

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.



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>



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

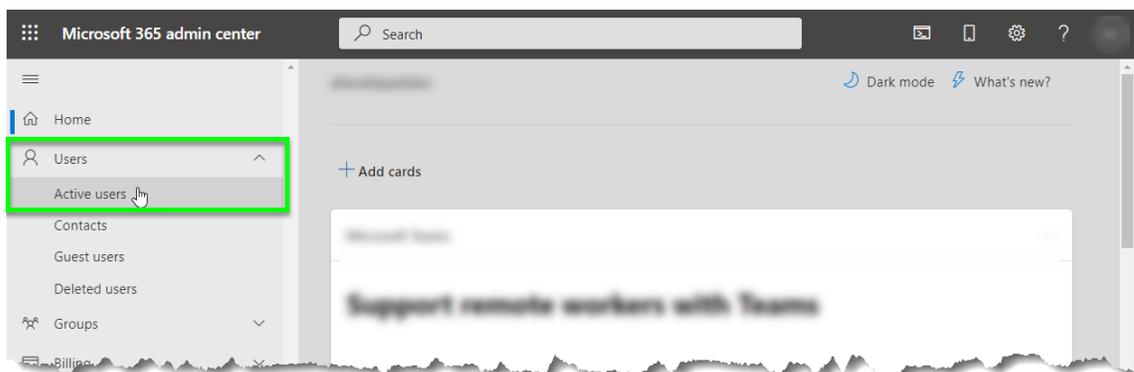
If your Microsoft 365 instance is hosted by a third-party vendor (i.e., GoDaddy, etc.), your Admin user interface may not match the instructions provided here. Please contact your email vendor for assistance. Feel free to provide a copy of this document to your vendor as a guide and explanation of what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

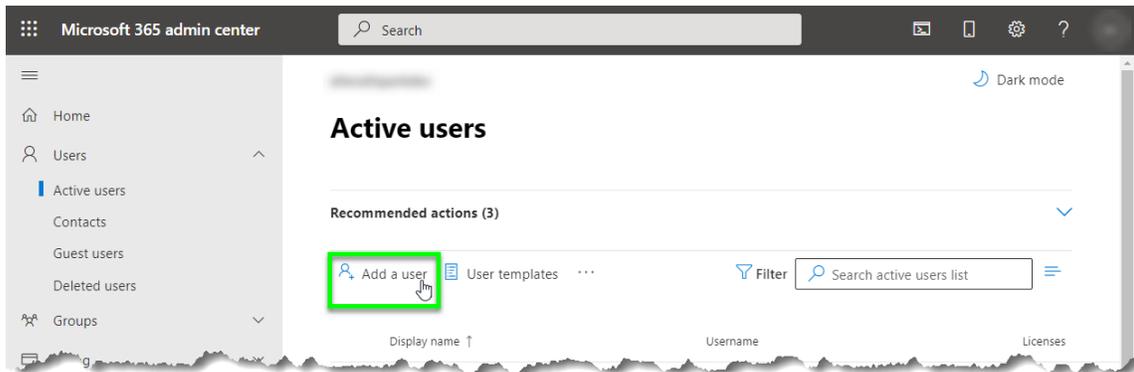
The instructions provided in this guide are not intended to provide security advice for configuring your Microsoft 365 instance. The documented steps represent the most direct approach available at the time of this writing to achieve the necessary access required by MoxiWorks products. Other methods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

Create a Service Account User

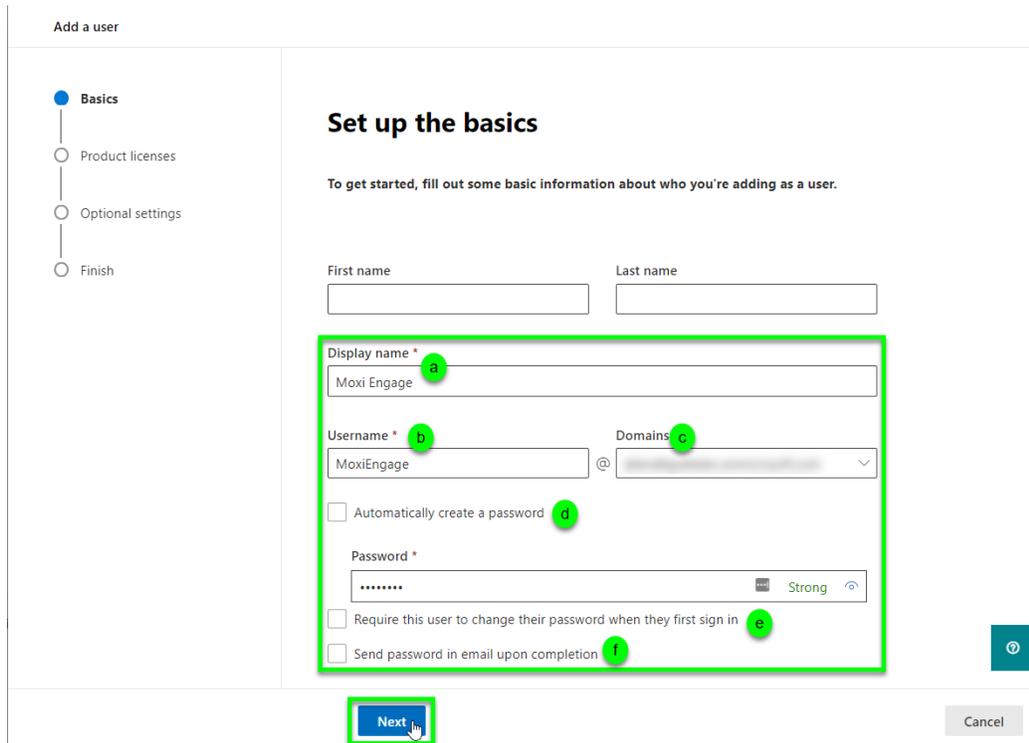
1. Login to your [Microsoft 365 Admin Center](#).
2. Click to expand the "Users" section of the menu, then click on the "Active users" option.



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).

A screenshot of the 'Add a user' form in the Microsoft 365 admin center. The form is titled 'Set up the basics' and includes a progress indicator on the left with steps: Basics (selected), Product licenses, Optional settings, and Finish. The main form fields are: 'First name' and 'Last name' (empty text boxes); 'Display name *' (text box containing 'Moxi Engage', marked with a green 'a'); 'Username *' (text box containing 'MoxiEngage', marked with a green 'b'); 'Domains' (dropdown menu, marked with a green 'c'); 'Automatically create a password' (checkbox, marked with a green 'd'); 'Password *' (password field with a strength indicator 'Strong', marked with a green 'e'); 'Require this user to change their password when they first sign in' (checkbox, marked with a green 'e'); and 'Send password in email upon completion' (checkbox, marked with a green 'f'). A blue 'Next' button is highlighted with a green box at the bottom, and a grey 'Cancel' button is visible to its right.

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.

Add a user

Basics
Product licenses
Optional settings
Finish

Assign product licenses

Assign the licenses you'd like this user to have.

Select location *
United States

Licenses (0)*

Assign user a product license

Microsoft 365 E5 Developer (without Windows and Audio Conferencing)
9 of 25 licenses available

Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

Apps (0)

Back Next Cancel

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

Add a user

- ✓ Basics
- ✓ Product licenses
- **Optional settings**
- Finish

Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles (User: no administration access) ▼

Profile info ▼

ⓘ

Back **Next** Cancel

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

Add a user

- ✓ Basics
- ✓ Product licenses
- ✓ Optional settings
- **Finish**

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
Moxi Engage
MoxiEngage@ [redacted]
[Edit](#)

Password
Type: Custom password
[Edit](#)

Product licenses
Create user without product license.
[Edit](#)

Roles (default)
User (no admin center access)
[Edit](#)

Profile info

[Back](#) [Finish adding](#) [Cancel](#)



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

Add a user

- ✓ Basics
- ✓ Product licenses
- ✓ Optional settings
- ✓ Finish

✓ Moxi Engage added to active users

Moxi Engage will now appear in your list of active users.

User details
Display name: Moxi Engage
Username: MoxiEngage@
Password: ***** [Show](#)

Licenses bought
None

Licenses assigned
None

Save these user settings as a template?

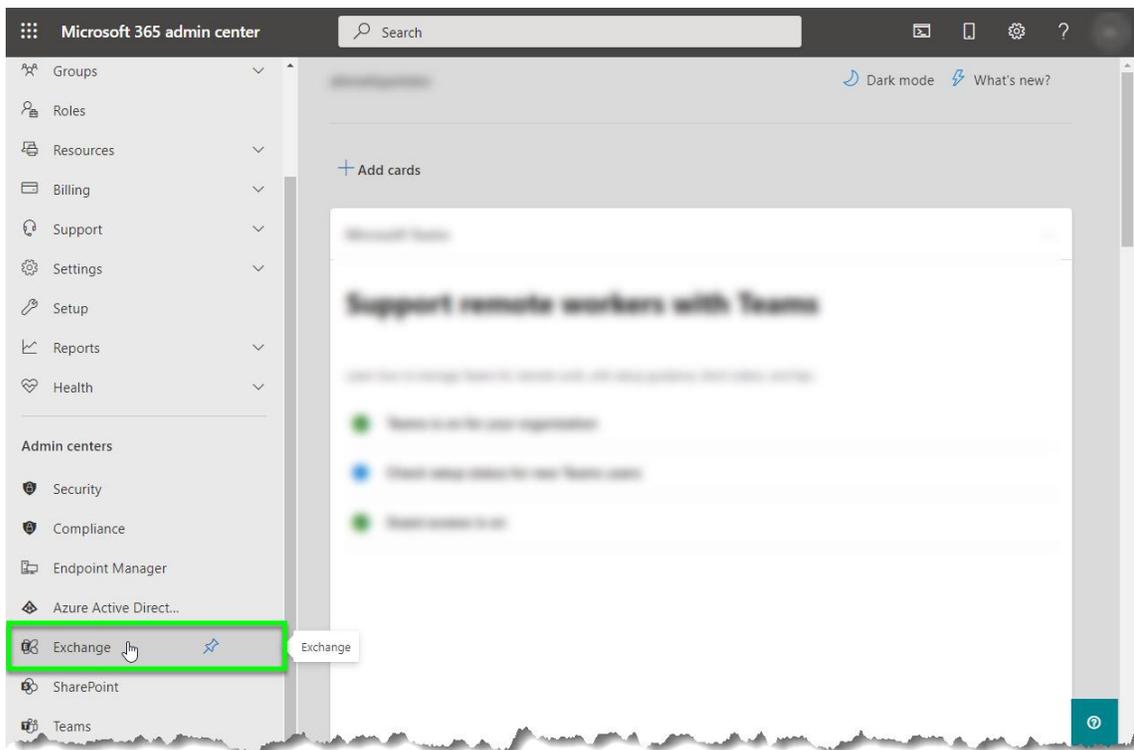
User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.

[Review settings for this user template](#)

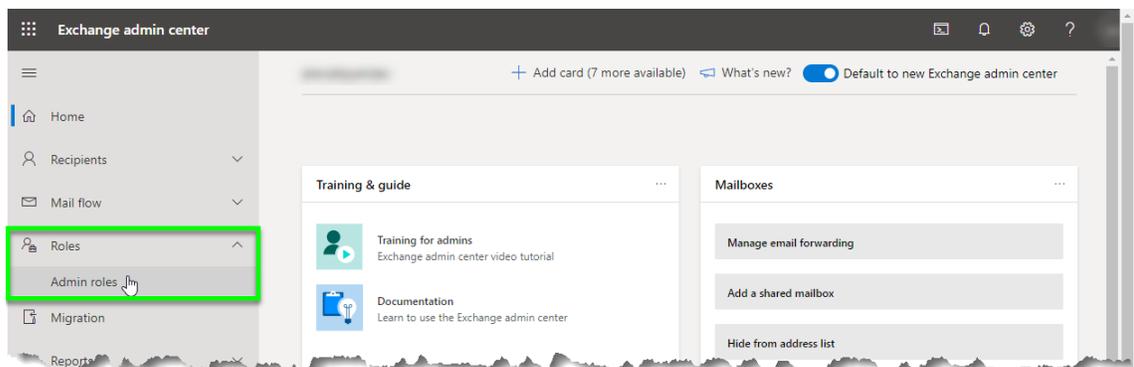
[Close](#)

Grant Application Impersonation to the Service Account User

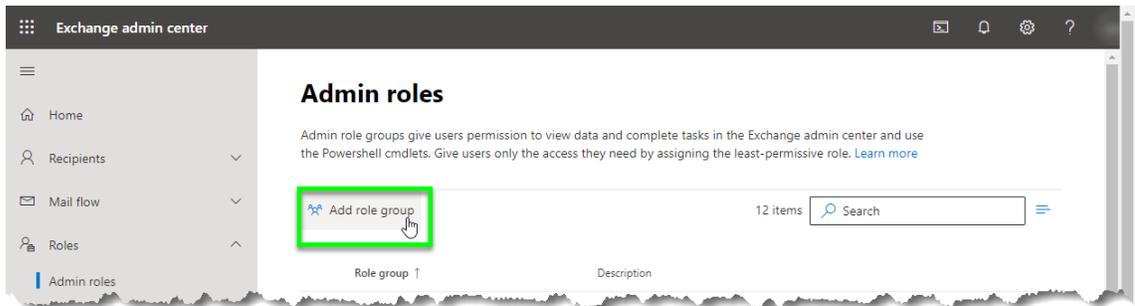
1. Login to your [Microsoft 365 Admin Center](#).
2. Click on the “Exchange” menu option under the “Admin centers” area of the menu. (If this option is not visible, you can click on “Show all” to expand the menu.)



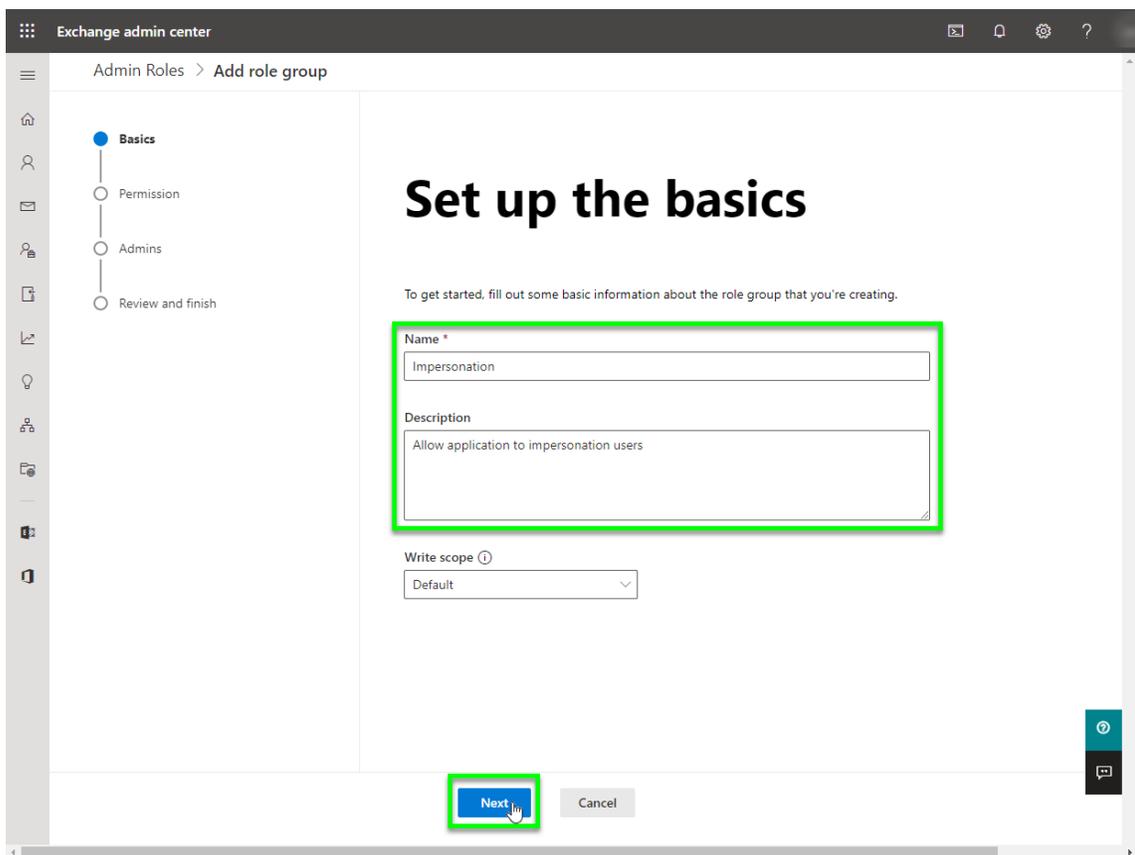
3. In the Exchange Admin Center, expand the “Roles” area of the menu and click on the “Admin roles” option.



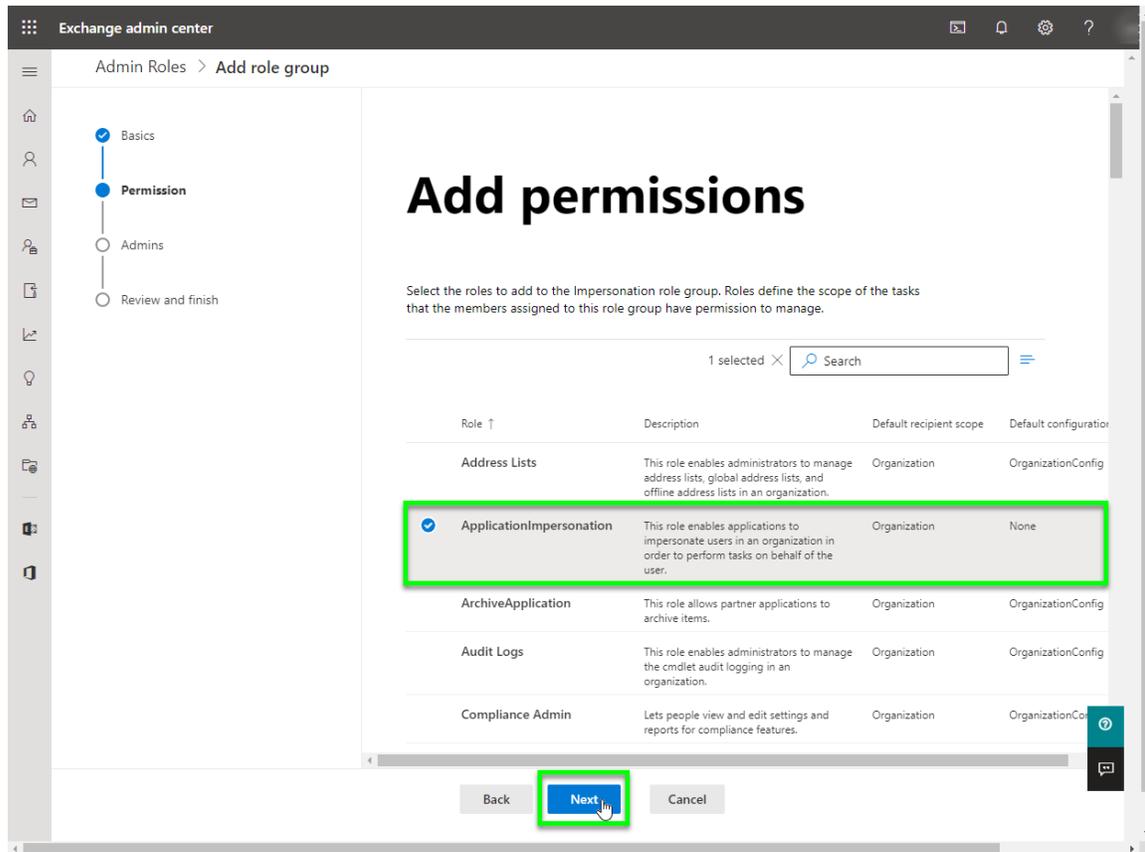
4. Click on the “Add role group” option button.



