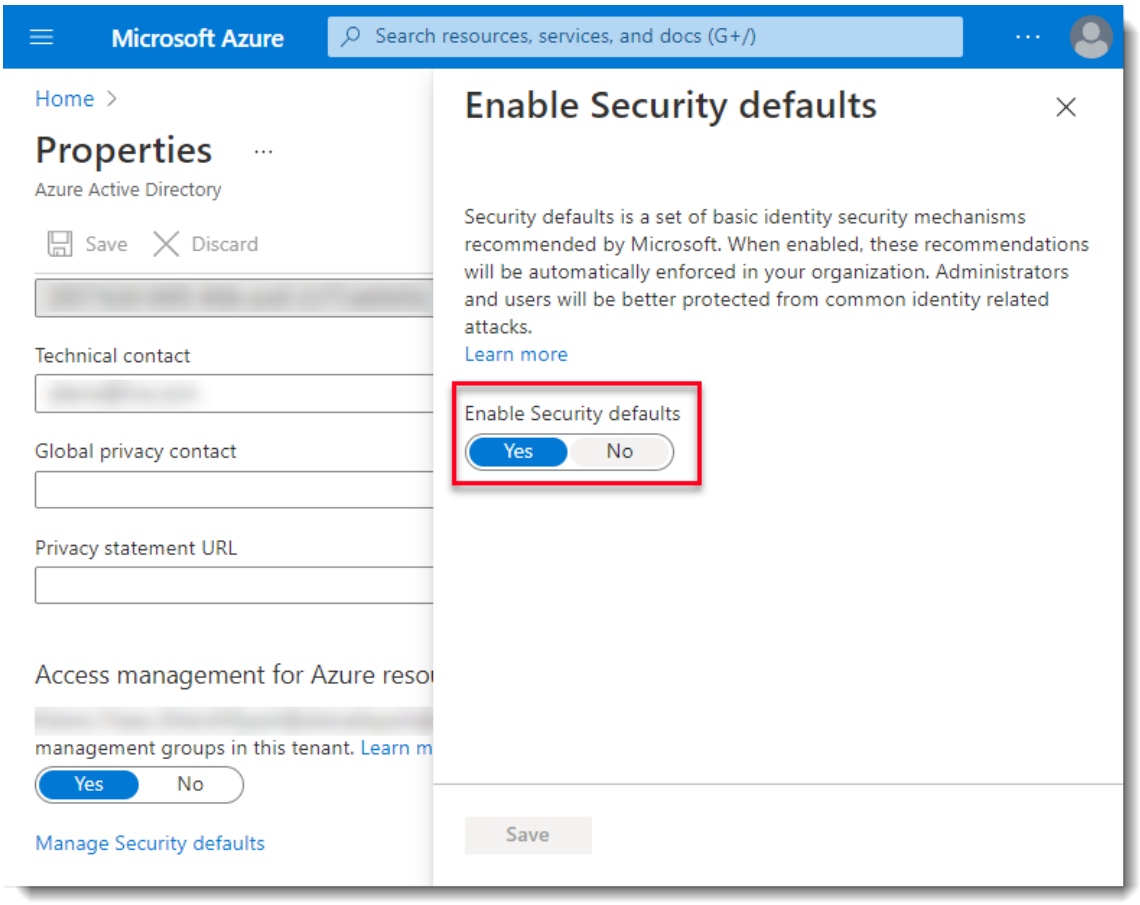


MoxiWorks

3. Click on the “Manage Security defaults” link at the bottom of the Properties page.



4. Note whether the Security defaults in your Microsoft 365 tenant are enabled, as shown here:

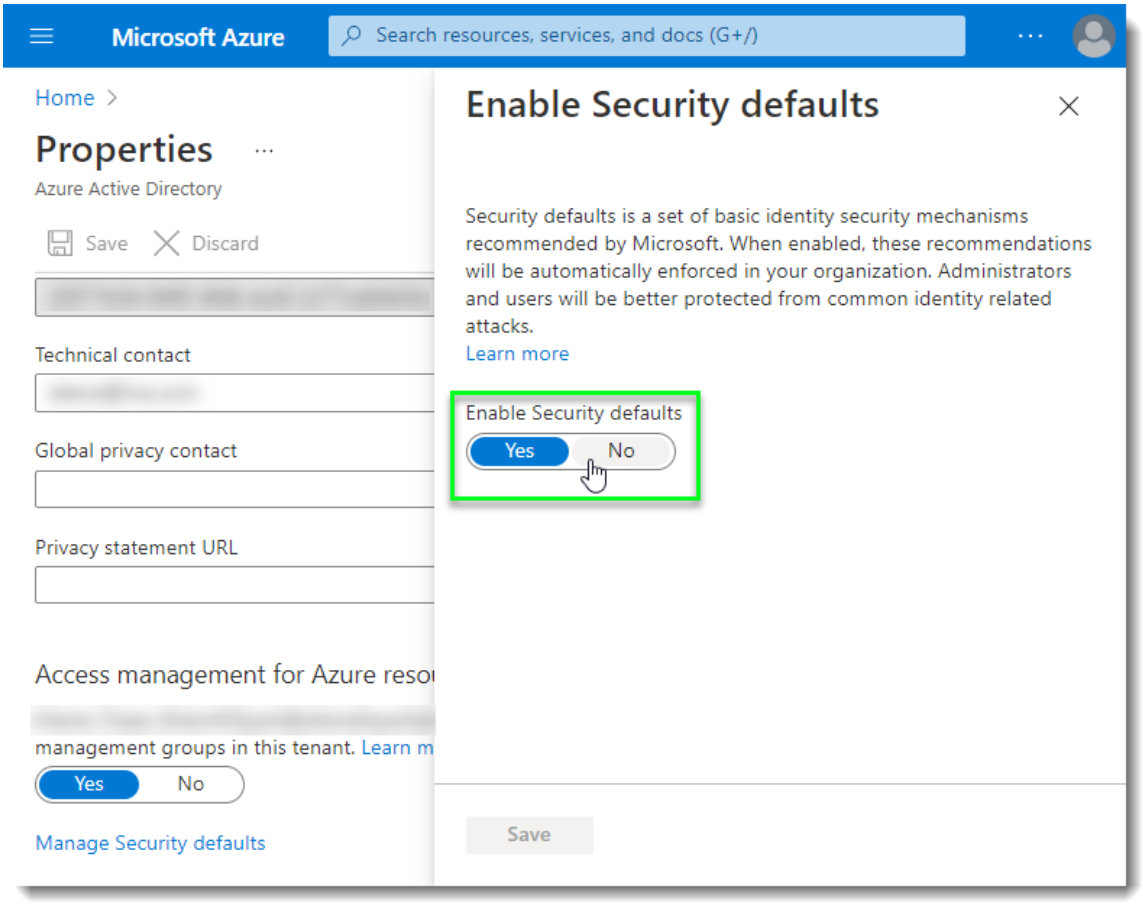


Note

If the Security defaults are not enabled, do not proceed with the following steps.

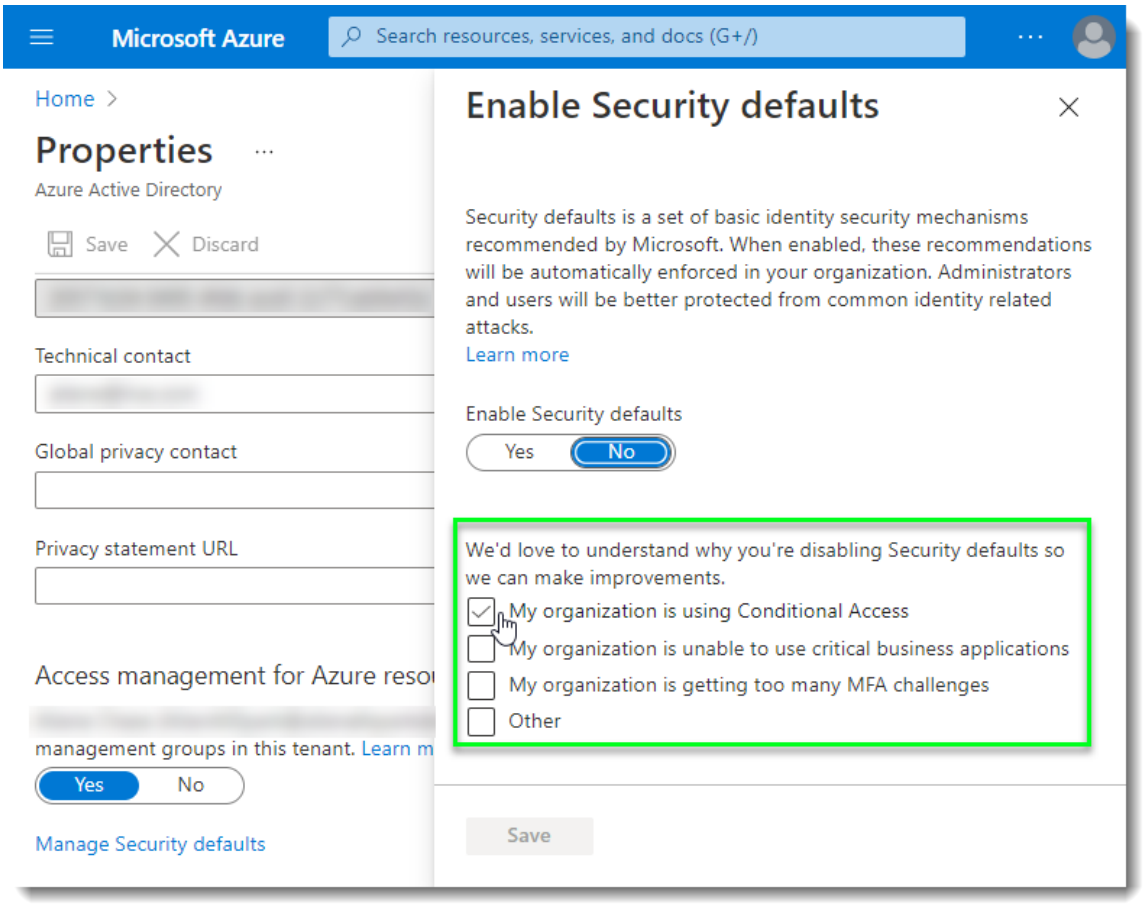
MoxiWorks

5. Click to toggle the “Enable Security defaults” Yes/No slider to the “No” setting.

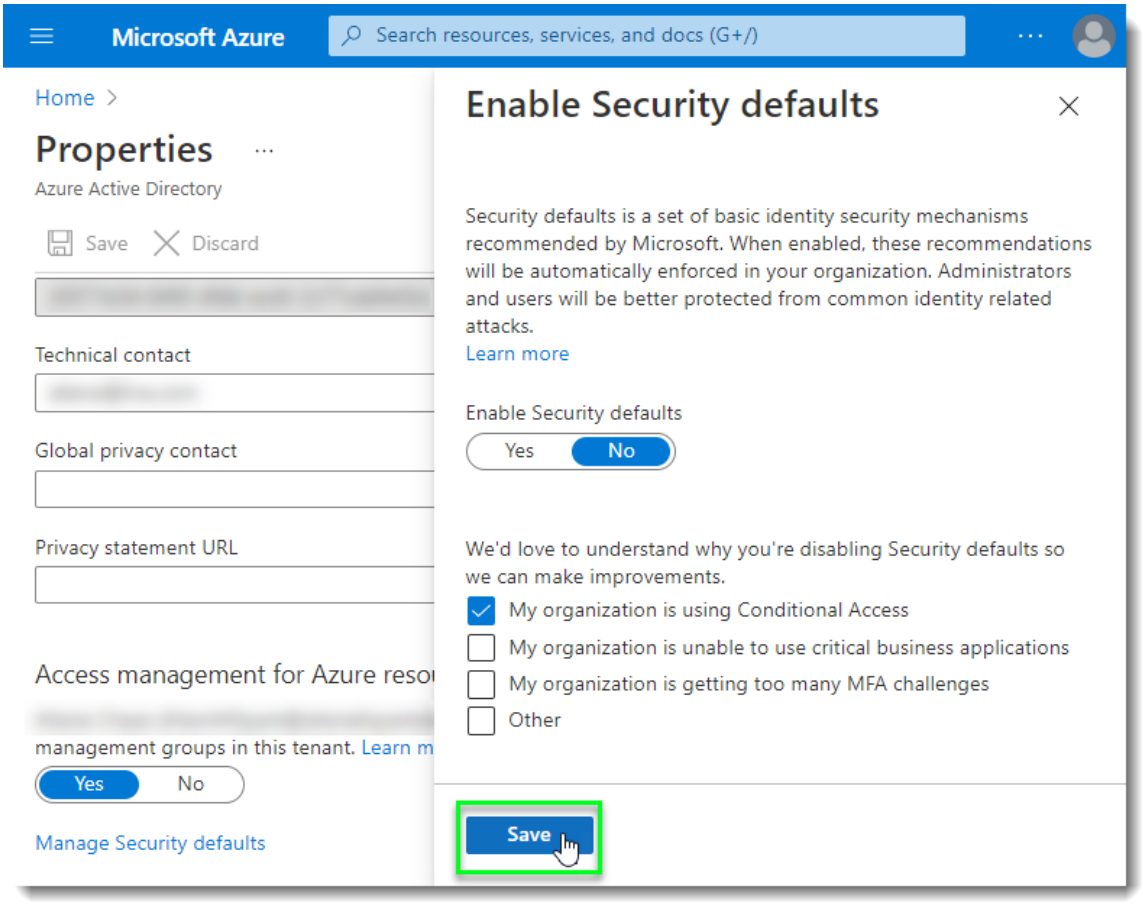


MoxiWorks

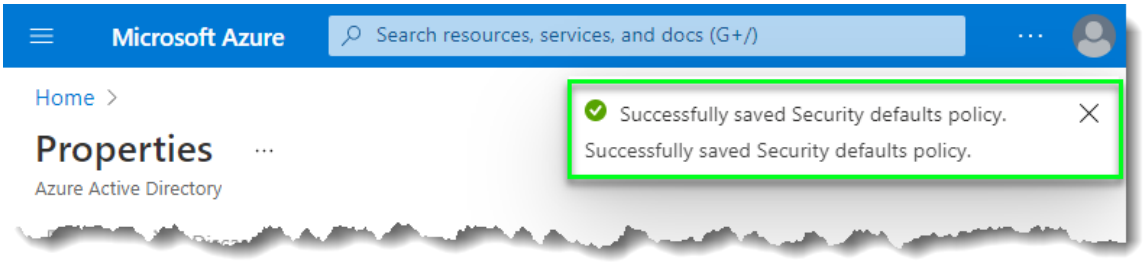
6. Select a reason for disabling Security defaults (i.e., “My organization is using Conditional Access”).