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.

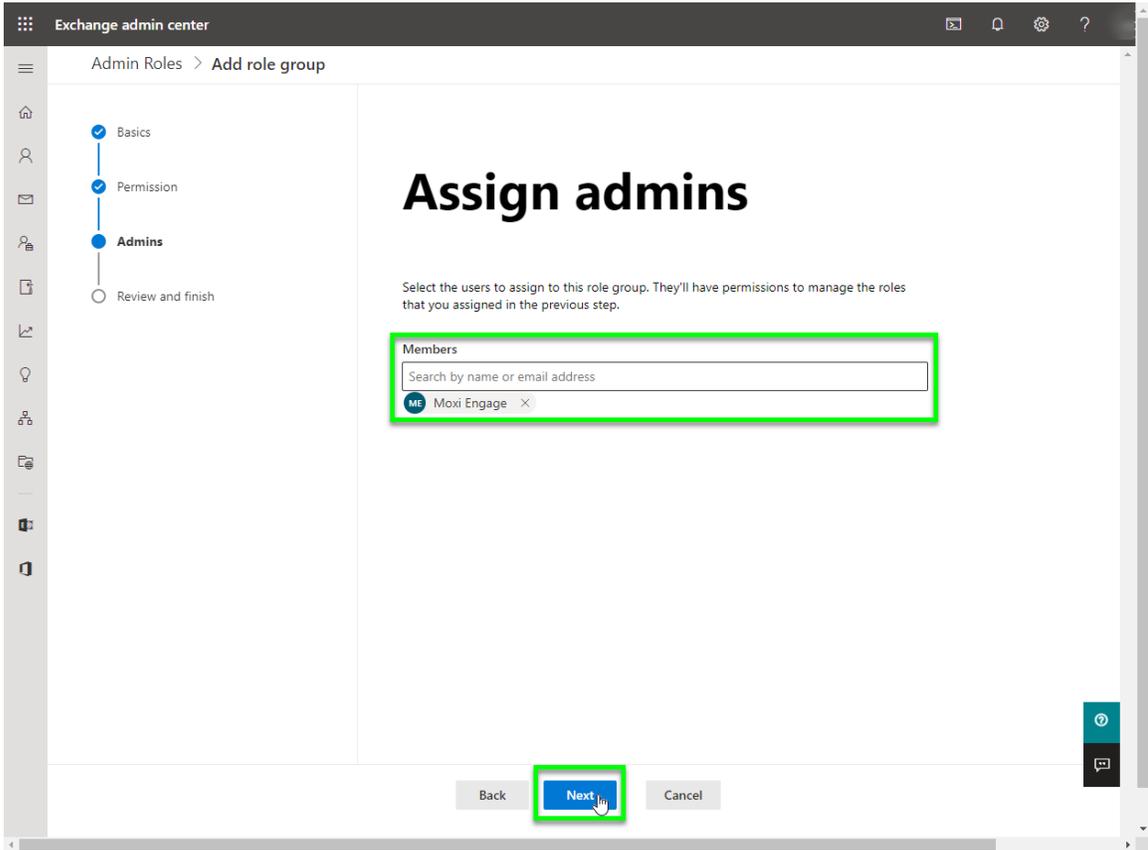


The screenshot shows the Exchange Admin Center interface for adding permissions to a role group. The page title is "Add permissions". A navigation pane on the left shows steps: Basics (checked), Permission (selected), Admins, and Review and finish. The main content area has a heading "Add permissions" and a sub-heading "Select the roles to add to the Impersonation role group. Roles define the scope of the tasks that the members assigned to this role group have permission to manage." Below this is a search bar with "1 selected" and a search input field. A table lists available roles:

Role ↑	Description	Default recipient scope	Default configuration
Address Lists	This role enables administrators to manage address lists, global address lists, and offline address lists in an organization.	Organization	OrganizationConfig
<input checked="" type="checkbox"/> ApplicationImpersonation	This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.	Organization	None
ArchiveApplication	This role allows partner applications to archive items.	Organization	OrganizationConfig
Audit Logs	This role enables administrators to manage the cmdlet audit logging in an organization.	Organization	OrganizationConfig
Compliance Admin	Lets people view and edit settings and reports for compliance features.	Organization	OrganizationCo

At the bottom of the page, there are three buttons: "Back", "Next" (highlighted with a green box and a mouse cursor), and "Cancel".

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



Exchange admin center

Admin Roles > Add role group

Basics
Permission
Admins
Review and finish

Assign admins

Select the users to assign to this role group. They'll have permissions to manage the roles that you assigned in the previous step.

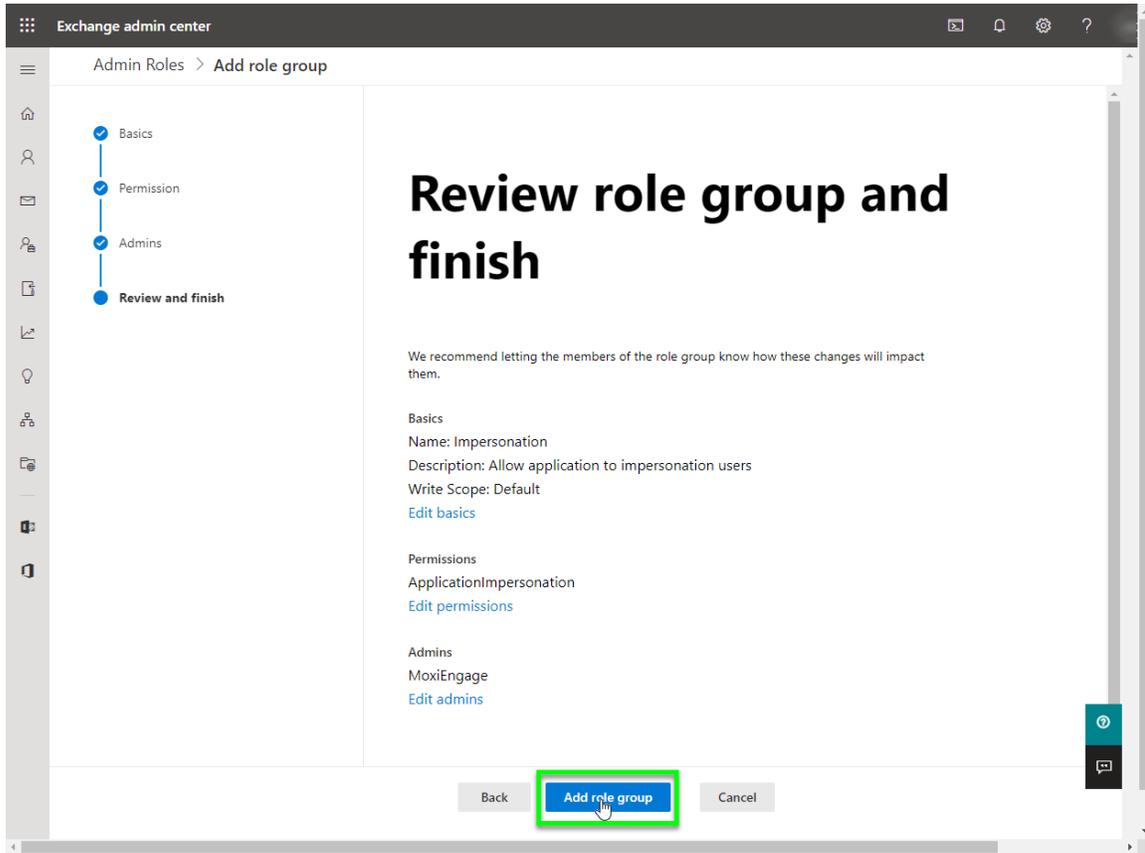
Members

Search by name or email address

ME Moxi Engage X

Back Next Cancel

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



Exchange admin center

Admin Roles > Add role group

Progress bar: Basics (checked), Permission (checked), Admins (checked), Review and finish (active)

Review role group and finish

We recommend letting the members of the role group know how these changes will impact them.

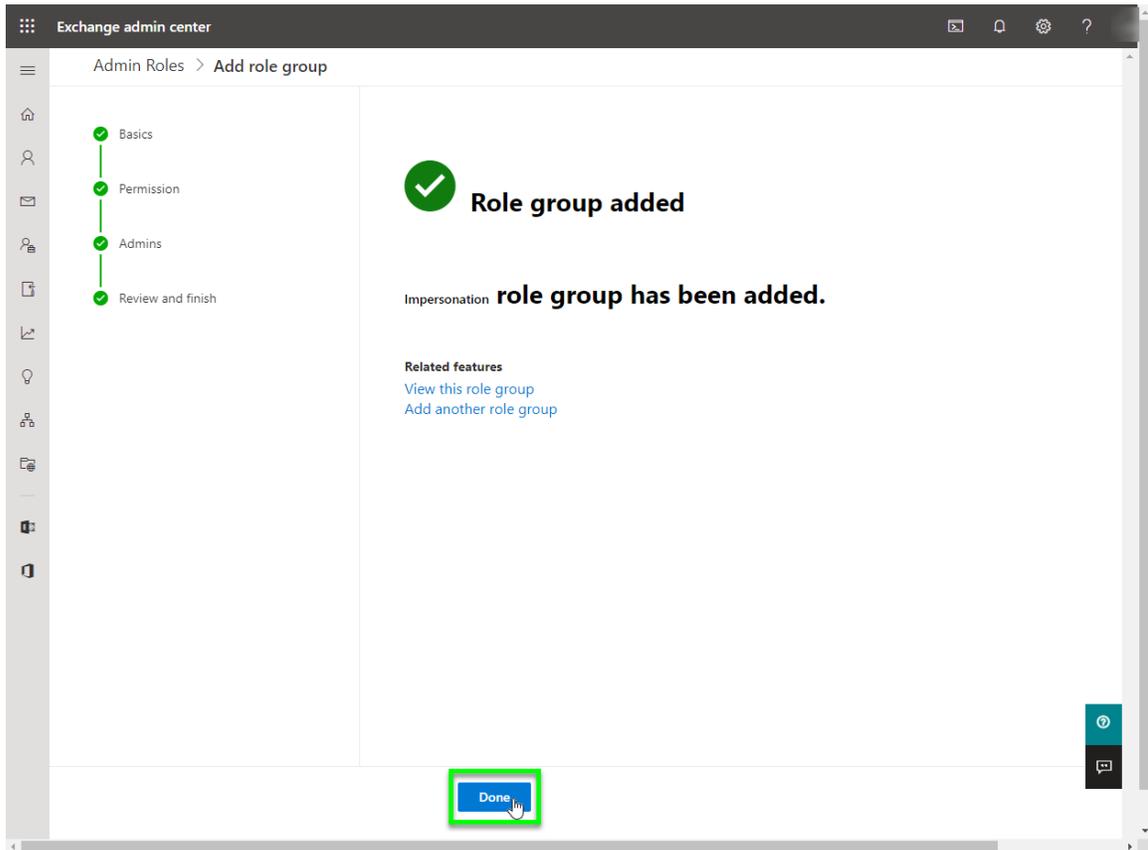
Basics
Name: Impersonation
Description: Allow application to impersonation users
Write Scope: Default
[Edit basics](#)

Permissions
ApplicationImpersonation
[Edit permissions](#)

Admins
MoxiEngage
[Edit admins](#)

Buttons: Back, **Add role group**, Cancel

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



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.



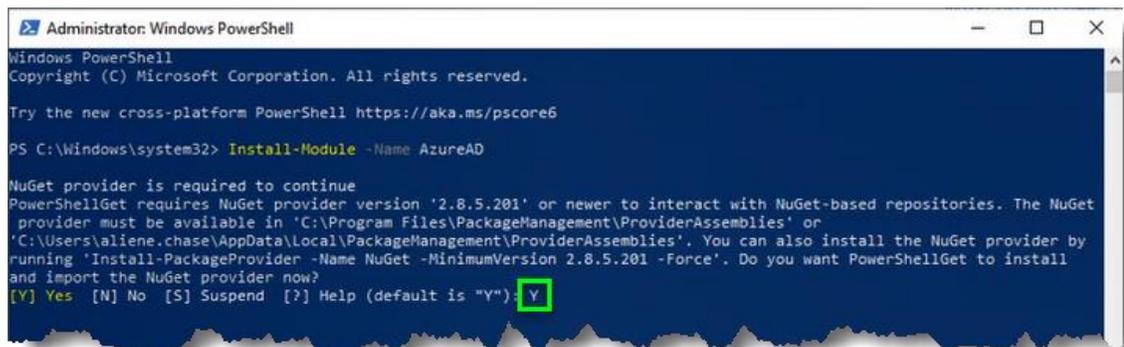
Note

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

3. Type

```
Y
```

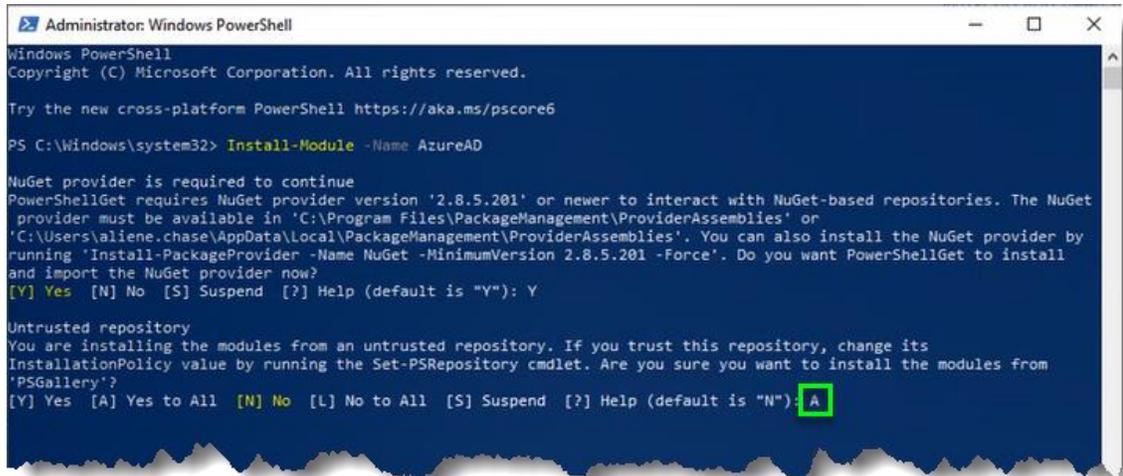
and press Enter on your keyboard to accept installation of the NuGet provider.



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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

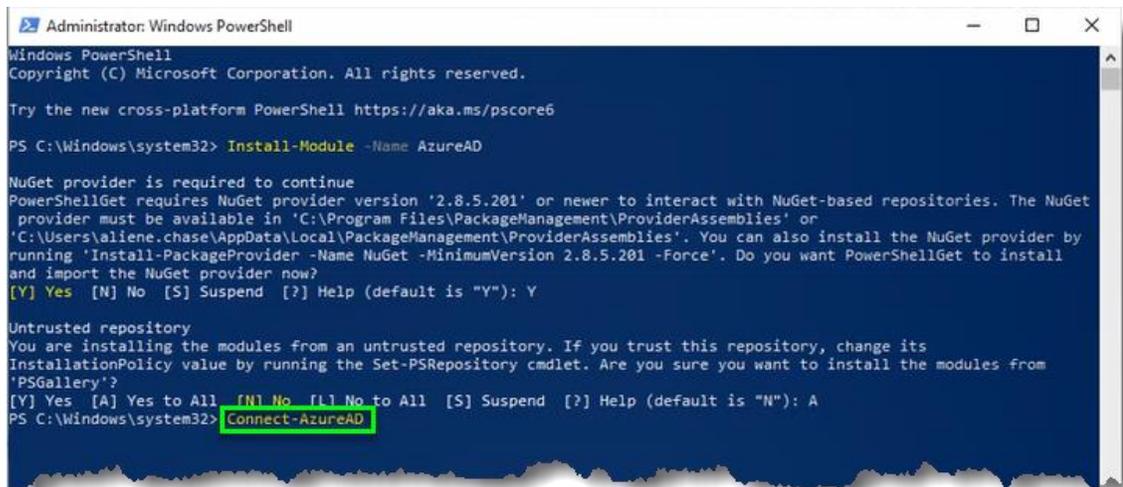
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\aliene.chase\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
```

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

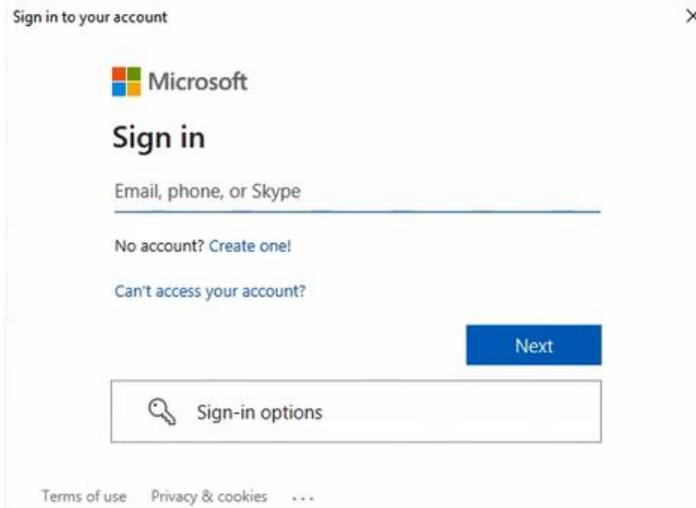
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name AzureAD

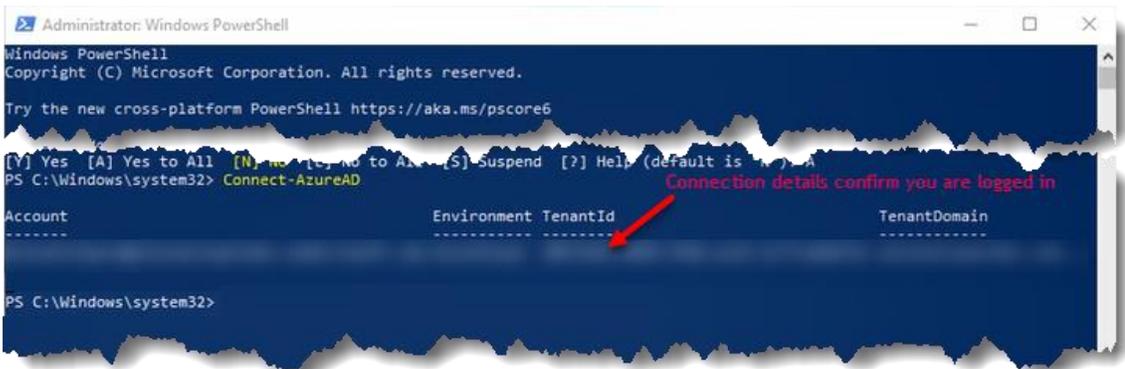
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\aliene.chase\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Windows\system32> Connect-AzureAD
```

- 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).