7. Click on the “Save” button.



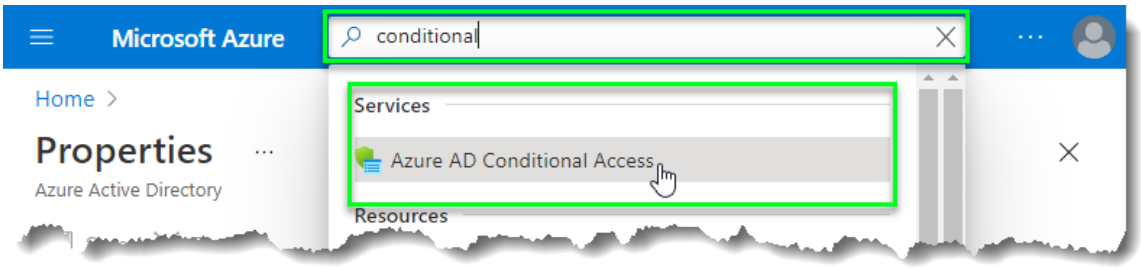
8. Observe the message indicating that your change to the Security defaults policy have been saved.



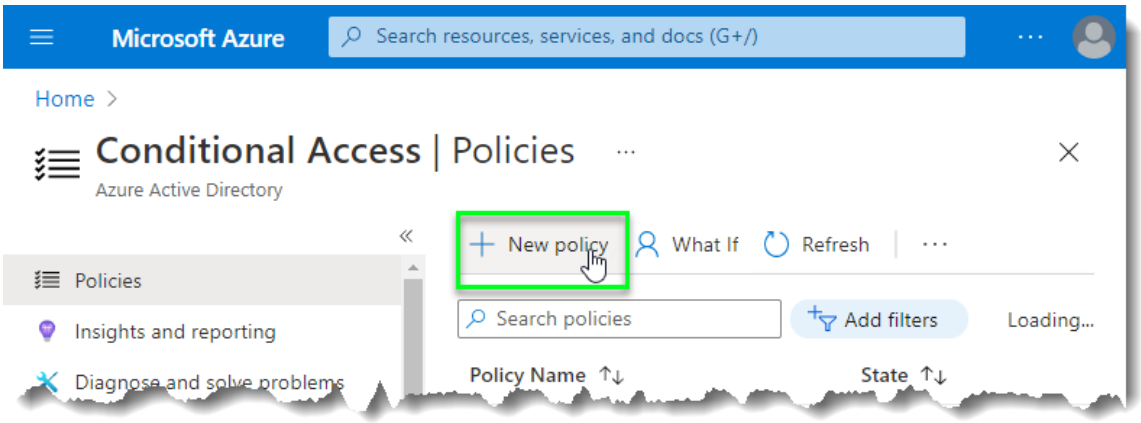
Note

At this point, all access controls managed by the Security defaults policy are disabled. This includes multi-factor authentication (MFA). If you are using MFA and wish to continue doing so, perform the following steps to reinstate the requirement for MFA on all users except the MoxiEngage service account.

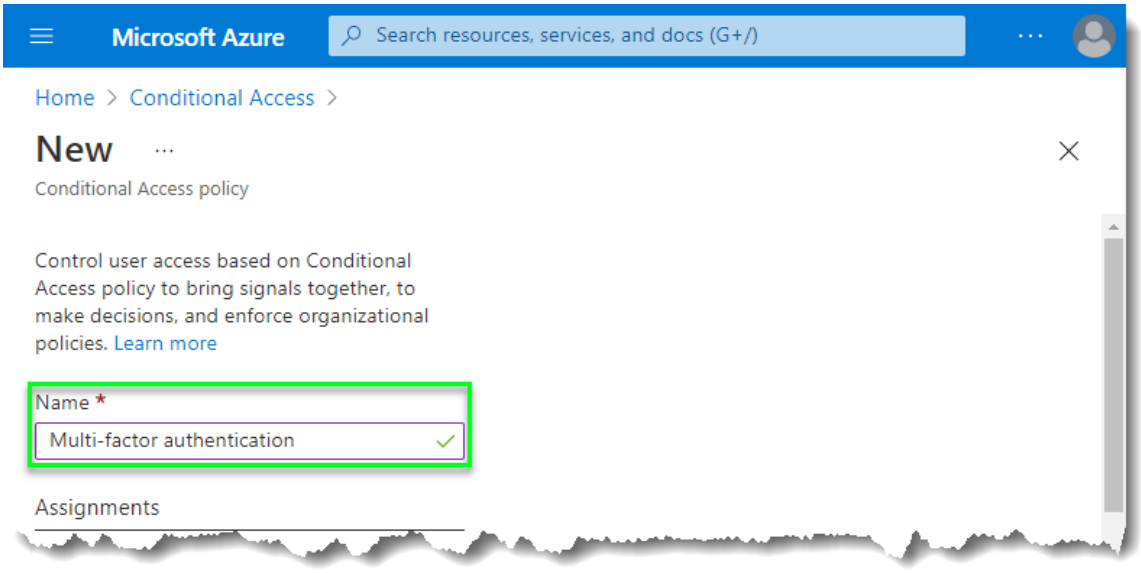
9. Enter “conditional” in the search box, then click on the “Azure AD Conditional Access” option in the resulting list of services.