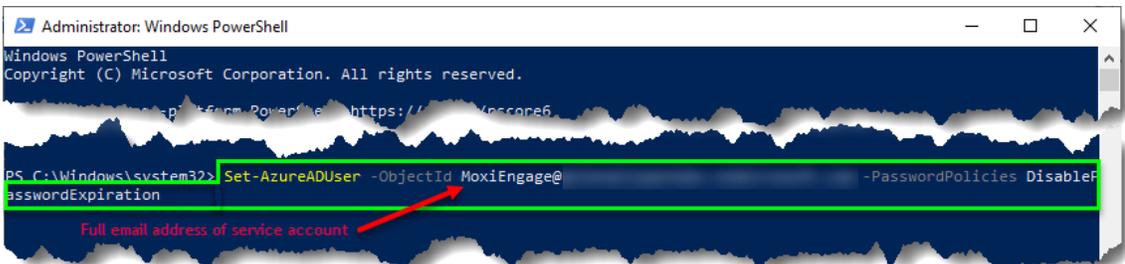
- When you have logged in successfully, connection information including your login account, environment, and domain will be displayed.



- At the prompt, type

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

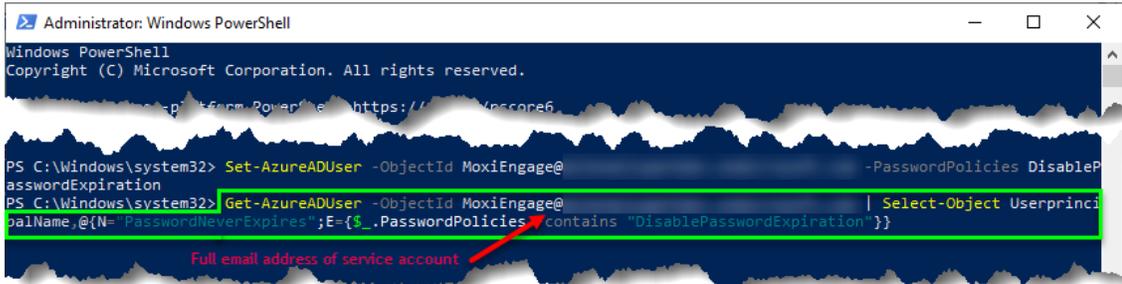
replacing "{email address}" with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard.



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

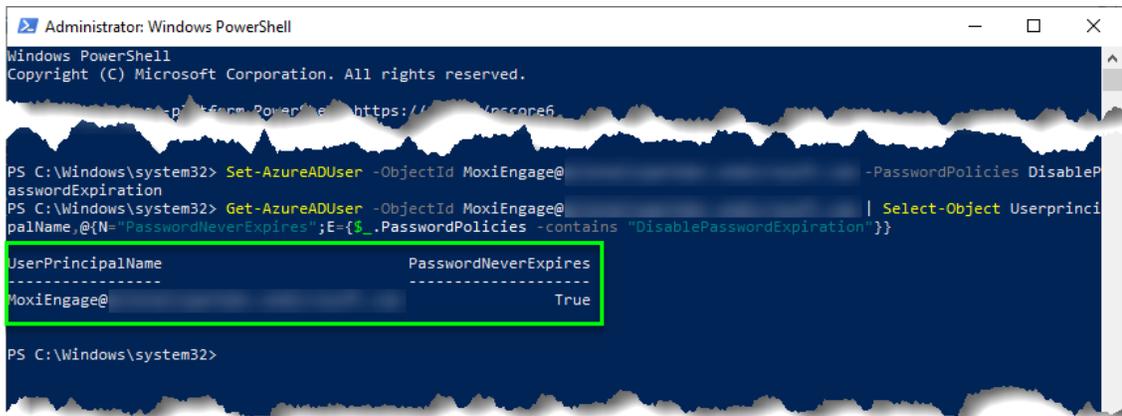
```
Get-AzureADUser -ObjectId {email address} | Select-Object  
UserPrincipalName,@{N="PasswordNeverExpires";E={$_.Password  
Policies -contains "DisablePasswordExpiration"}}
```

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



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The prompt is "PS C:\Windows\system32>". The command entered is `Get-AzureADUser -ObjectId MoxiEngage@ | Select-Object UserPrincipalName,@{N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}}`. A red arrow points to the email address placeholder in the command, with the text "Full email address of service account" written below it.

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



The screenshot shows the same Windows PowerShell terminal window. The command from the previous step has been executed, and the output is displayed in a table format. The output is highlighted with a green box.

UserPrincipalName	PasswordNeverExpires
MoxiEngage@	True

Test Service Account Impersonation for MoxiEngage

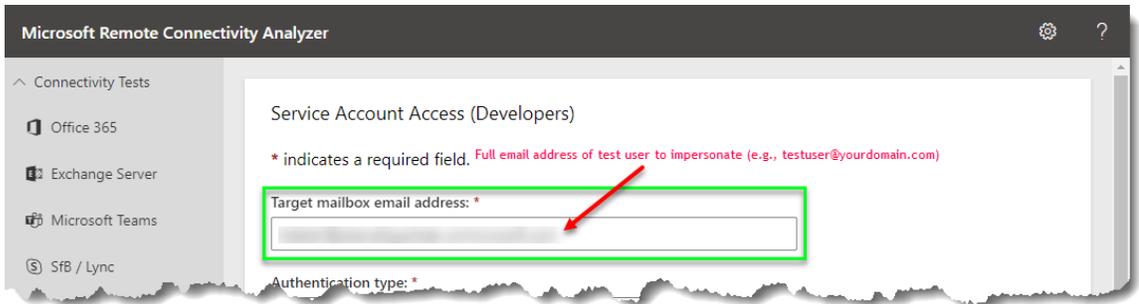
It is best practice to test the impersonation role of your MoxiEngage service account before you provide the service account credentials to MoxiWorks. This will prevent delays in your onboarding process. If the impersonation testing fails, additional configuration steps may be required.

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](#).



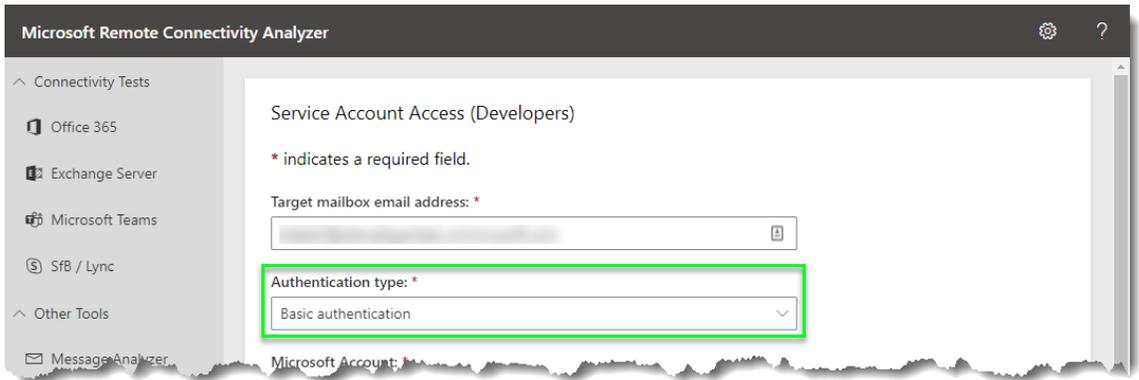
The screenshot shows the Microsoft Remote Connectivity Analyzer interface. The left sidebar lists 'Connectivity Tests' with options for Office 365, Exchange Server, Microsoft Teams, and SfB / Lync. The main content area is titled 'Service Account Access (Developers)'. It includes a note: '* indicates a required field.' Below this, there is a text input field labeled 'Target mailbox email address: *' which is currently empty. Below that is a dropdown menu labeled 'Authentication type: *'.

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



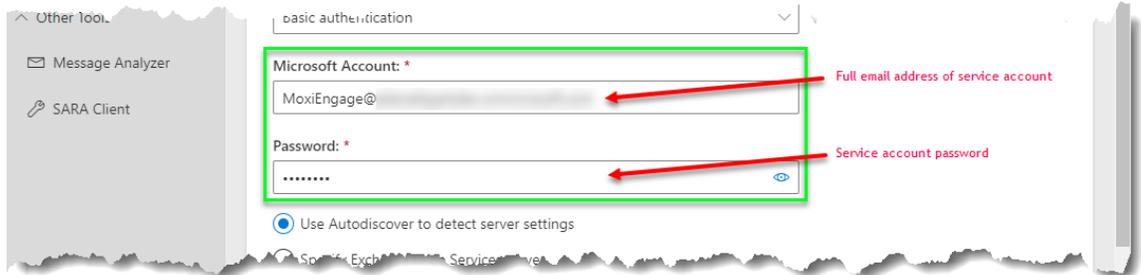
This screenshot is similar to the previous one, but the 'Target mailbox email address: *' field is now highlighted with a green border. A red arrow points to the field. A red note above the field reads: 'Full email address of test user to impersonate (e.g., testuser@yourdomain.com)'. The 'Authentication type: *' dropdown is also visible below.

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



This screenshot shows the 'Authentication type: *' dropdown menu highlighted with a green border. The dropdown is open, and 'Basic authentication' is selected. The 'Target mailbox email address: *' field is still highlighted with a green border. The 'Microsoft Account: *' field is partially visible at the bottom.

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.



Other tools

- Message Analyzer
- SARA Client

basic authentication

Microsoft Account: *

MoxiEngage@

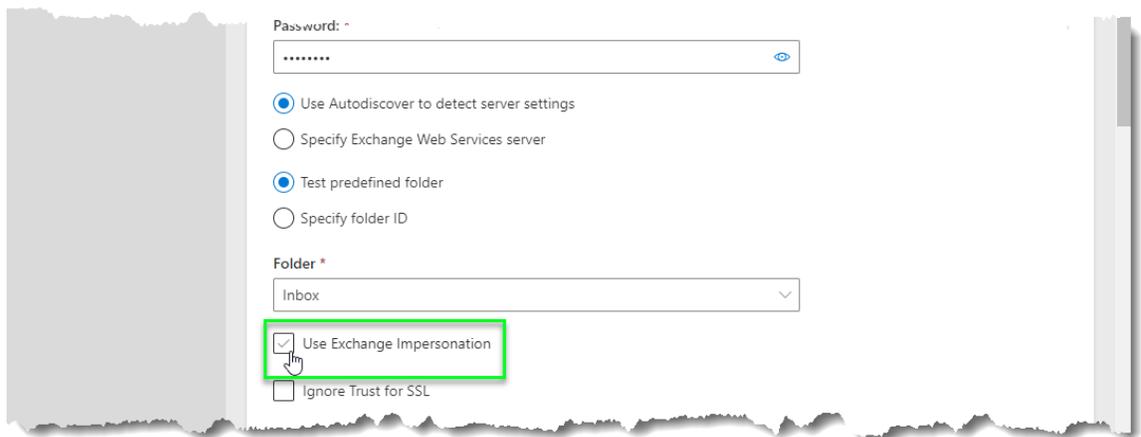
Password: *

.....

Use Autodiscover to detect server settings

Specify Exchange Web Services server

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



Password: *

.....

Use Autodiscover to detect server settings

Specify Exchange Web Services server

Test predefined folder

Specify folder ID

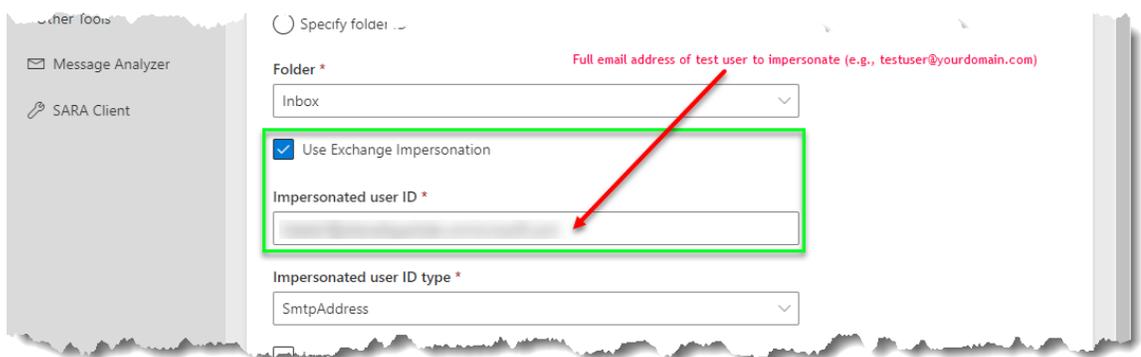
Folder *

Inbox

Use Exchange Impersonation

Ignore Trust for SSL

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.)



Other tools

- Message Analyzer
- SARA Client

Specify folder

Folder *

Inbox

Use Exchange Impersonation

Impersonated user ID *

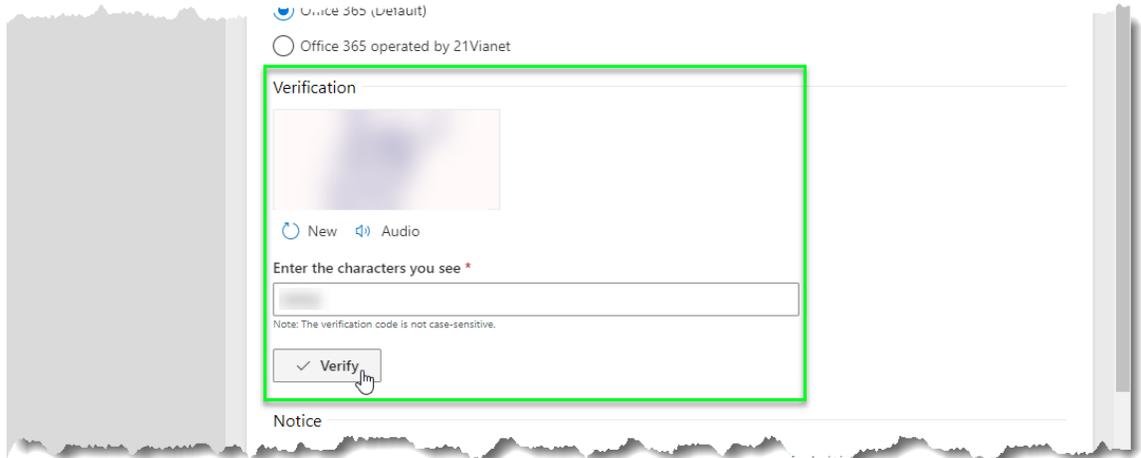
.....

Impersonated user ID type *

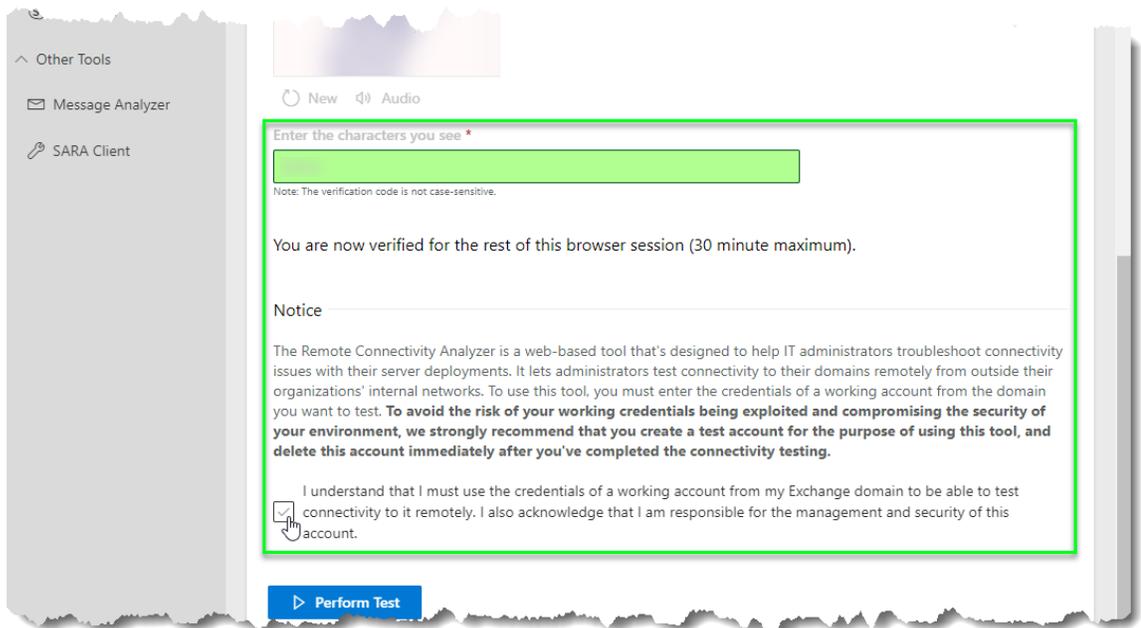
SmtAddress

Full email address of test user to impersonate (e.g., testuser@yourdomain.com)

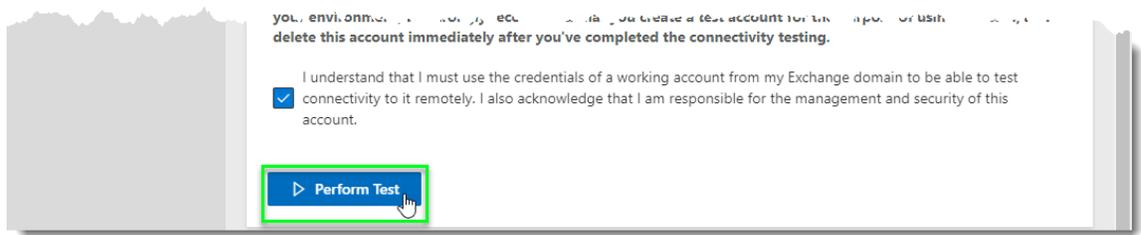
8. Enter the displayed Verification code in the “Enter the characters you see” box of the form, then click on the “Verify” button.



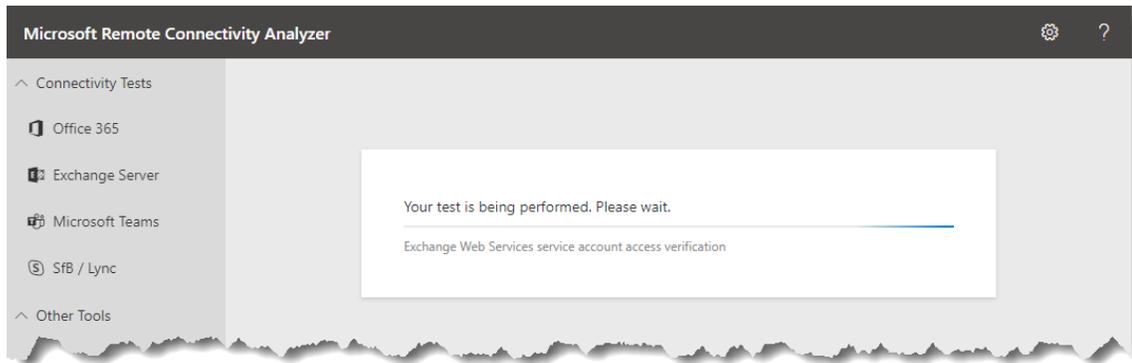
9. Observe that your verification code was accepted for the browser session, then mark the checkbox next to the acknowledgement statement.



10. Click on the “Perform Test” button.

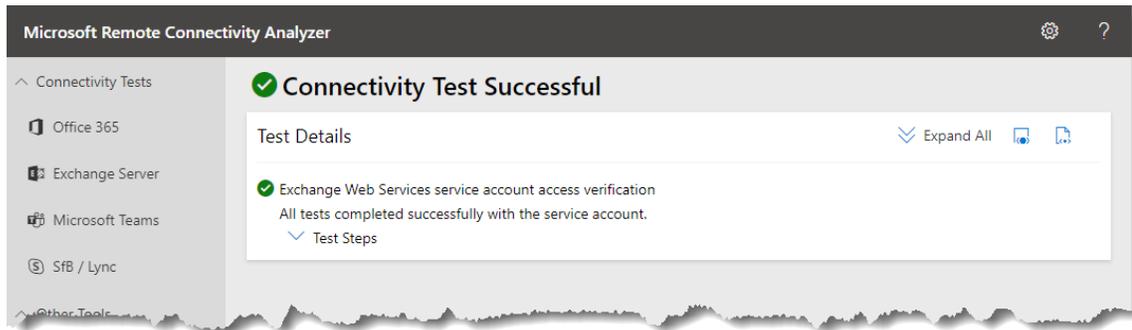


11. Wait while the test is performed.

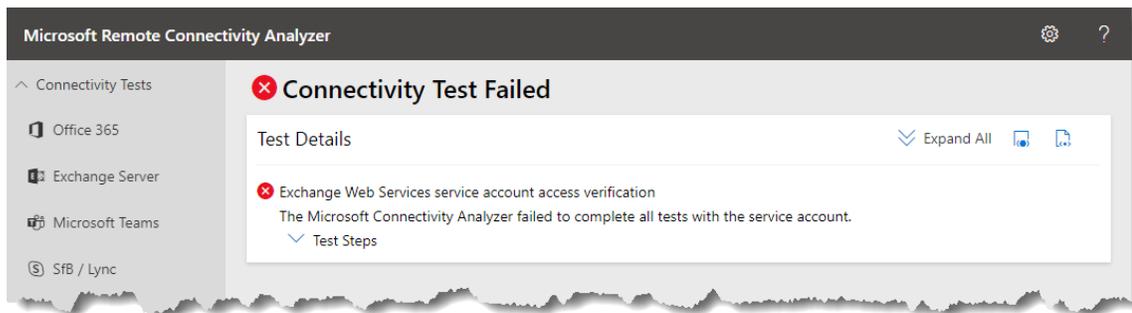


12. Observe the results of the test.

- 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.



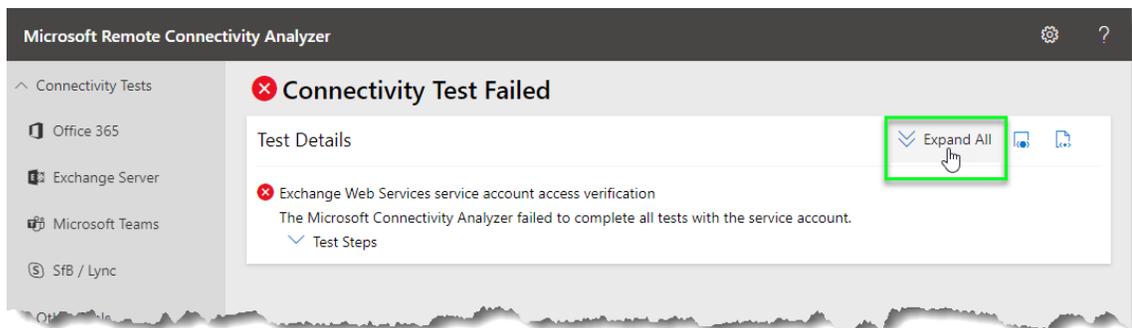
- b. If the test failed, review the error messages. Refer to [Troubleshoot Service Account Impersonation for MoxiEngage](#) in this document for guidance in resolving the most commonly encountered issues.



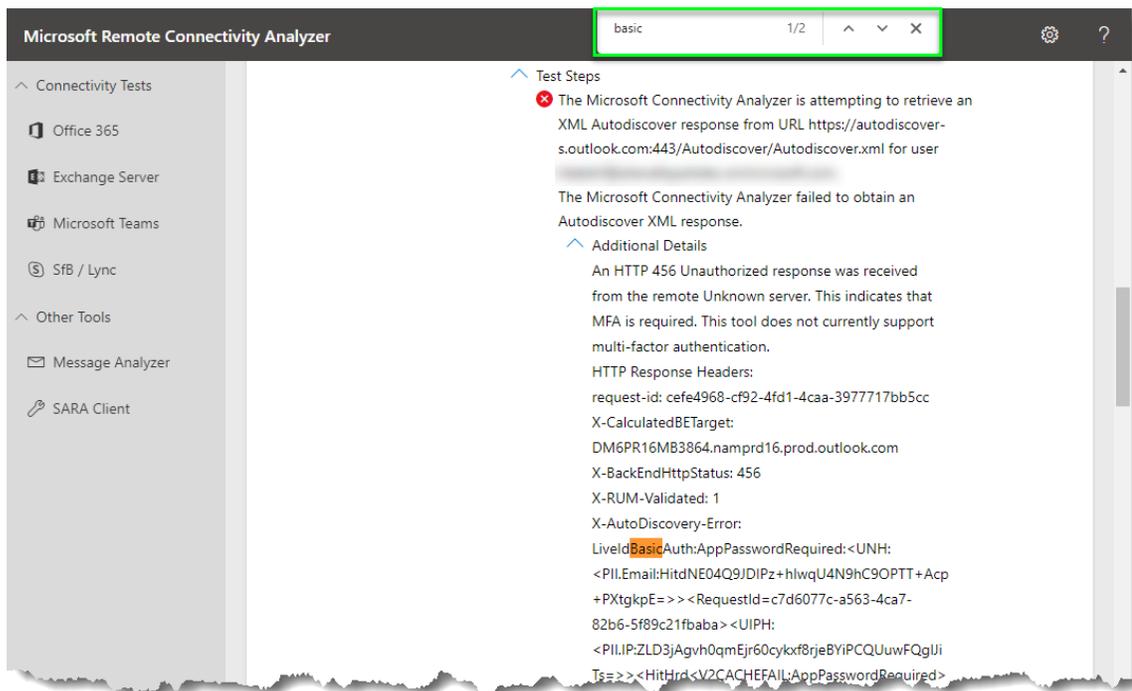
Troubleshoot Service Account Impersonation for MoxiEngage

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](#).

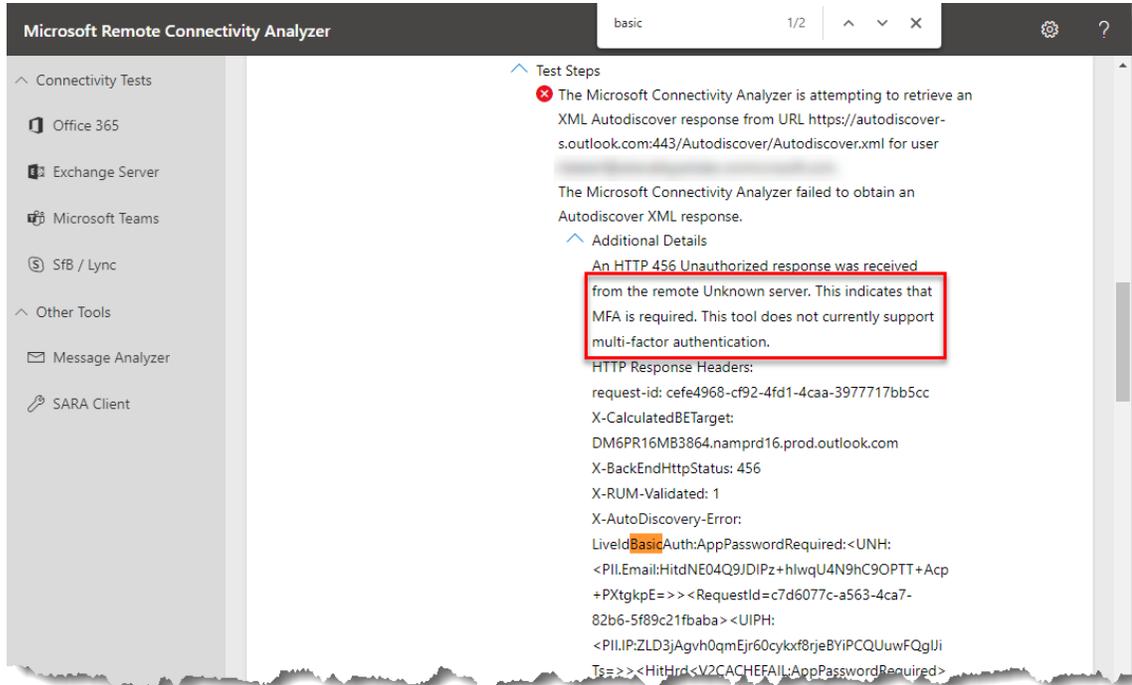
1. Click on the icon next to the “Expand All” label to expand the log messages.



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.



- 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](#).



Microsoft Remote Connectivity Analyzer

basic 1/2

Connectivity Tests

- Office 365
- Exchange Server
- Microsoft Teams
- SfB / Lync
- Other Tools
- Message Analyzer
- SARA Client

Test Steps

The Microsoft Connectivity Analyzer is attempting to retrieve an XML Autodiscover response from URL https://autodiscover.s.outlook.com:443/Autodiscover/Autodiscover.xml for user [redacted]

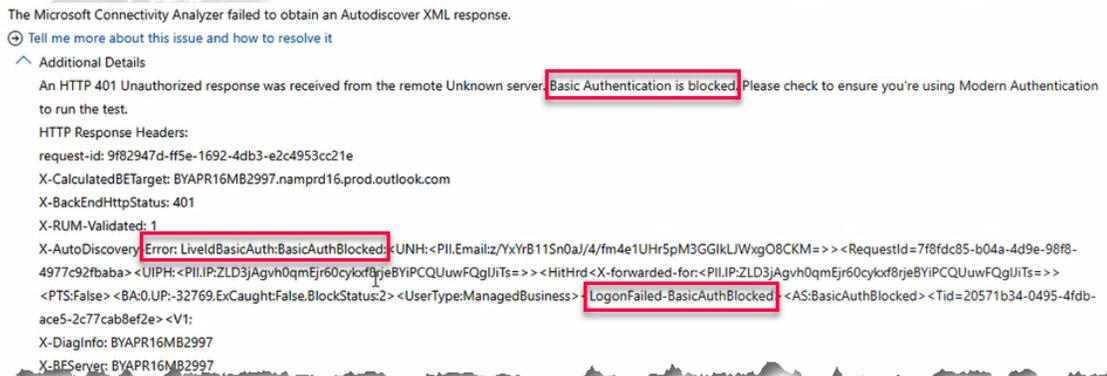
The Microsoft Connectivity Analyzer failed to obtain an Autodiscover XML response.

Additional Details

An HTTP 456 Unauthorized response was received from the remote Unknown server. This indicates that MFA is required. This tool does not currently support multi-factor authentication.

HTTP Response Headers:

```
request-id: cefe4968-cf92-4fd1-4caa-3977717bb5cc
X-CalculatedBETarget: DM6PR16MB3864.namprd16.prod.outlook.com
X-BackEndHttpStatus: 456
X-RUM-Validated: 1
X-AutoDiscovery-Error: LiveIdBasicAuth:AppPasswordRequired:<UNH:
<PIL.Email:HitdNE04Q9JDIPz+hlwqU4N9hC9OPTT+Acp
+PXtgpE=>><RequestId=c7d6077c-a563-4ca7-82b6-5f89c21fbaba><UIPH:
<PIL.IP:ZLD3jAgvh0qmEjr60cykxf8rjeBYiPCQUuWFQgUjI
Ts=>><HitHrd<V2CACHEFAIL:AppPasswordRequired>
```



The Microsoft Connectivity Analyzer failed to obtain an Autodiscover XML response.

[Tell me more about this issue and how to resolve it](#)

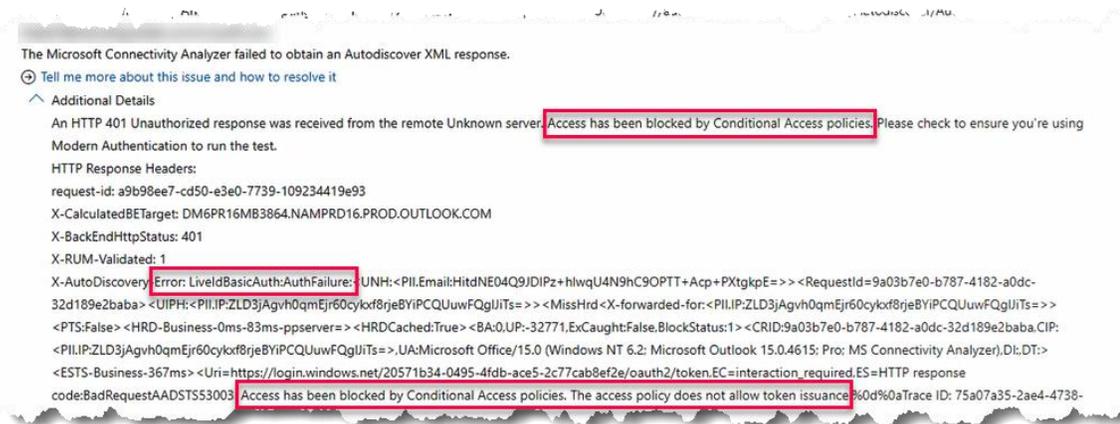
Additional Details

An HTTP 401 Unauthorized response was received from the remote Unknown server. Basic Authentication is blocked. Please check to ensure you're using Modern Authentication to run the test.

HTTP Response Headers:

```
request-id: 9f82947d-ff5e-1692-4db3-e2c4953cc21e
X-CalculatedBETarget: BYAPR16MB2997.namprd16.prod.outlook.com
X-BackEndHttpStatus: 401
X-RUM-Validated: 1
X-AutoDiscovery-Error: LiveIdBasicAuth:BasicAuthBlocked:<UNH:<PIL.Email:YxyfB115n0aj/4/fm4e1UHR5pM3GGikLJWxgO8CKM=>><RequestId=7f8fdc85-b04a-4d9e-98f8-4977c92fbaba><UIPH:<PIL.IP:ZLD3jAgvh0qmEjr60cykxf8rjeBYiPCQUuWFQgUjI
Ts=>><HitHrd<X-forwarded-for:<PIL.IP:ZLD3jAgvh0qmEjr60cykxf8rjeBYiPCQUuWFQgUjI
Ts=>><PTS:False><BA:0,UP:-32769.ExCaught:False.BlockStatus:2><UserType:ManagedBusiness><LogonFailed-BasicAuthBlocked><AS:BasicAuthBlocked><Tid=20571b34-0495-4fdb-ace5-2c77cab8ef2e><V1:
X-DiagInfo: BYAPR16MB2997
X-BEServer: BYAPR16MB2997
```

- 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.

- 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.

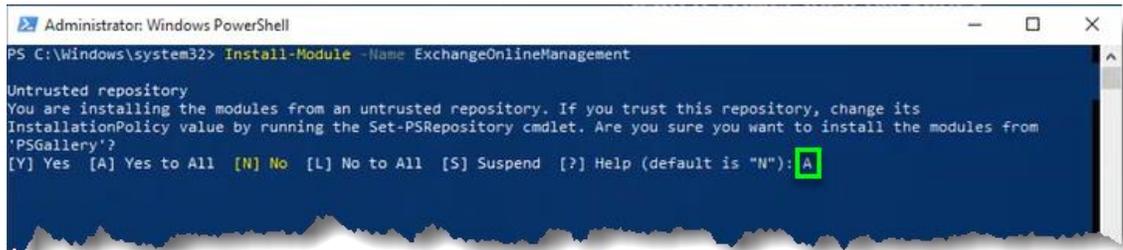
- At the PowerShell prompt, type `Install-Module -Name ExchangeOnlineManagement` and press Enter on your keyboard.



- 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.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Install-Module -Name ExchangeOnlineManagement

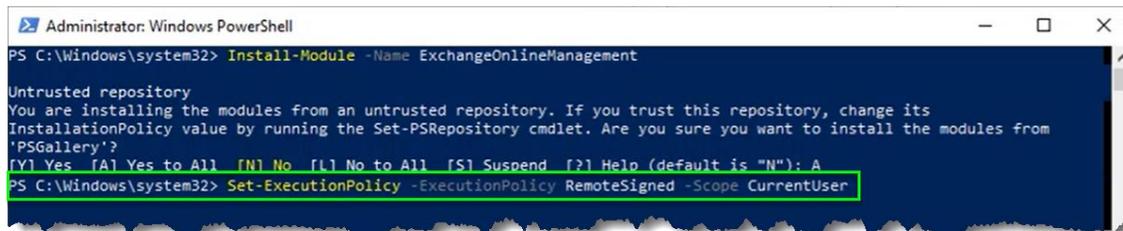
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
```

- Wait for the prompt. It may take a moment to complete the installation.

- Type

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope
CurrentUser
```

and press Enter on your keyboard.



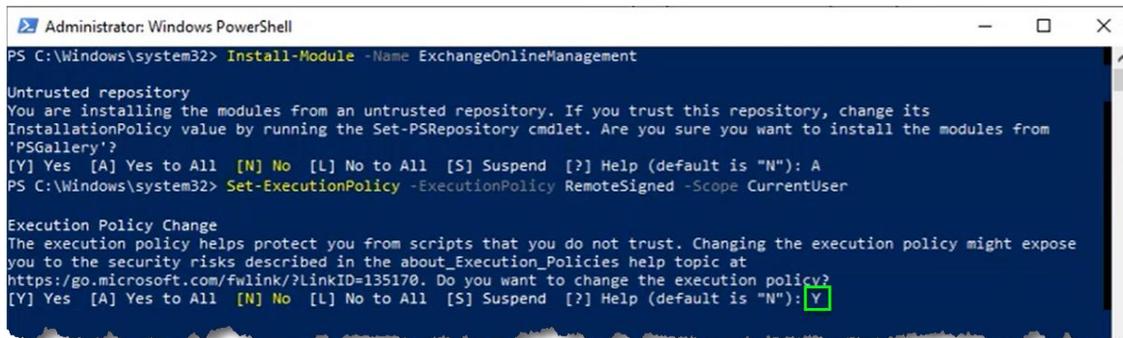
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Install-Module -Name ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

- Confirm the change to your PowerShell execution policy. Type

Y

and press Enter on your keyboard.