10. Click on the “New policy” button.

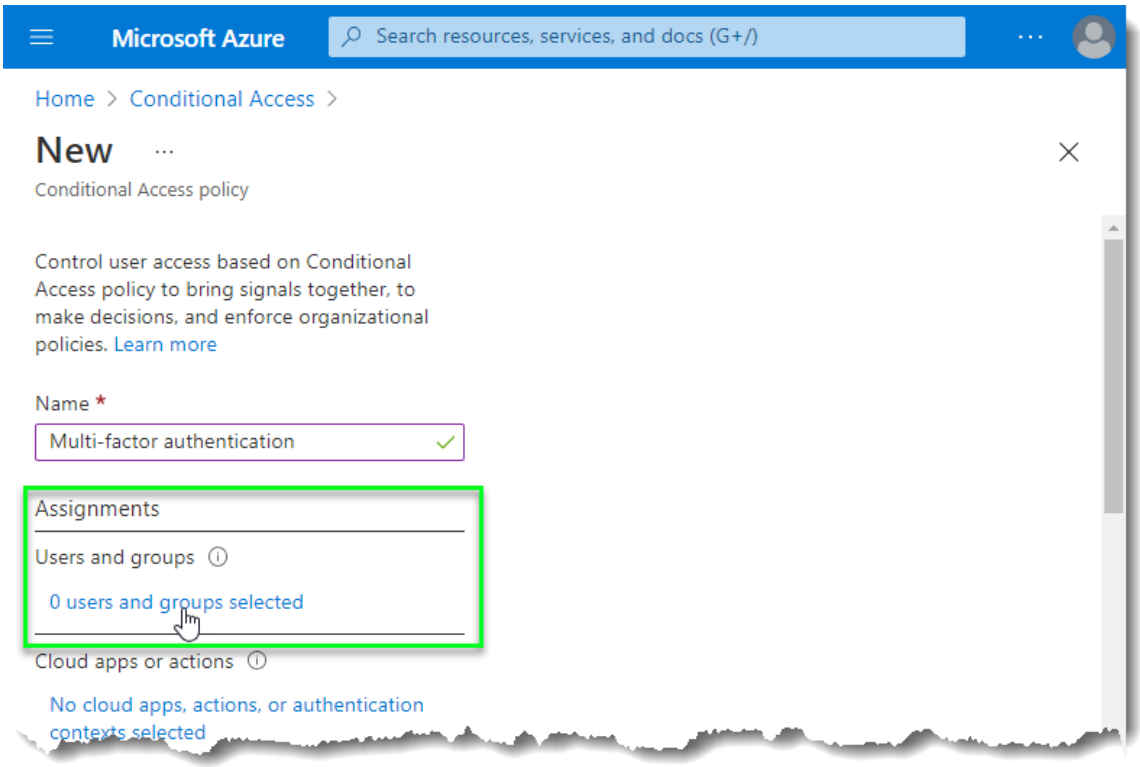


11. Enter a name for your policy in the “Name” box (e.g., “Multi-factor authentication”).

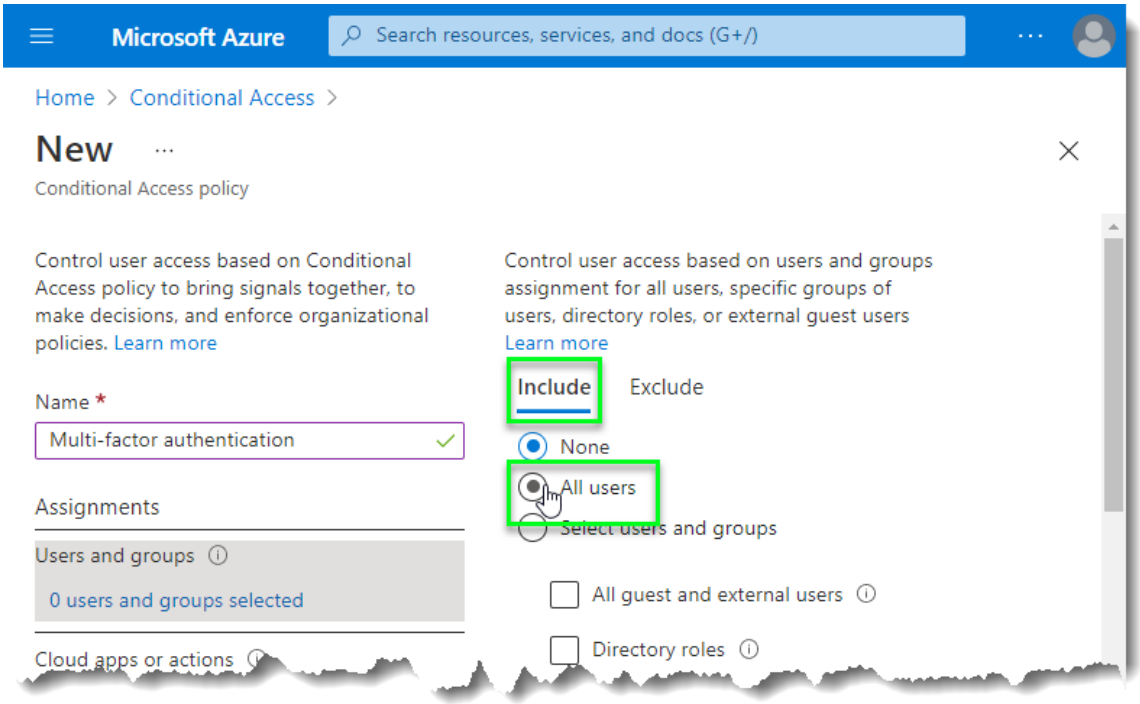


MoxiWorks

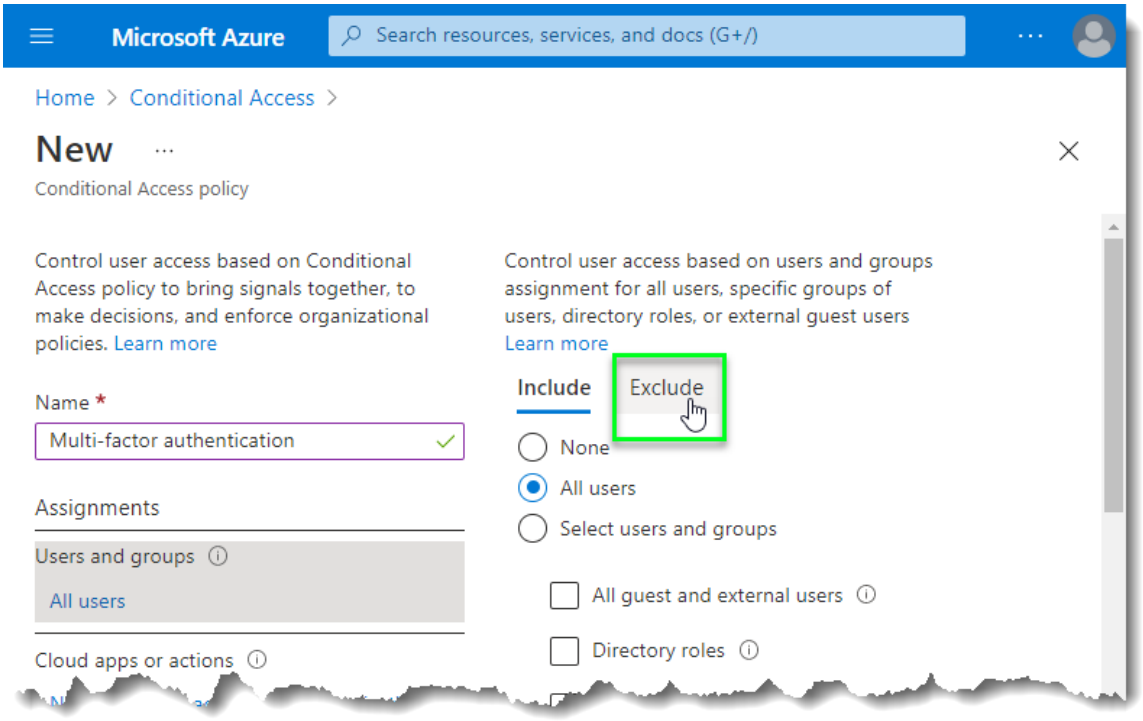
12. Click on the “0 users and groups selected” link in the “Assignments: Users and Groups” section.