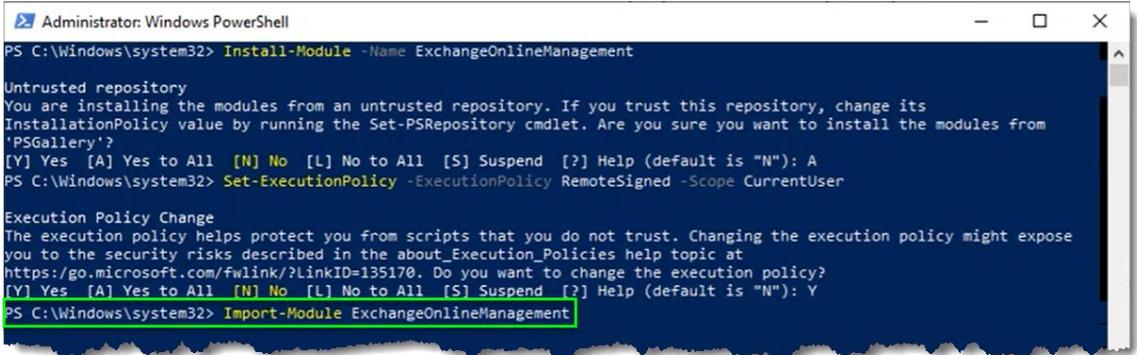
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Install-Module -Name ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
```

7. Type

`Import-Module ExchangeOnlineManagement`
and press Enter on your keyboard.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Install-Module -Name ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?linkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Windows\system32> Import-Module ExchangeOnlineManagement
```

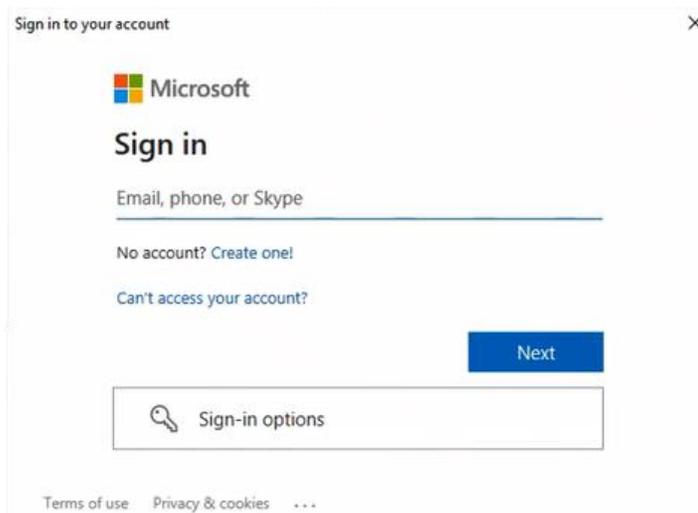
8. Type

`Connect-ExchangeOnline`
and press Enter on your keyboard.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Connect-ExchangeOnline
```

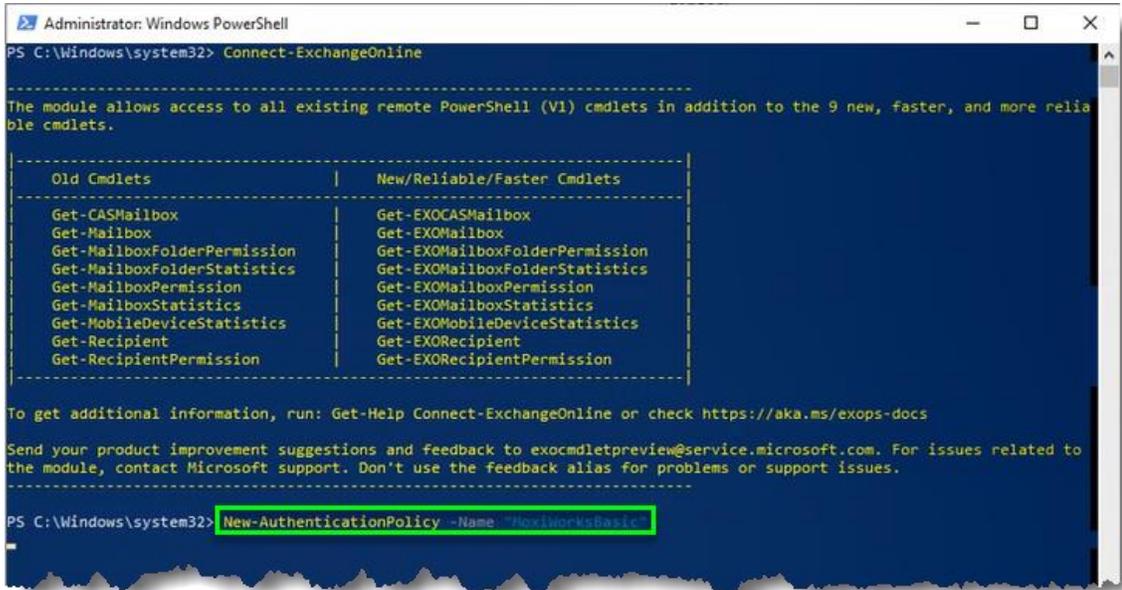
9. Follow the on-screen instructions to log into your Microsoft 365 account using a login with administrative rights. The login screen that may appear as a pop-up over your PowerShell window supports multi-factor authentication (MFA).



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

11. Type

`New-AuthenticationPolicy -Name "MoxiWorksBasic"`
and press Enter on your keyboard.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Connect-ExchangeOnline

-----
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more reliable cmdlets.

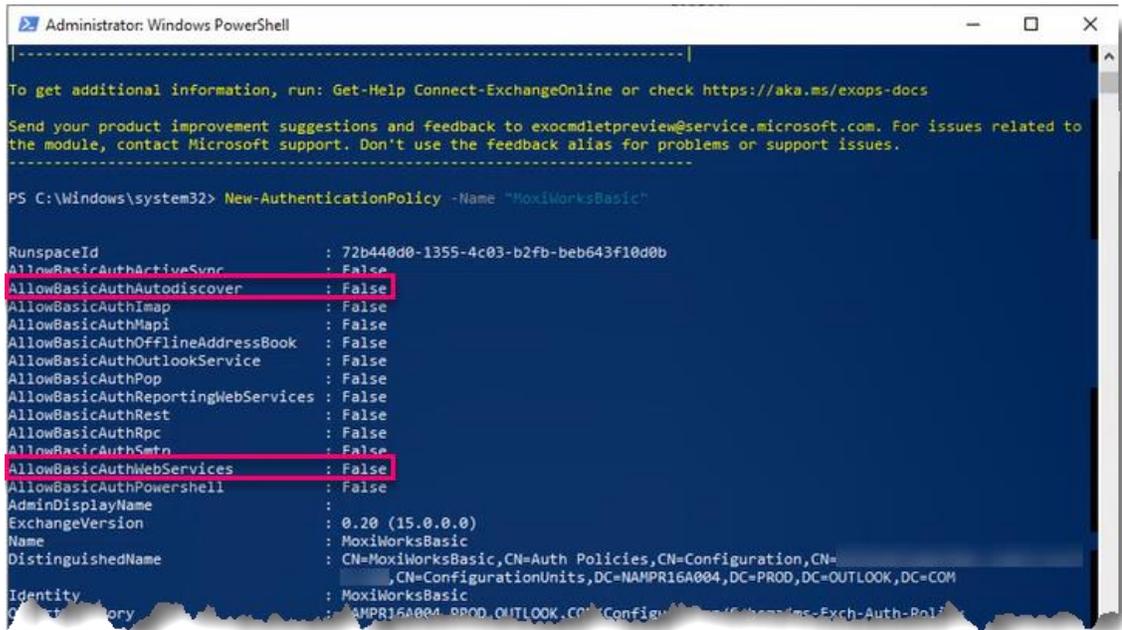
-----
| Old Cmdlets | New/Reliable/Faster Cmdlets |
-----|-----|
| Get-CASMailbox | Get-EXOCASMailbox |
| Get-Mailbox | Get-EXOMailbox |
| Get-MailboxFolderPermission | Get-EXOMailboxFolderPermission |
| Get-MailboxFolderStatistics | Get-EXOMailboxFolderStatistics |
| Get-MailboxPermission | Get-EXOMailboxPermission |
| Get-MailboxStatistics | Get-EXOMailboxStatistics |
| Get-MobileDeviceStatistics | Get-EXOMobileDeviceStatistics |
| Get-Recipient | Get-EXORecipient |
| Get-RecipientPermission | Get-EXORecipientPermission |
-----

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.

-----
PS C:\Windows\system32> New-AuthenticationPolicy -Name "MoxiWorksBasic"
```

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.



```
Administrator: Windows PowerShell

-----
To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.

-----
PS C:\Windows\system32> New-AuthenticationPolicy -Name "MoxiWorksBasic"

RunspaceId : 72b440d0-1355-4c03-b2fb-beb643f10d0b
AllowBasicAuthActiveSync : False
AllowBasicAuthAutoDiscover : False
AllowBasicAuthImap : False
AllowBasicAuthMapi : False
AllowBasicAuthOfflineAddressBook : False
AllowBasicAuthOutlookService : False
AllowBasicAuthPop : False
AllowBasicAuthReportingWebServices : False
AllowBasicAuthRest : False
AllowBasicAuthRpc : False
AllowBasicAuthSetn : False
AllowBasicAuthWebServices : False
AllowBasicAuthPowerShell : False
AdminDisplayName :
ExchangeVersion : 0.20 (15.0.0.0)
Name : MoxiWorksBasic
DistinguishedName : CN=MoxiWorksBasic,CN=Auth Policies,CN=Configuration,CN=
                        ,CN=ConfigurationUnits,DC=NAMEPR16A004,DC=PROD,DC=OUTLOOK,DC=COM
Identity : MoxiWorksBasic
Category : NAMEPR16A004-PROD.OUTLOOK.COM\Configuration\Groups\ms-Exch-Auth-Poli
```

13. Type

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

and press Enter on your keyboard.

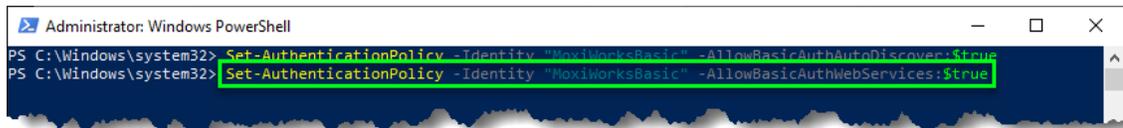


```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthAutoDiscover:$true
```

14. Type

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

and press Enter on your keyboard.

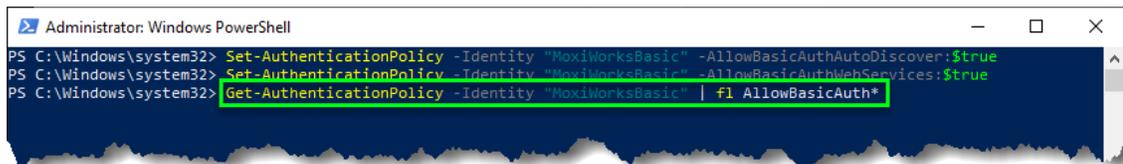


```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthAutoDiscover:$true  
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthWebServices:$true
```

15. To verify the settings, type

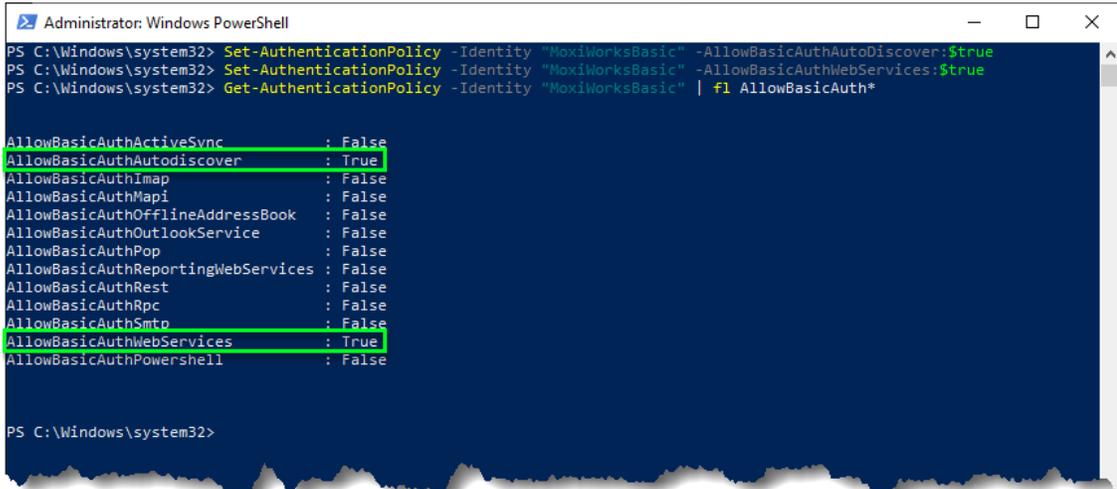
```
Get-AuthenticationPolicy -Identity "MoxiWorksBasic" | fl  
AllowBasicAuth*
```

and press Enter on your keyboard.



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthAutoDiscover:$true  
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthWebServices:$true  
PS C:\Windows\system32> Get-AuthenticationPolicy -Identity "MoxiWorksBasic" | fl AllowBasicAuth*
```

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



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthAutoDiscover:$true
PS C:\Windows\system32> Set-AuthenticationPolicy -Identity "MoxiWorksBasic" -AllowBasicAuthWebServices:$true
PS C:\Windows\system32> Get-AuthenticationPolicy -Identity "MoxiWorksBasic" | fl AllowBasicAuth*

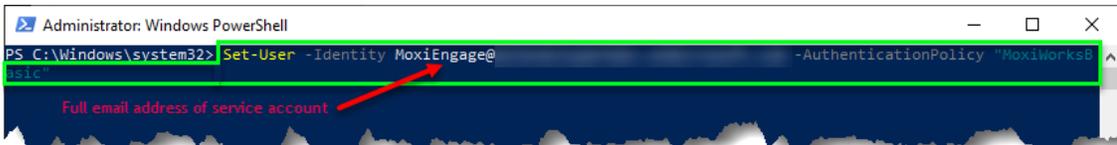
AllowBasicAuthActiveSync           : False
AllowBasicAuthAutodiscover          : True
AllowBasicAuthImap                  : False
AllowBasicAuthMapi                  : False
AllowBasicAuthOfflineAddressBook   : False
AllowBasicAuthOutlookService        : False
AllowBasicAuthPop                   : False
AllowBasicAuthReportingWebServices  : False
AllowBasicAuthRest                  : False
AllowBasicAuthRpc                   : False
AllowBasicAuthSmtpt                 : False
AllowBasicAuthWebServices           : True
AllowBasicAuthPowerShell            : False

PS C:\Windows\system32>
```

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.



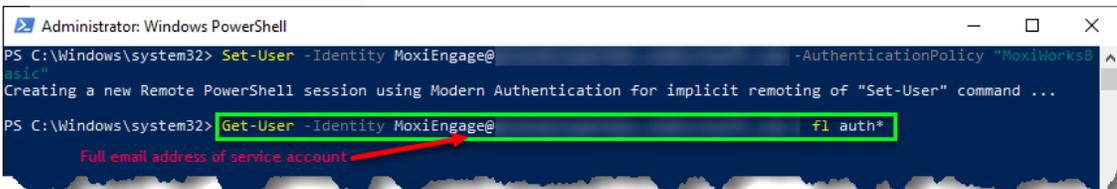
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-User -Identity MoxiEngage@ -AuthenticationPolicy "MoxiWorksBasic"
Full email address of service account
```

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

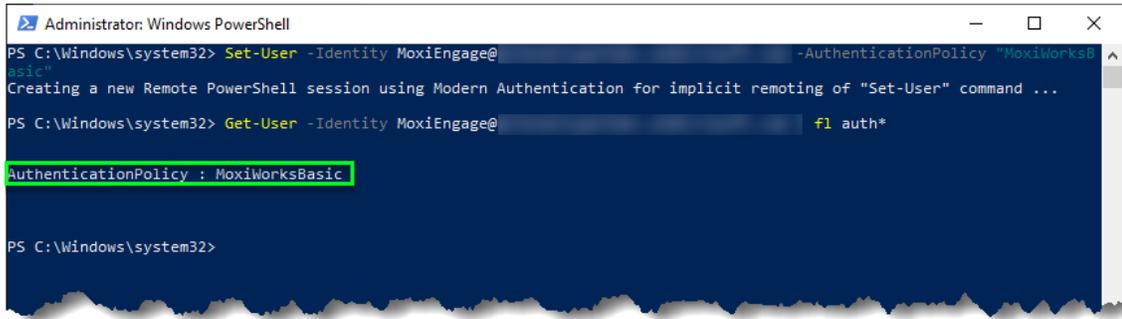
```
Get-User -Identity {email address} | fl auth*
```

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.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-User -Identity MoxiEngage@ -AuthenticationPolicy "MoxiWorksBasic"
Creating a new Remote PowerShell session using Modern Authentication for implicit remoting of "Set-User" command ...
PS C:\Windows\system32> Get-User -Identity MoxiEngage@ | fl auth*
Full email address of service account
```

20. Observe the response indicating the applied authentication policy.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-User -Identity MoxiEngage@ -AuthenticationPolicy "MoxiWorksBasic"
Creating a new Remote PowerShell session using Modern Authentication for implicit remoting of "Set-User" command ...
PS C:\Windows\system32> Get-User -Identity MoxiEngage@ -fl auth*
AuthenticationPolicy : MoxiWorksBasic
PS C:\Windows\system32>
```

21. Return to [Test Service Account Impersonation for MoxiEngage](#) to verify that impersonation using the service account is successful.

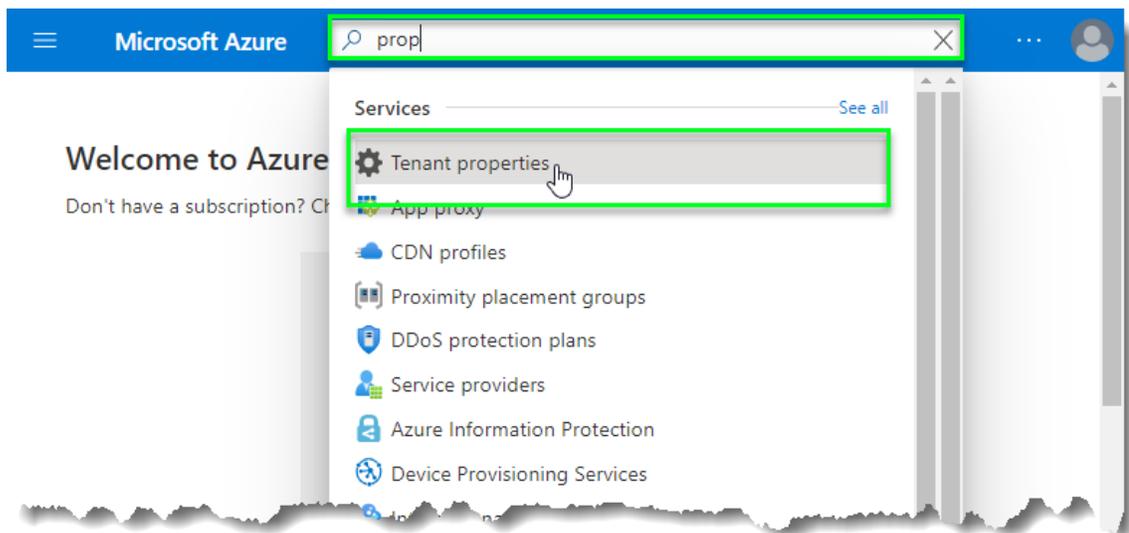
Adjust Conditional Access Policy for Service Account

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.

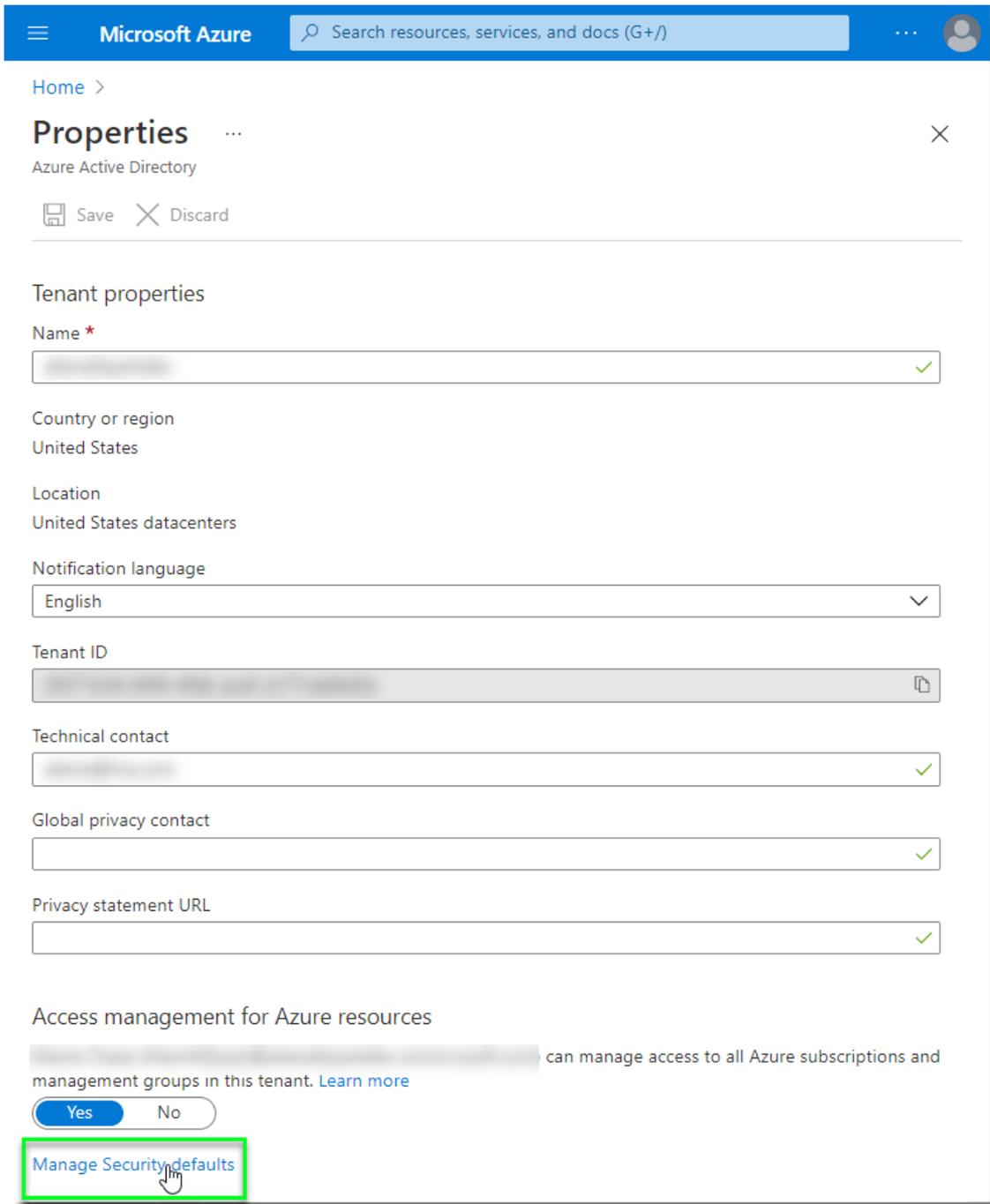
The instructions provided here will assist you in disabling the "Security Defaults" Conditional Access Policy and creating a new Conditional Access Policy that requires multi-factor authentication (MFA) for all users except the MoxiEngage service account. Any additional security considerations and/or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



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



Microsoft Azure Search resources, services, and docs (G+)

Home >

Properties

Azure Active Directory

Save Discard

Tenant properties

Name *

Country or region
United States

Location
United States datacenters

Notification language
English

Tenant ID

Technical contact

Global privacy contact

Privacy statement URL

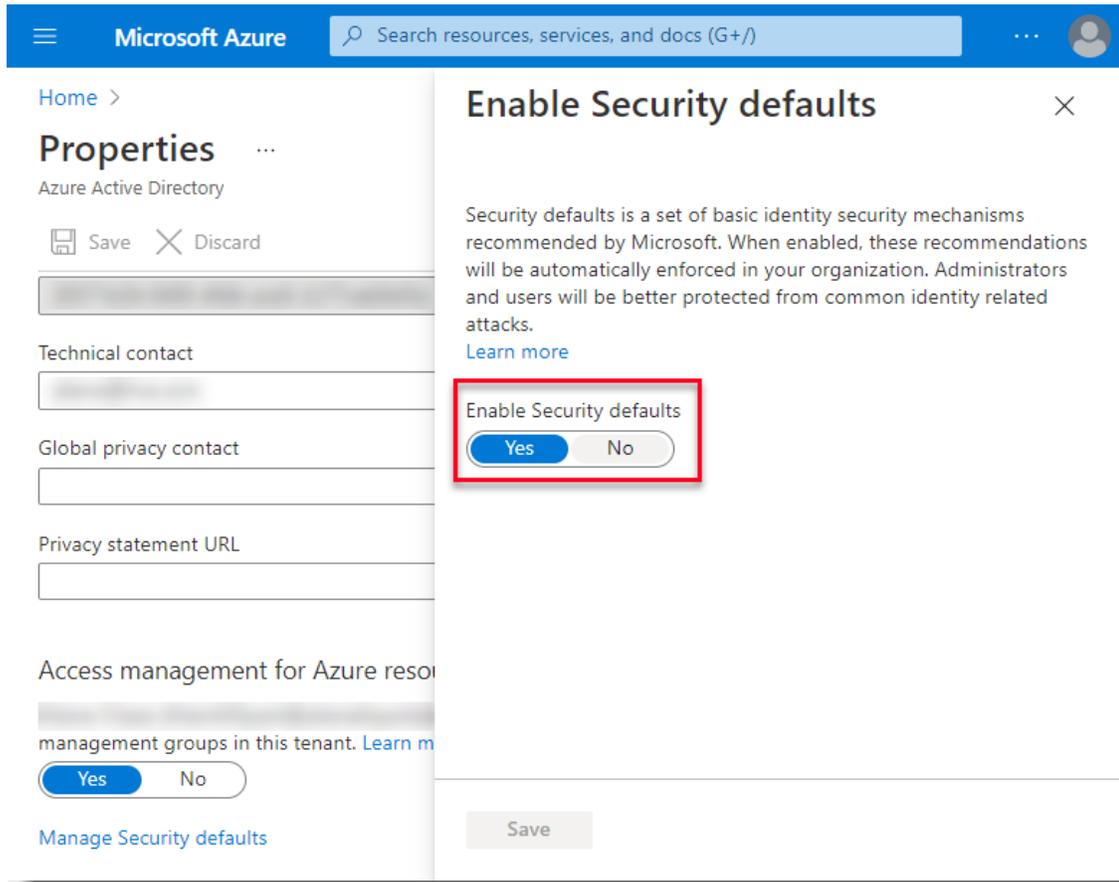
Access management for Azure resources

can manage access to all Azure subscriptions and management groups in this tenant. [Learn more](#)

Yes No

[Manage Security defaults](#)

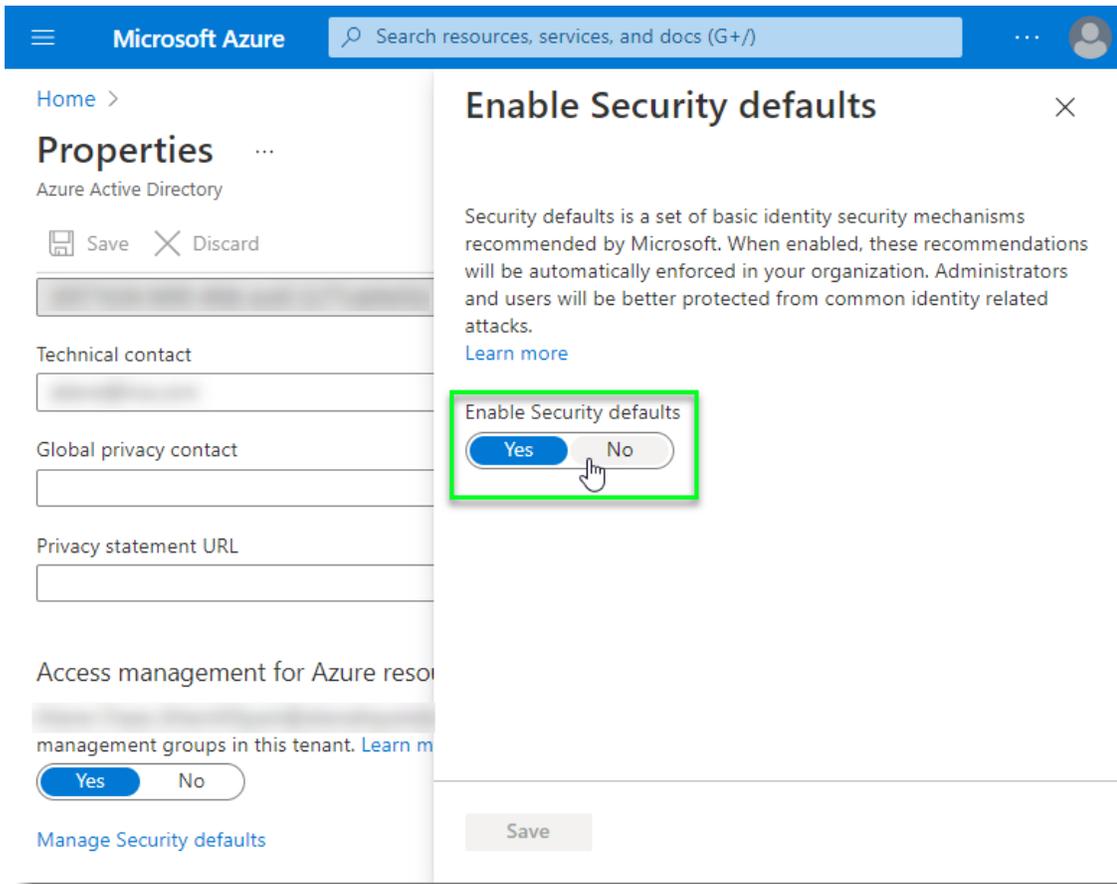
4. Note whether the Security defaults in your Microsoft 365 tenant are enabled, as shown here:



Note

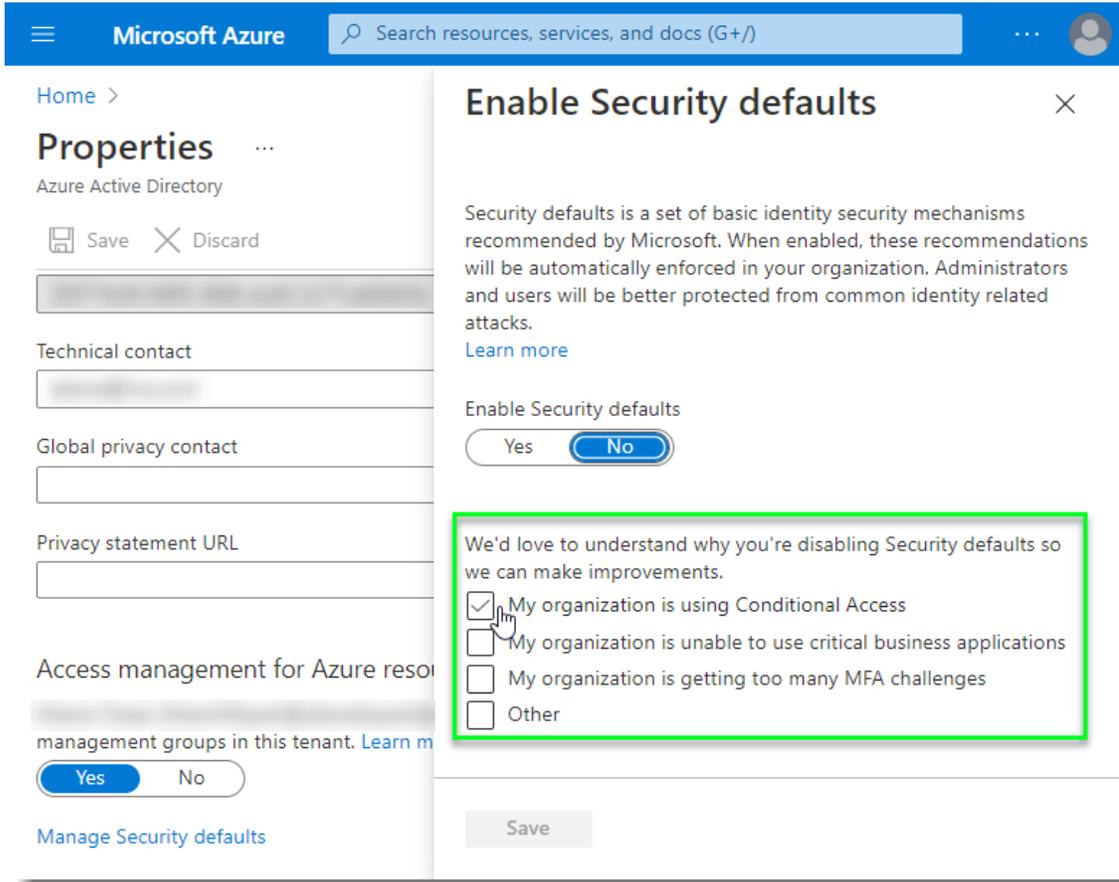
If the Security defaults are not enabled, do not proceed with the following steps.

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



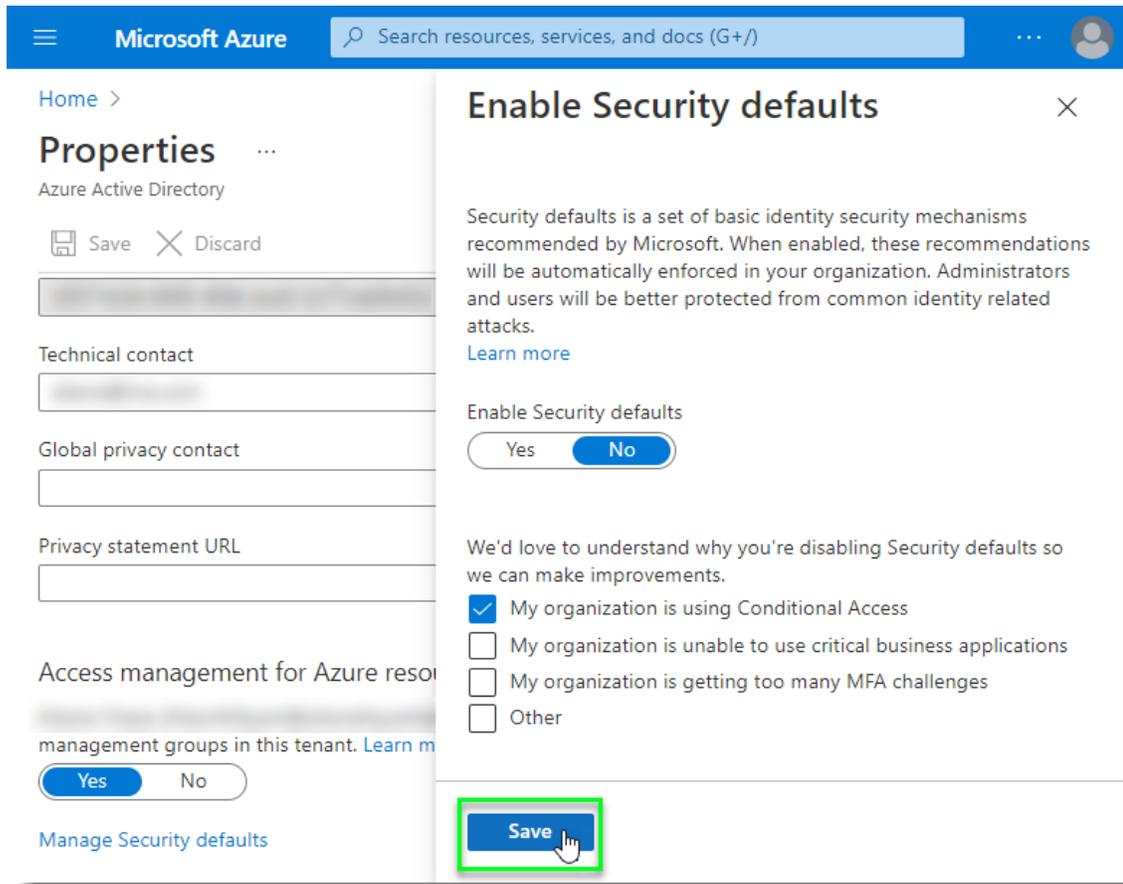
The screenshot shows the Microsoft Azure portal interface. On the left, the 'Properties' section for 'Azure Active Directory' is visible, with fields for 'Technical contact', 'Global privacy contact', and 'Privacy statement URL'. Below this, there is a section for 'Access management for Azure resources' with a 'Yes/No' toggle. The main content area is titled 'Enable Security defaults' and contains a descriptive paragraph about security defaults. Below the text is a 'Yes/No' toggle, which is highlighted with a green box and has a mouse cursor pointing to the 'No' option. A 'Save' button is located at the bottom of the panel.

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