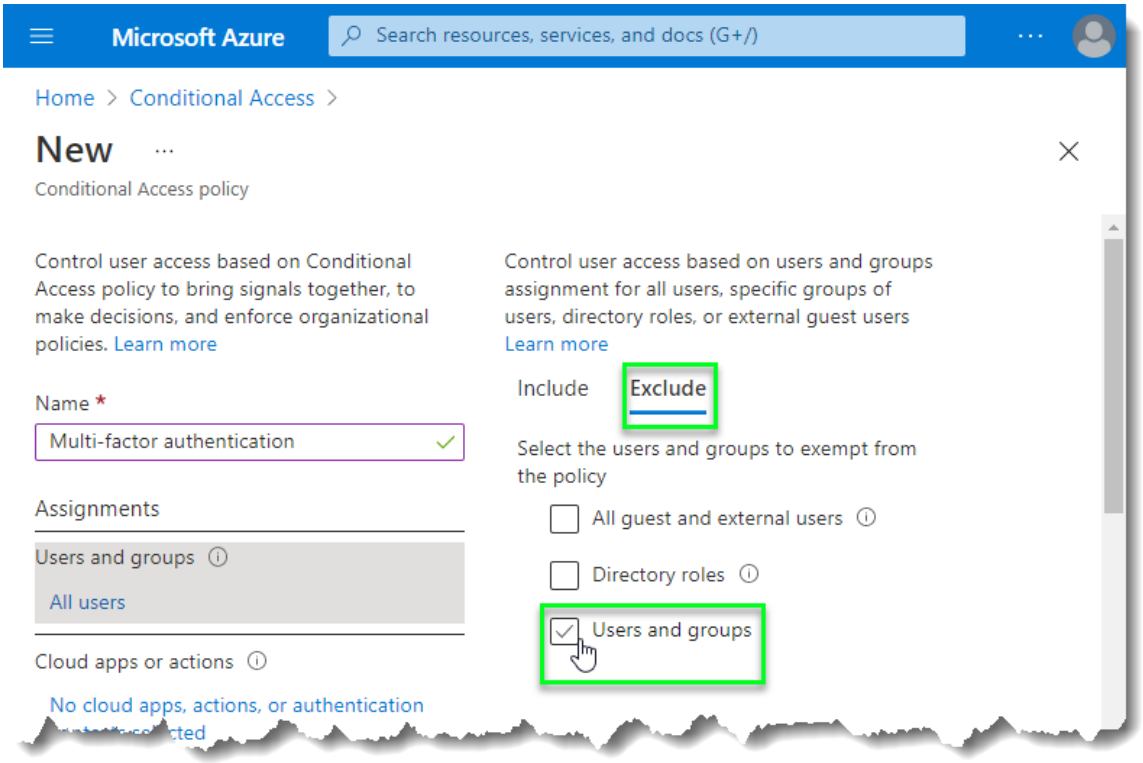
13. Ensure the “Include” tab of the overlay form is selected, then click on the radio button next to the “All users” label.



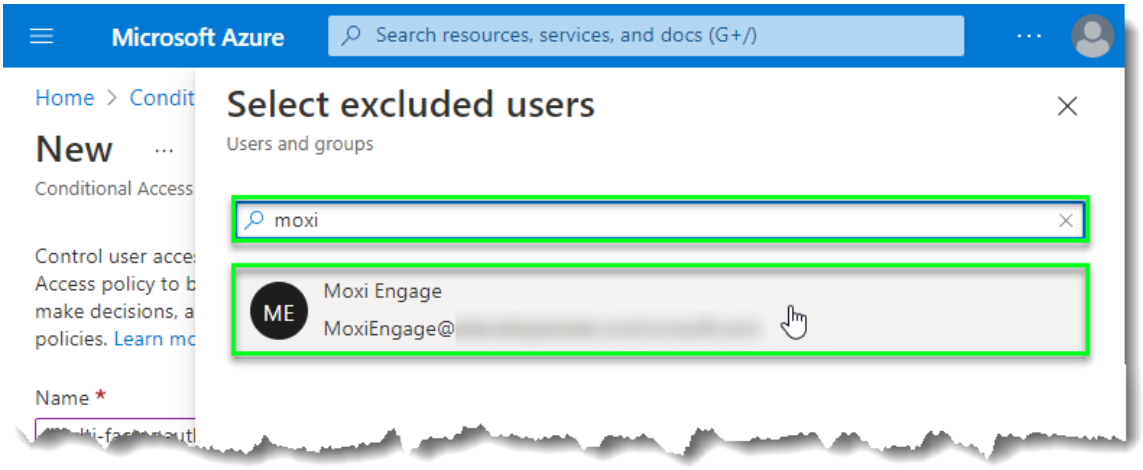
14. Click on the “Exclude” tab of the overlay form.



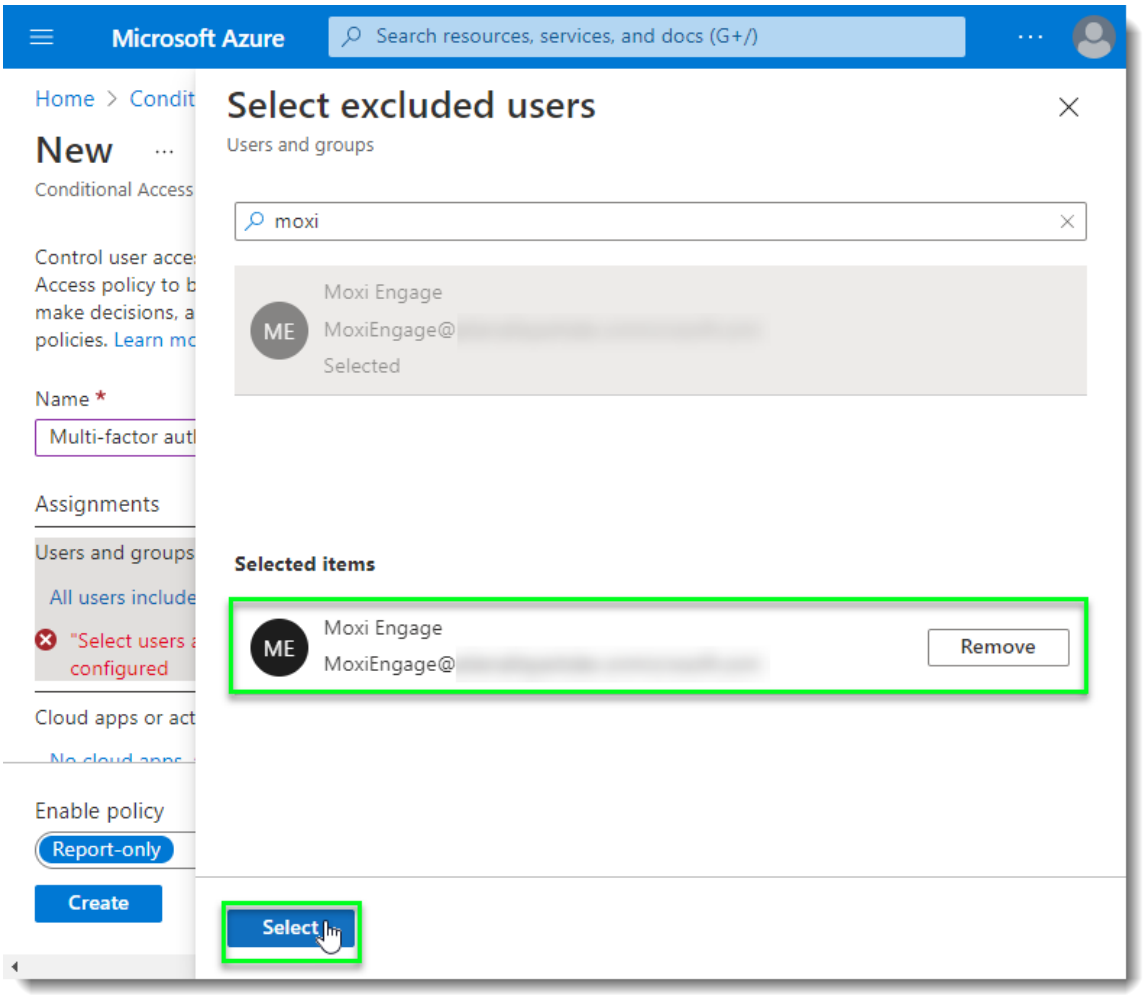
15. Ensure the “Exclude” tab of the overlay form is selected, then mark the checkbox next to the “Users and groups” label.



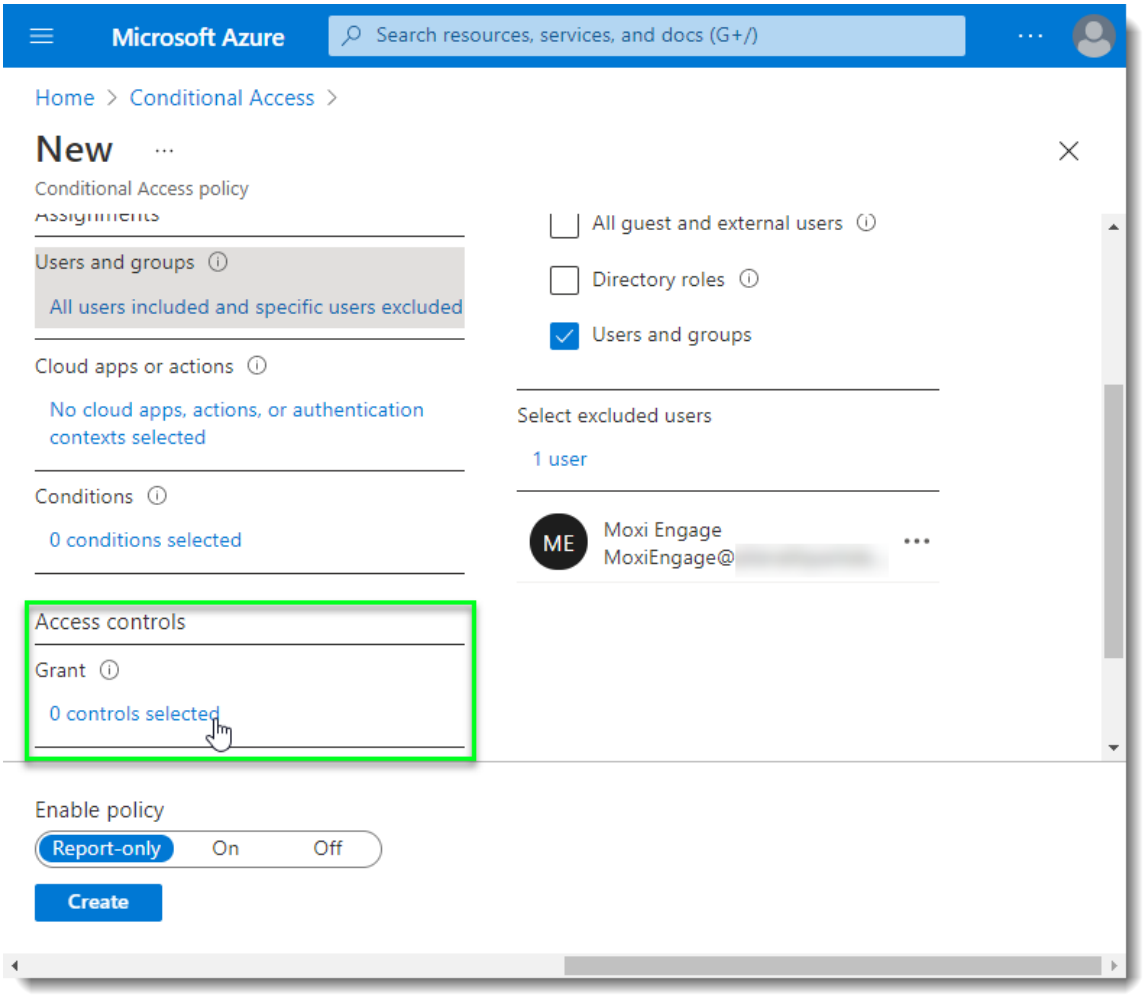
16. Begin typing the name of the service account in the “Select excluded users” search box (e.g., “Moxi”), then click on the service account user in the list to select it for exclusion.



17. Note that the service account user is in the “Selected items” list, then click on the “Select” button.

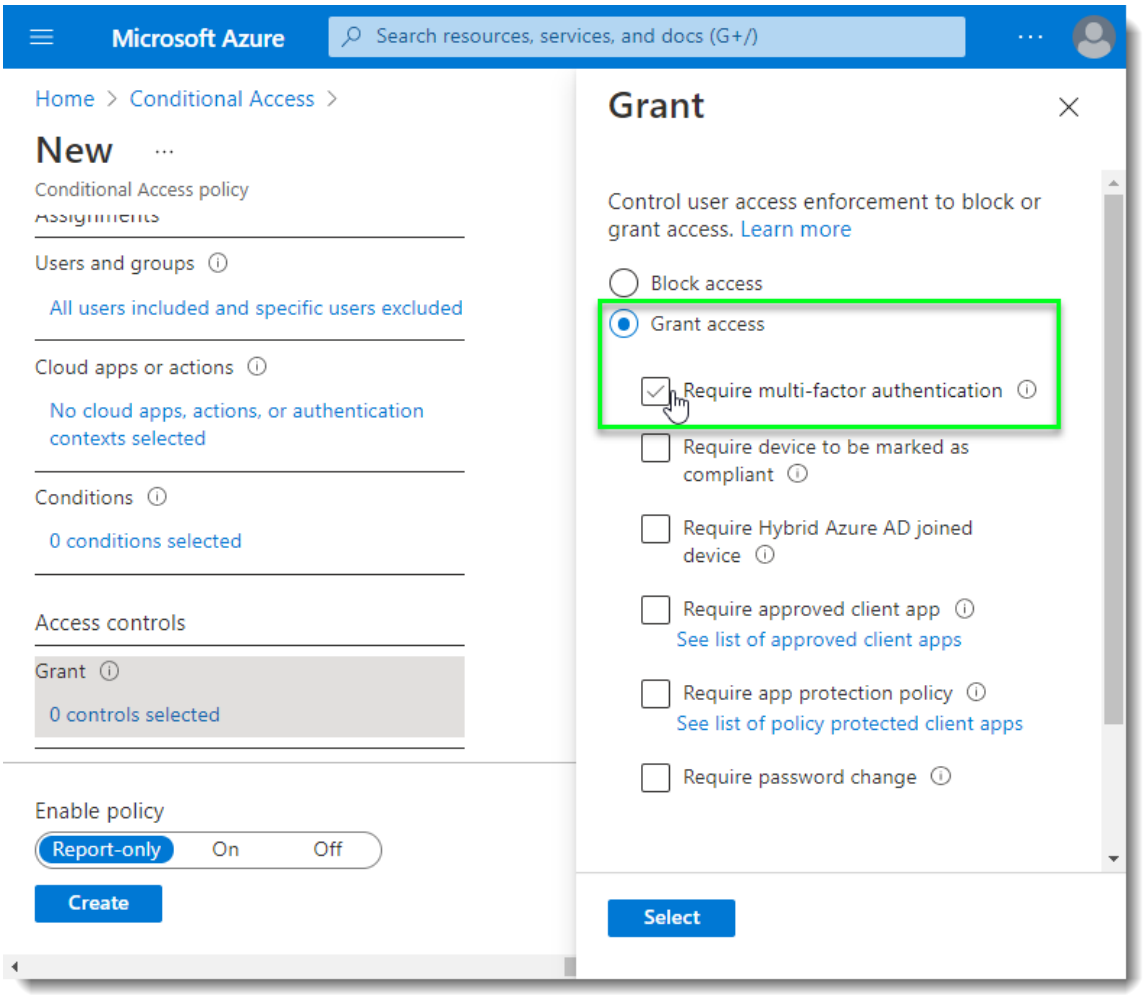


18. Click on the “0 controls selected” link in the “Access controls: Grant” section.

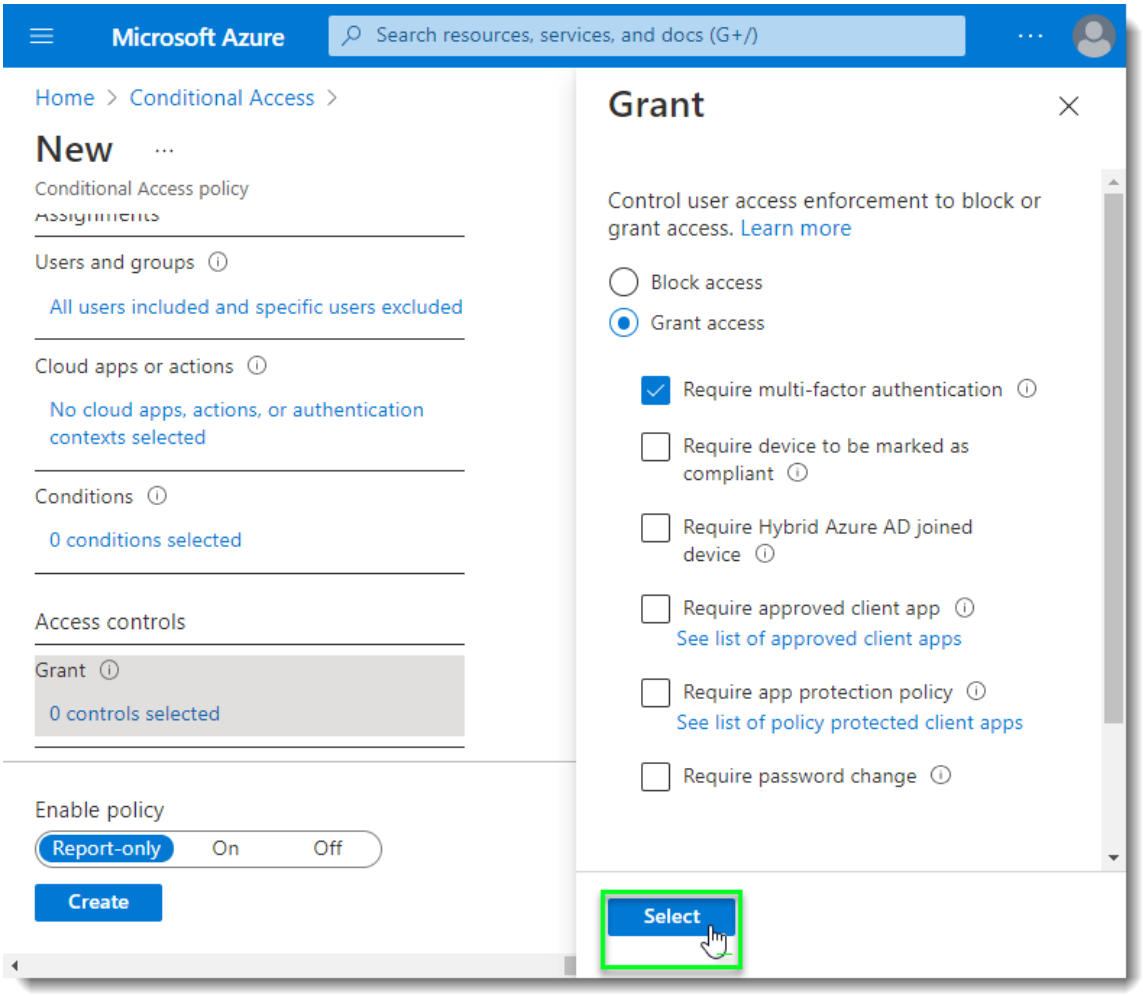


MoxiWorks

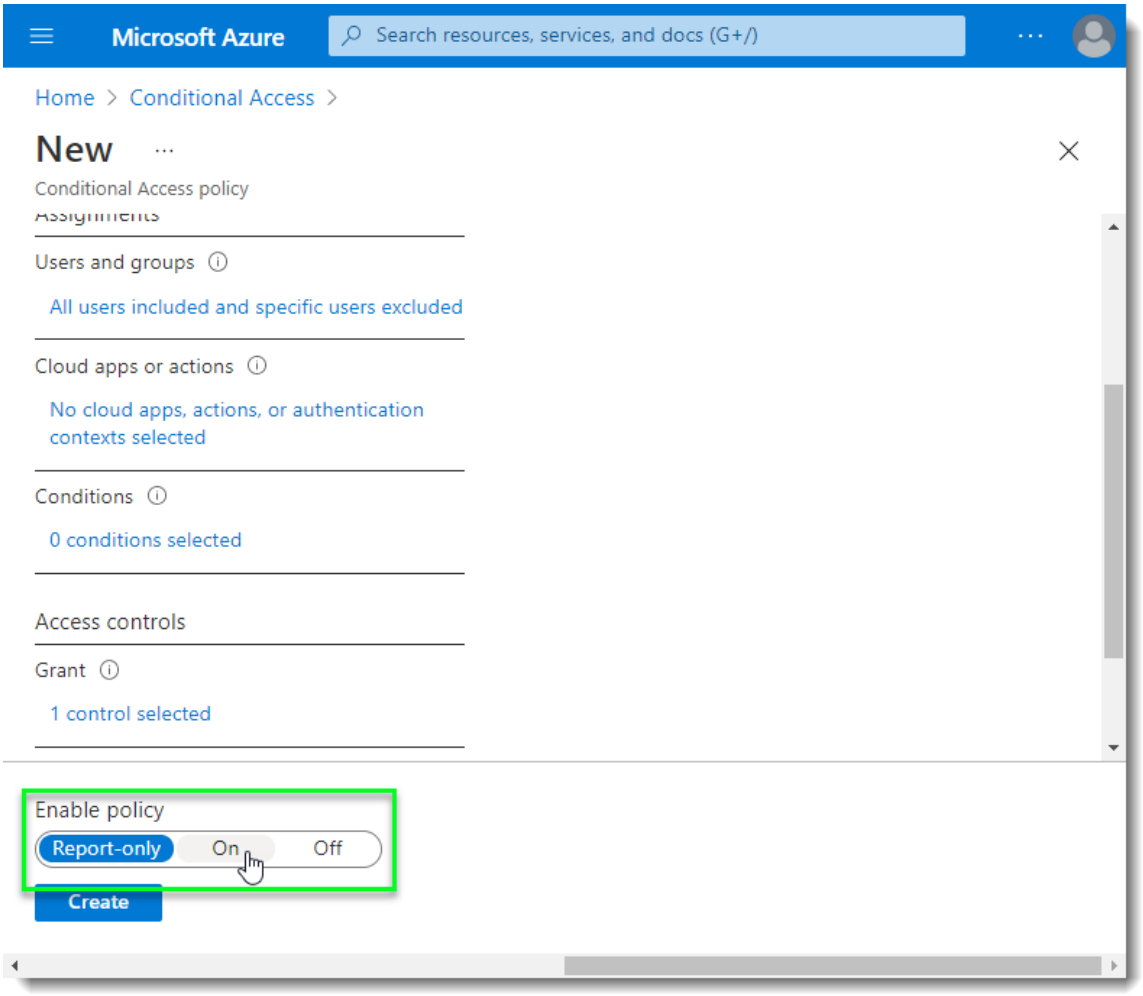
19. Ensure the “Grant access” radio button is selected, then mark the checkbox next to the “Require multi-factor authentication” label.



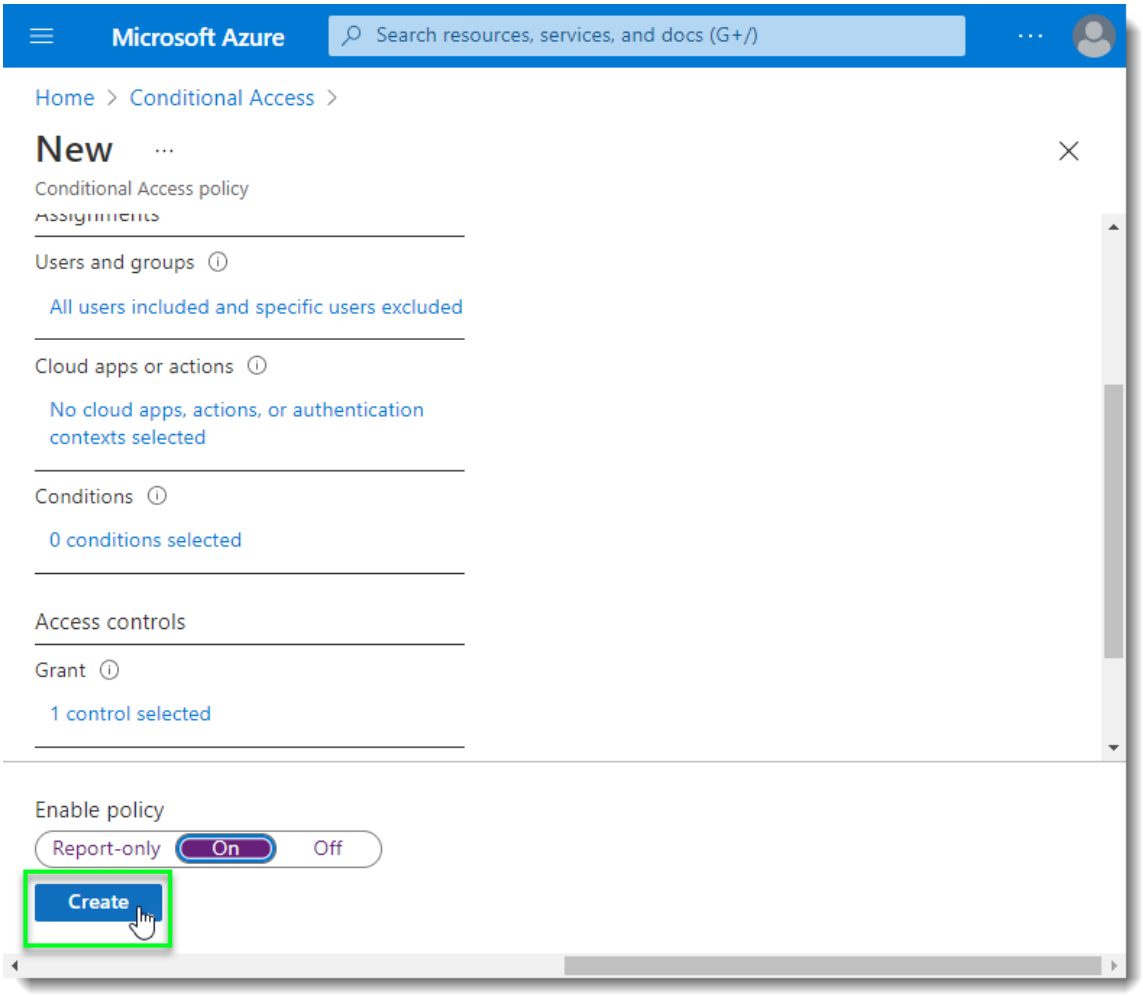
20. Click on the “Select” button.



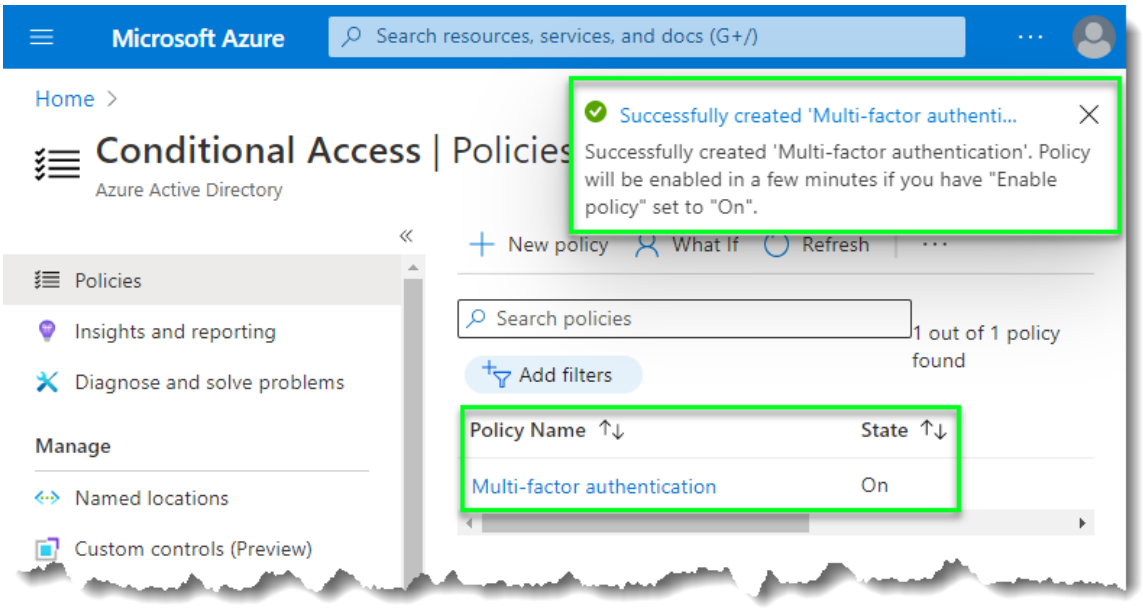
21. Click to select “On” from the “Enable policy” slider.



22. Click on the “Create” button.



23. Observe the notification that your new policy has been created and that the new policy is displayed in the list of Conditional Access Policies with an “On” State.



24. Return to Test Service Account Impersonation for MoxiEngage to verify that impersonation using the service account is successful.

Related Resources

The following resources may provide additional information you need to perform the requisite tasks:

- Compare Active Directory to Azure Active Directory
- Azure AD PowerShell Module
- Connect to Microsoft 365 with PowerShell
- Set an individual user's password to never expire
- End of support for Basic Authentication access to Exchange Online API’s for Office 365 customers
- Exchange Online deprecating Basic Authentication (Basic Auth)
- What are security defaults?
- Disable Basic authentication in Exchange Online
- Exchange Online Management PowerShell Module
- About PowerShell Execution Policies
- Connect to Exchange Online PowerShell
- What is Conditional Access?