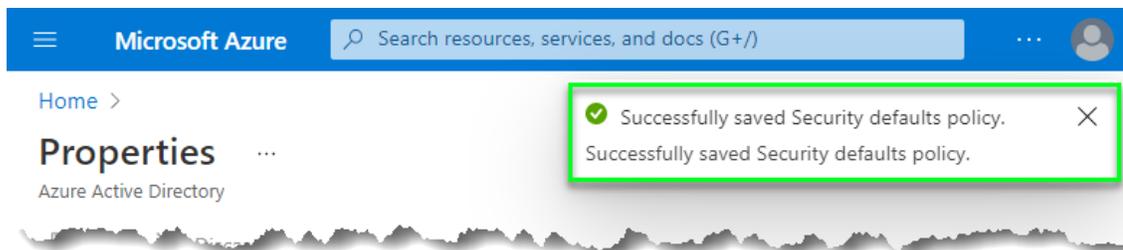


The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with a 'Properties' section for 'Azure Active Directory', including fields for 'Technical contact', 'Global privacy contact', and 'Privacy statement URL'. Below this is an 'Access management for Azure resources' section with 'Yes' and 'No' buttons. The main content area is titled 'Enable Security defaults' and contains a description of security defaults, a 'Learn more' link, and a toggle switch set to 'No'. Below the toggle is a section titled 'We'd love to understand why you're disabling Security defaults so we can make improvements.' with a list of four radio button options: 'My organization is using Conditional Access' (checked), 'My organization is unable to use critical business applications', 'My organization is getting too many MFA challenges', and 'Other'. A green box highlights this list. At the bottom of the dialog is a 'Save' button.

7. Click on the “Save” button.



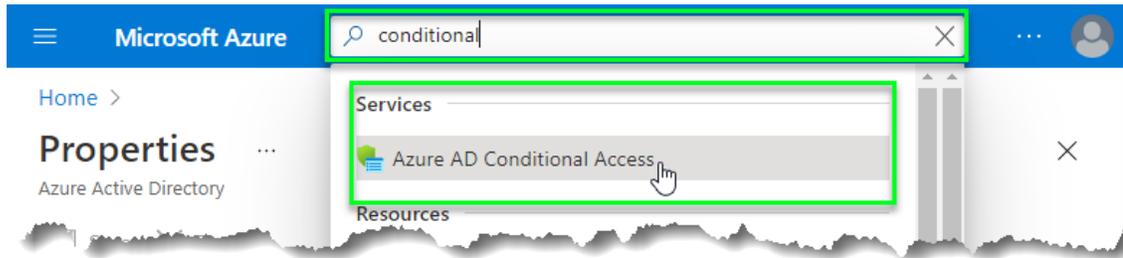
8. Observe the message indicating that your change to the Security defaults policy have been saved.



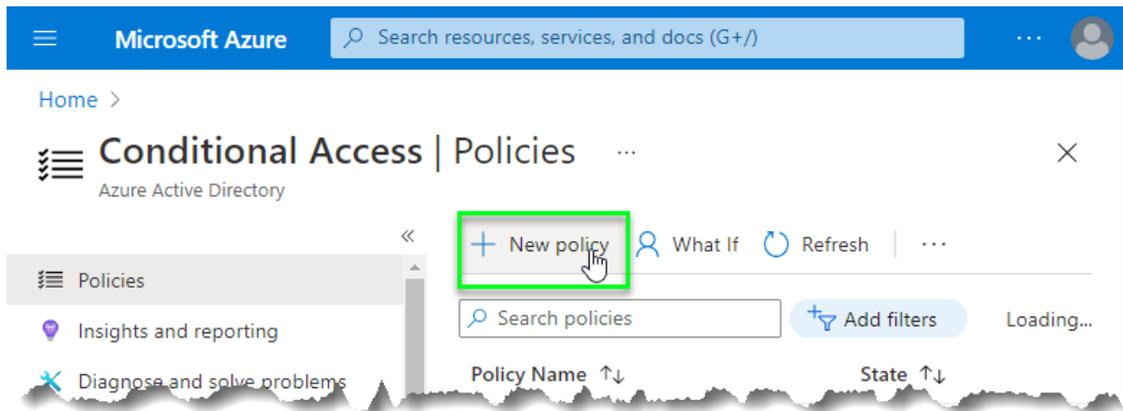
Note

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.

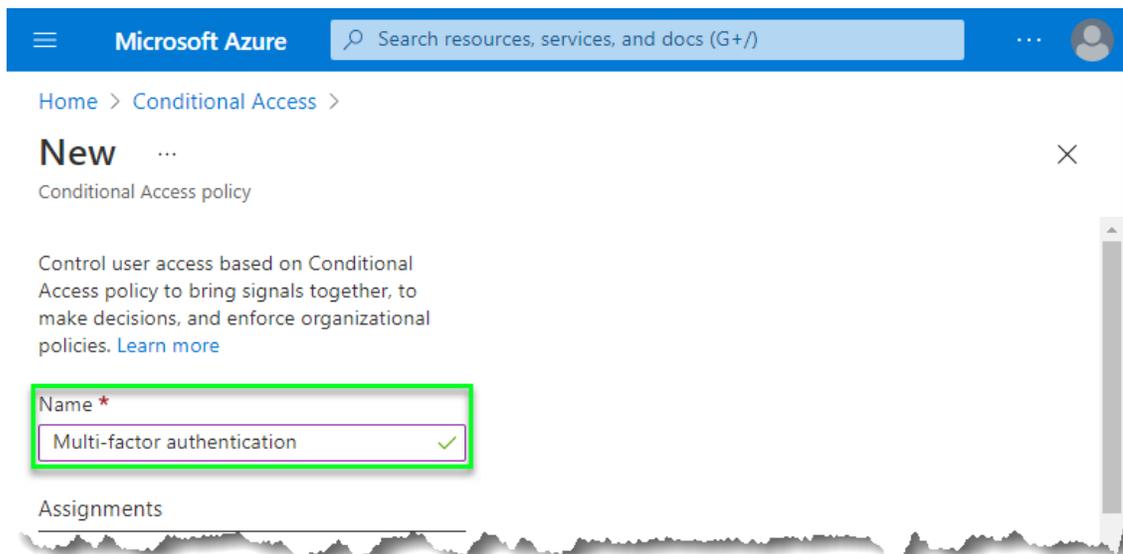
9. Enter “conditional” in the search box, then click on the “Azure AD Conditional Access” option in the resulting list of services.



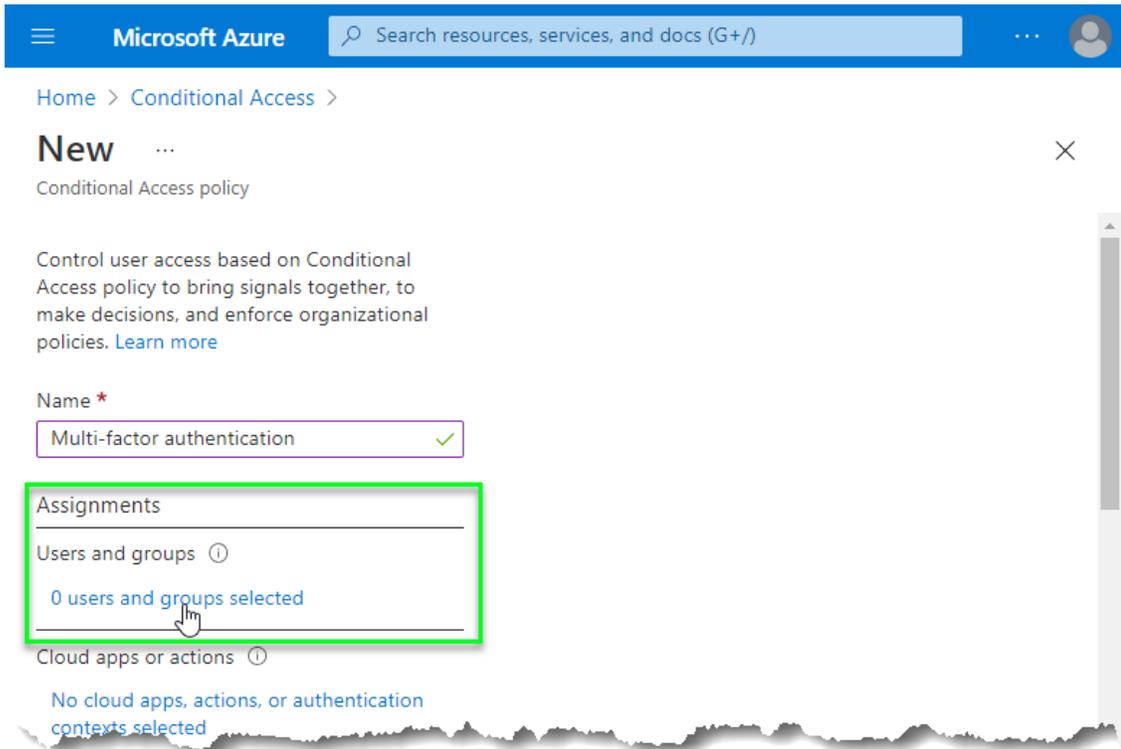
10. Click on the “New policy” button.



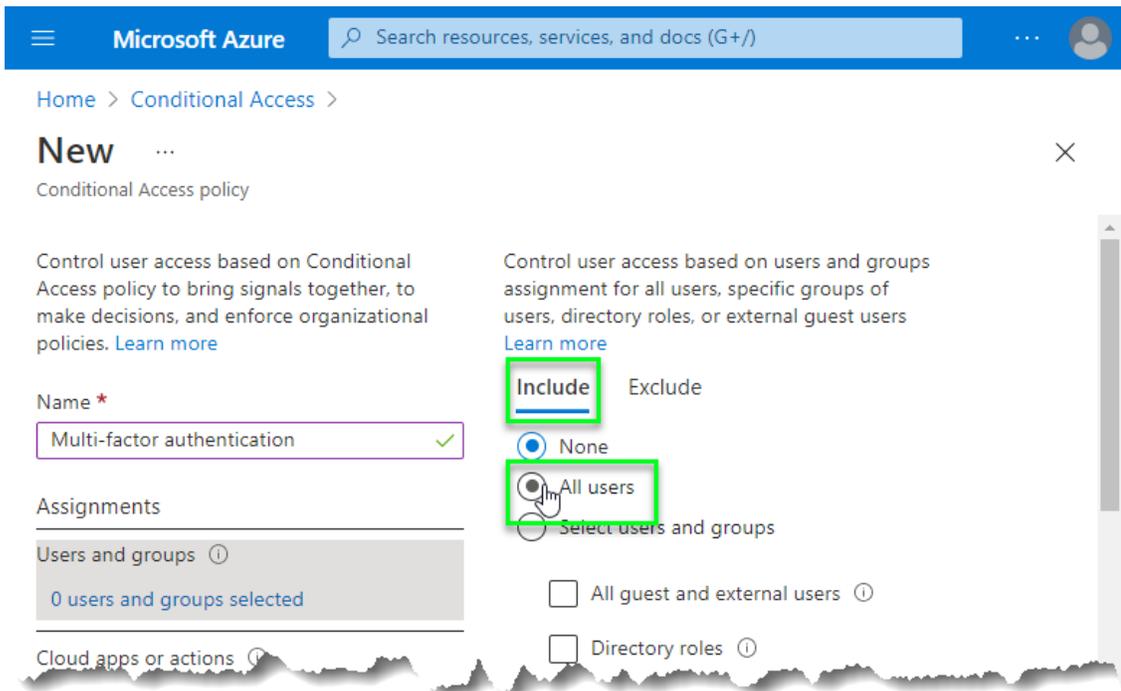
11. Enter a name for your policy in the “Name” box (e.g., “Multi-factor authentication”).



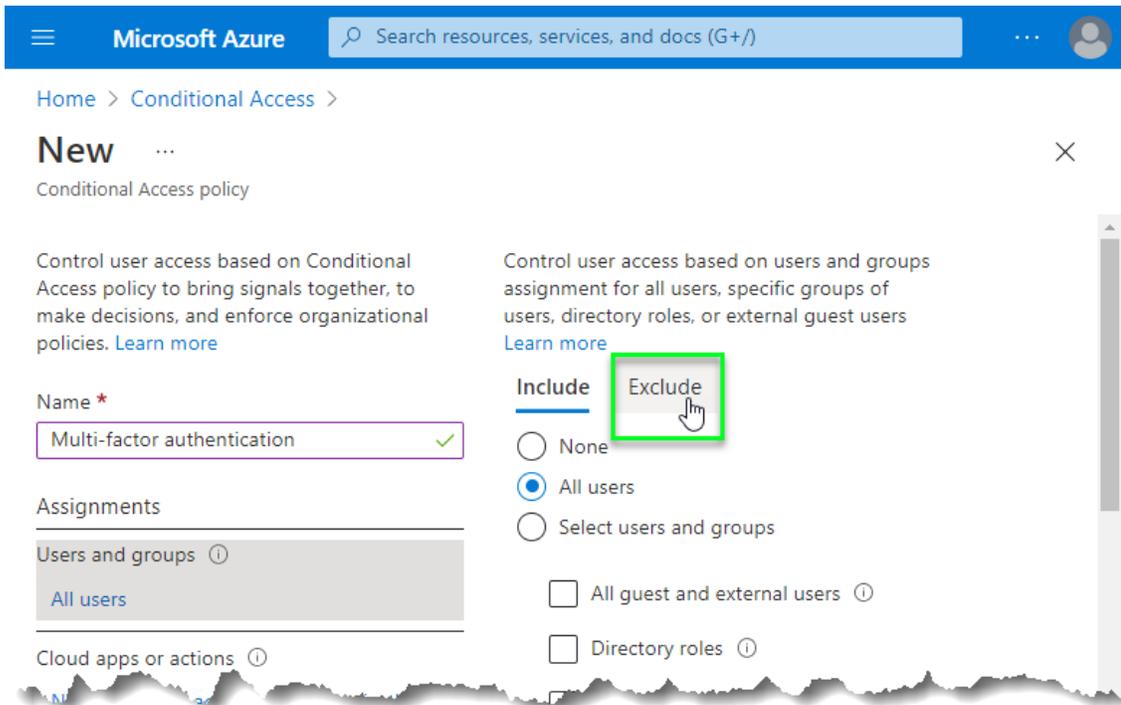
12. Click on the “0 users and groups selected” link in the “Assignments: Users and Groups” section.



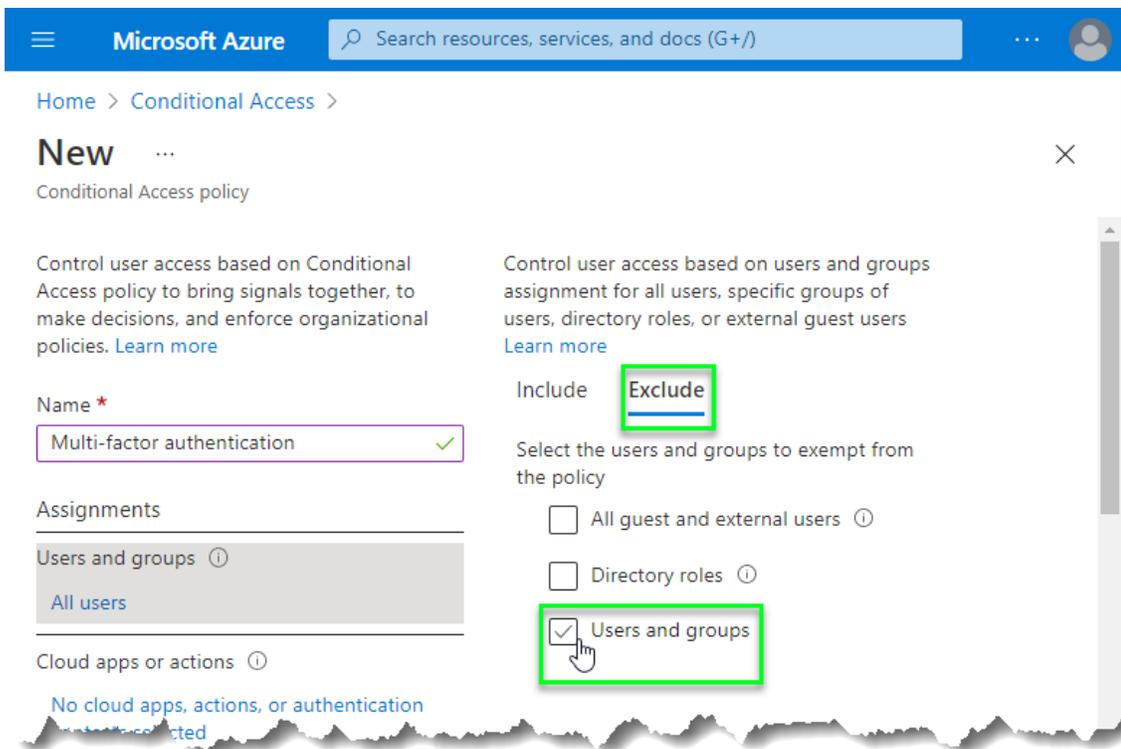
13. Ensure the “Include” tab of the overlay form is selected, then click on the radio button next to the “All users” label.



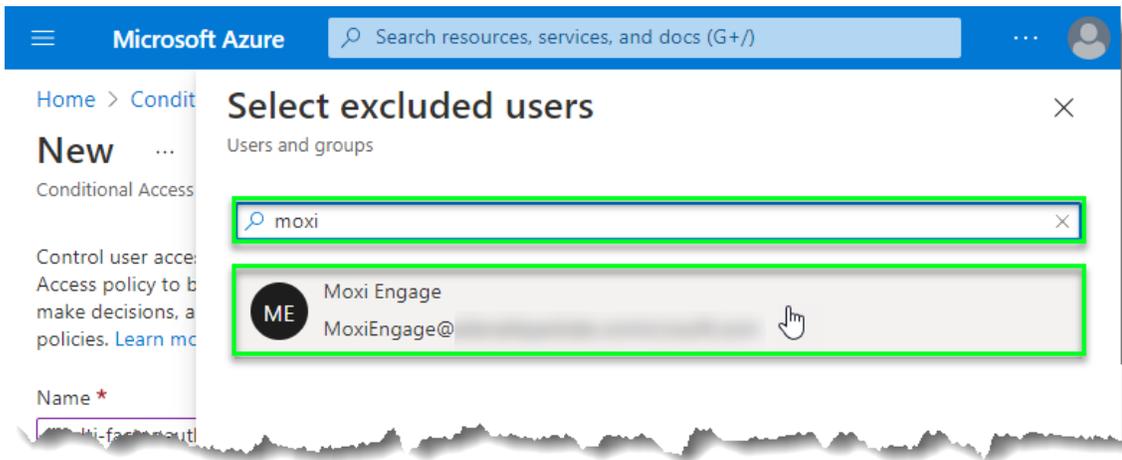
14. Click on the “Exclude” tab of the overlay form.



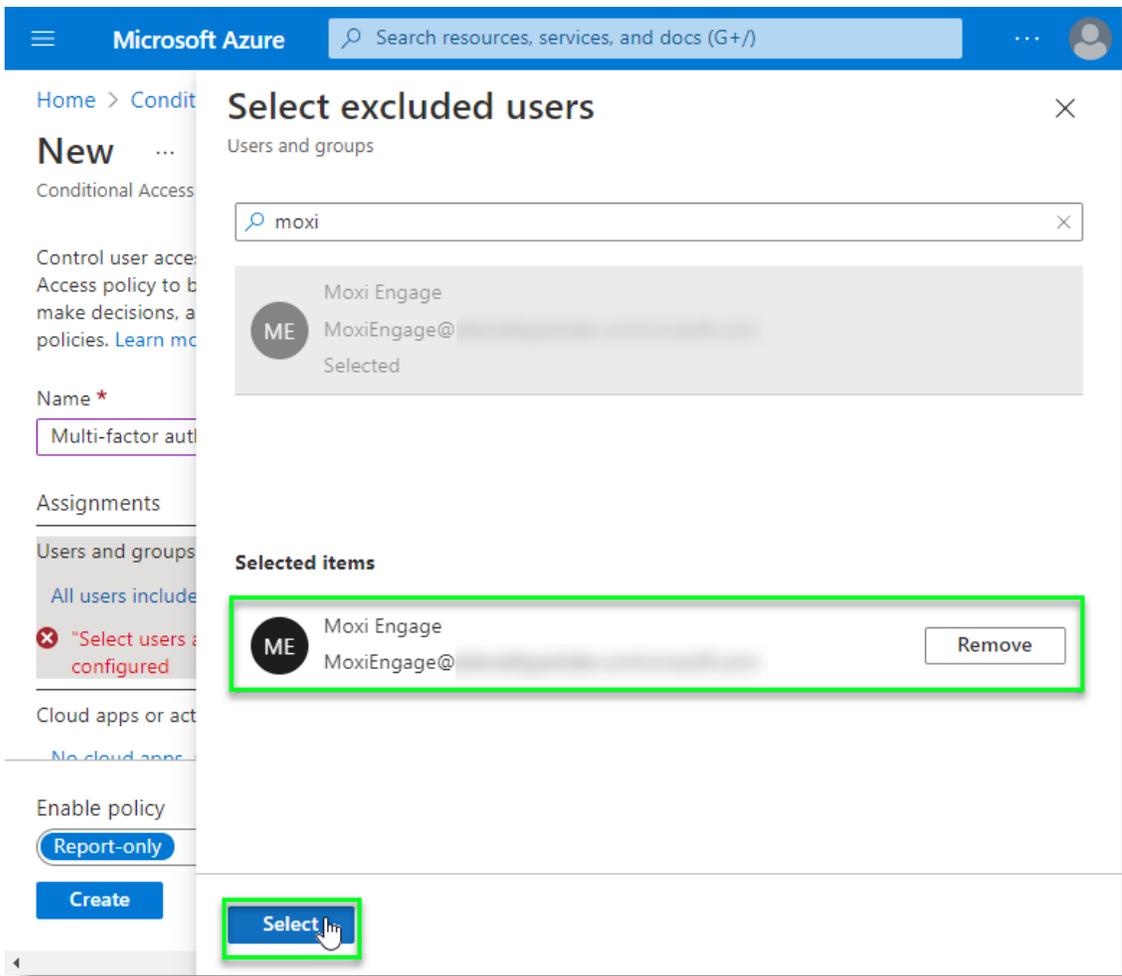
15. Ensure the “Exclude” tab of the overlay form is selected, then mark the checkbox next to the “Users and groups” label.



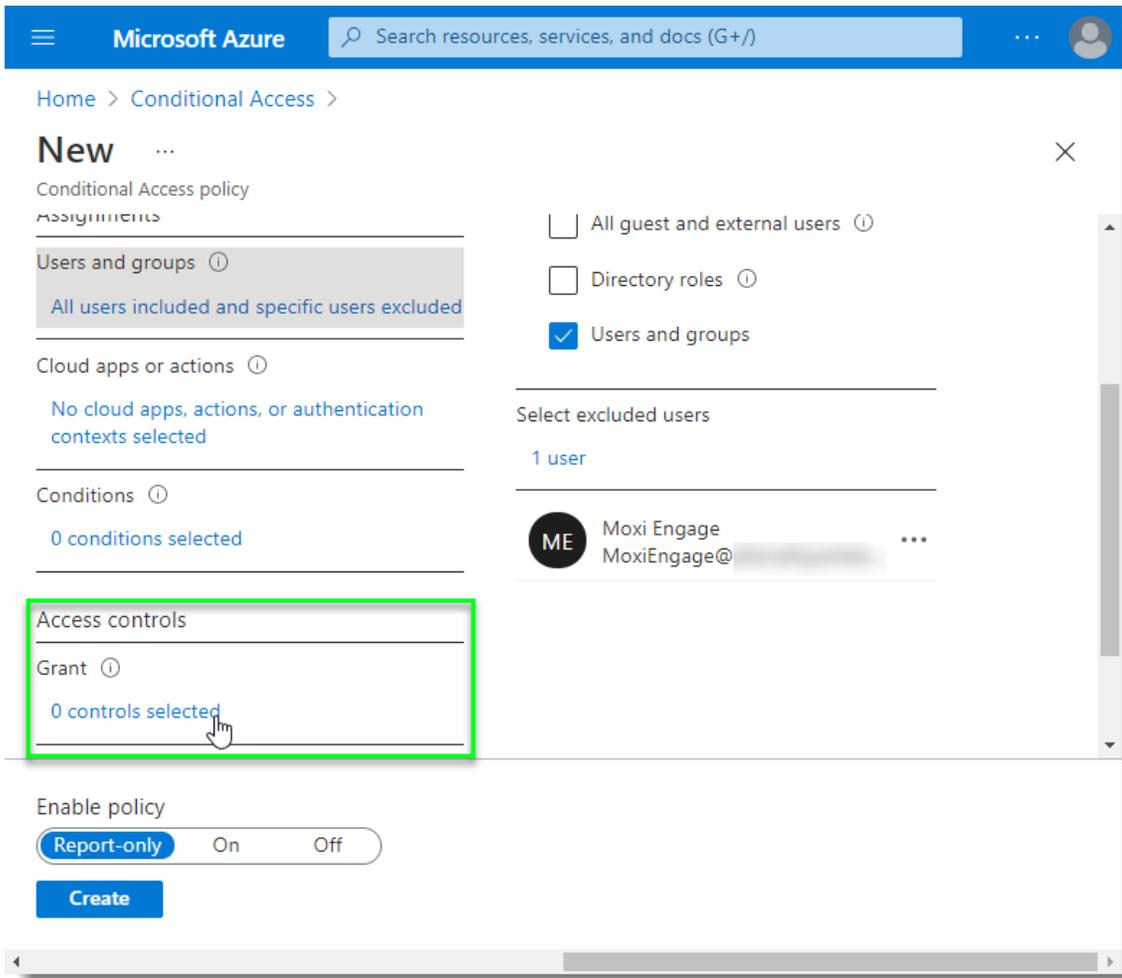
- 16. Begin typing the name of the service account in the “Select excluded users” search box (e.g., “Moxi”), then click on the service account user in the list to select it for exclusion.



- 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.



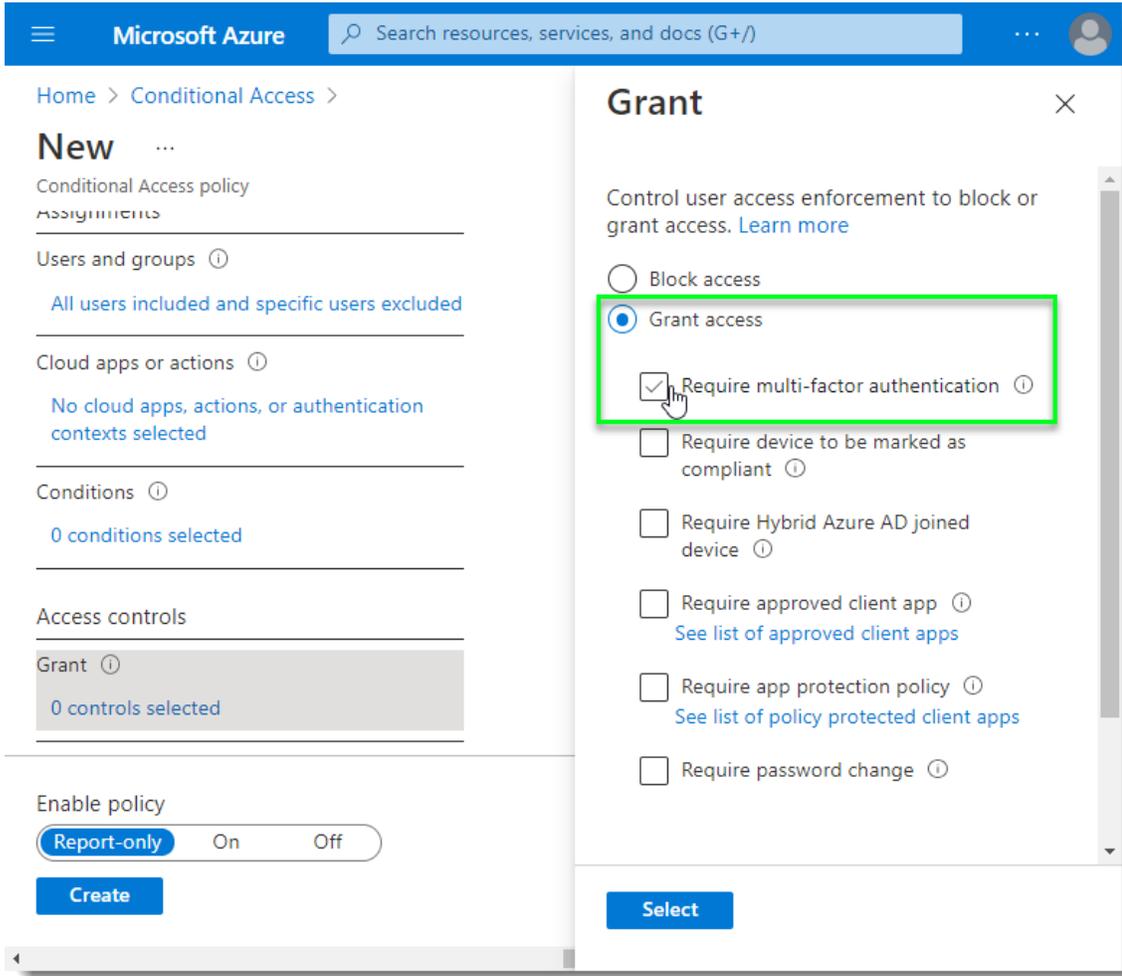
The screenshot shows the Microsoft Azure portal interface for creating a new Conditional Access policy. The breadcrumb navigation is "Home > Conditional Access >". The main heading is "New" with a close button (X). The page is divided into several sections:

- Assignments:** Includes "Users and groups" (with a help icon) and "All users included and specific users excluded".
- Cloud apps or actions:** Includes "No cloud apps, actions, or authentication contexts selected".
- Conditions:** Includes "0 conditions selected".
- Access controls:** This section is highlighted with a green box. It contains a "Grant" heading (with a help icon) and a link that says "0 controls selected". A mouse cursor is clicking on this link.
- Enable policy:** Includes a "Report-only" button, "On" and "Off" radio buttons, and a "Create" button.

On the right side of the page, there are additional options for user selection:

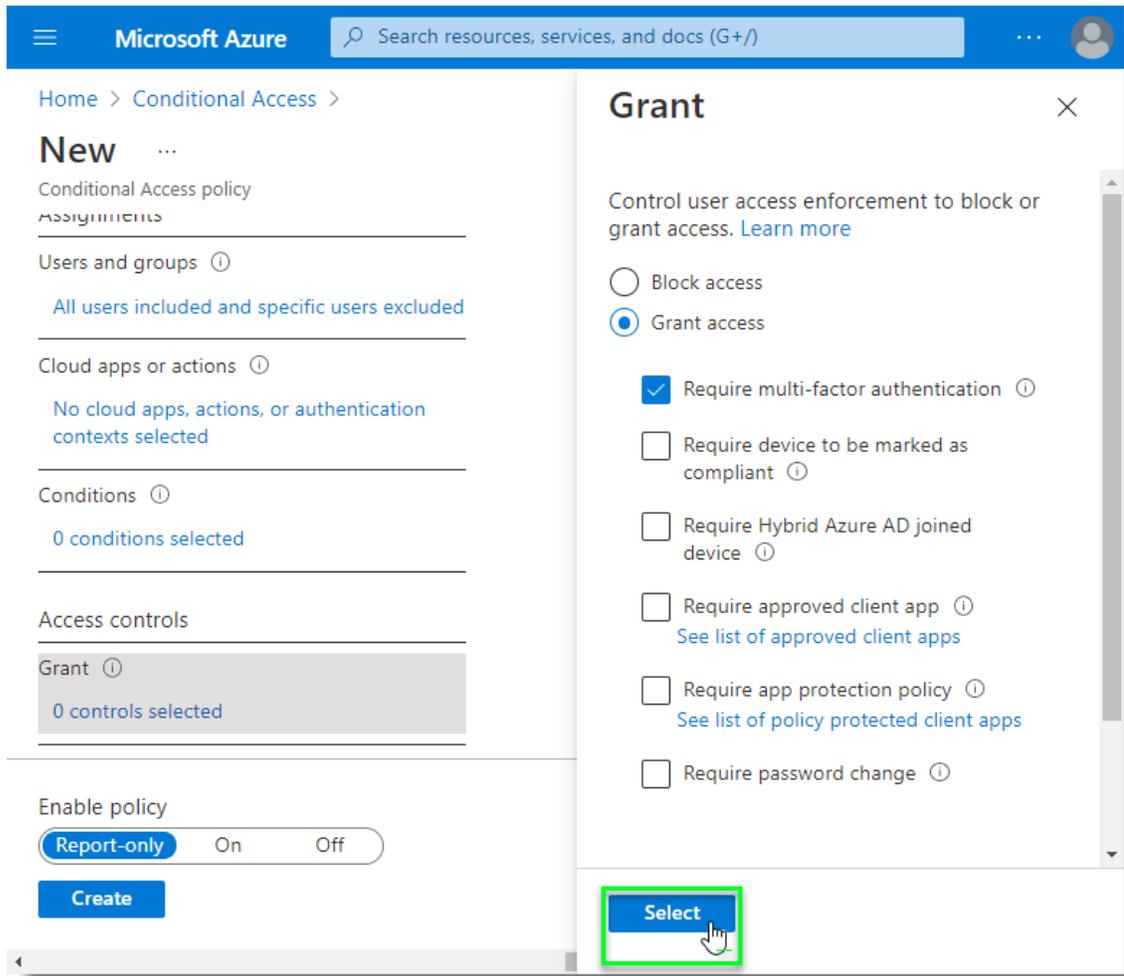
- Checkboxes for "All guest and external users", "Directory roles", and "Users and groups" (which is checked).
- A section titled "Select excluded users" showing "1 user" selected.
- A list of excluded users, including "Moxi Engage" (MoxiEngage@) with a three-dot menu icon.

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

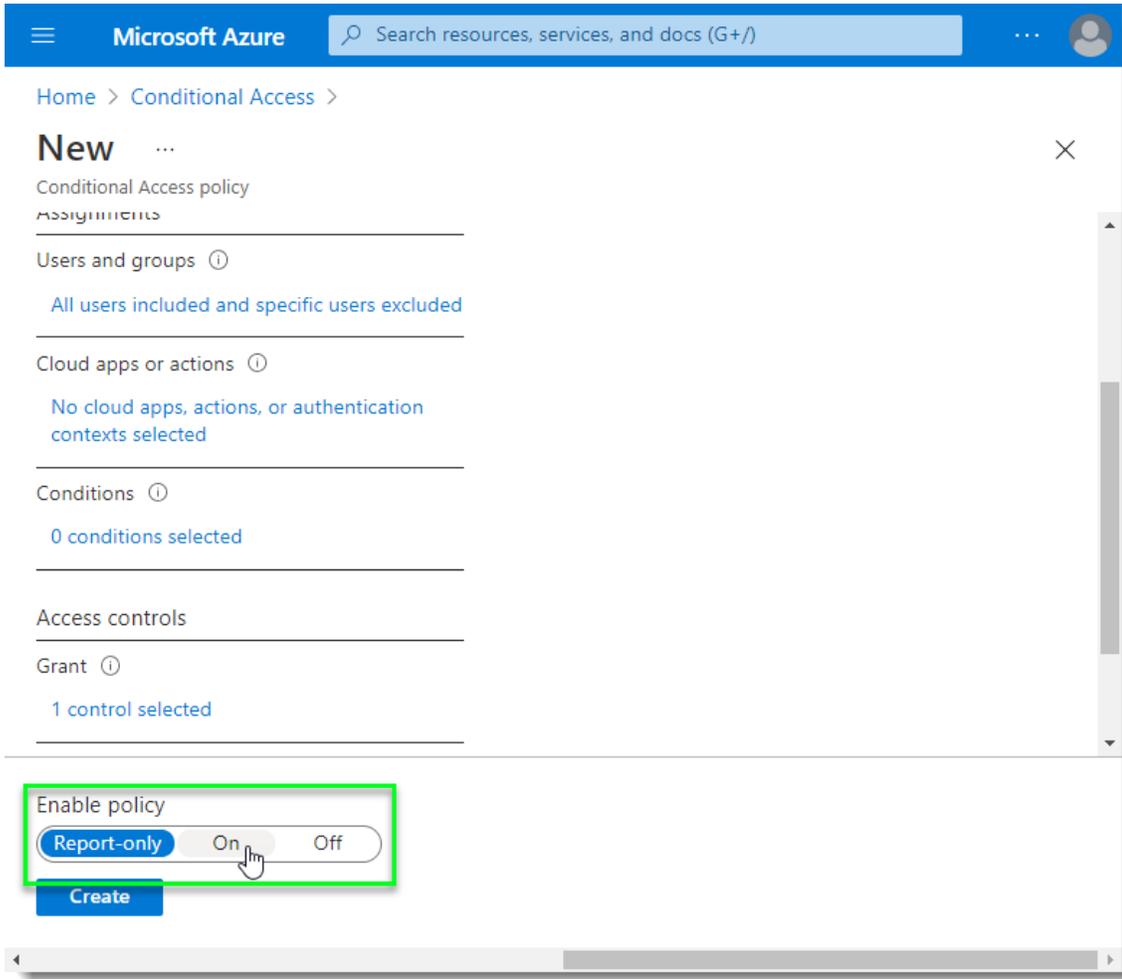


The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The main navigation bar at the top includes the Microsoft Azure logo, a search bar, and a user profile icon. The breadcrumb trail indicates the current location: Home > Conditional Access > Grant. The left sidebar contains a 'New' section with various configuration options: 'Conditional Access policy' (with a sub-section for assignments), 'Users and groups' (with a link to 'All users included and specific users excluded'), 'Cloud apps or actions' (with a link to 'No cloud apps, actions, or authentication contexts selected'), 'Conditions' (with a link to '0 conditions selected'), and 'Access controls' (with a link to 'Grant' and '0 controls selected'). The 'Enable policy' section at the bottom left shows a toggle set to 'Report-only' (with 'On' and 'Off' options) and a 'Create' button. The main content area is titled 'Grant' and features a close button (X). It contains the following options: 'Block access' (unselected), 'Grant access' (selected and highlighted with a green box), 'Require multi-factor authentication' (checked and highlighted with a green box), 'Require device to be marked as compliant' (unchecked), 'Require Hybrid Azure AD joined device' (unchecked), 'Require approved client app' (unchecked, with a link to 'See list of approved client apps'), 'Require app protection policy' (unchecked, with a link to 'See list of policy protected client apps'), and 'Require password change' (unchecked). A 'Select' button is located at the bottom right of the configuration panel.

20. Click on the “Select” button.



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

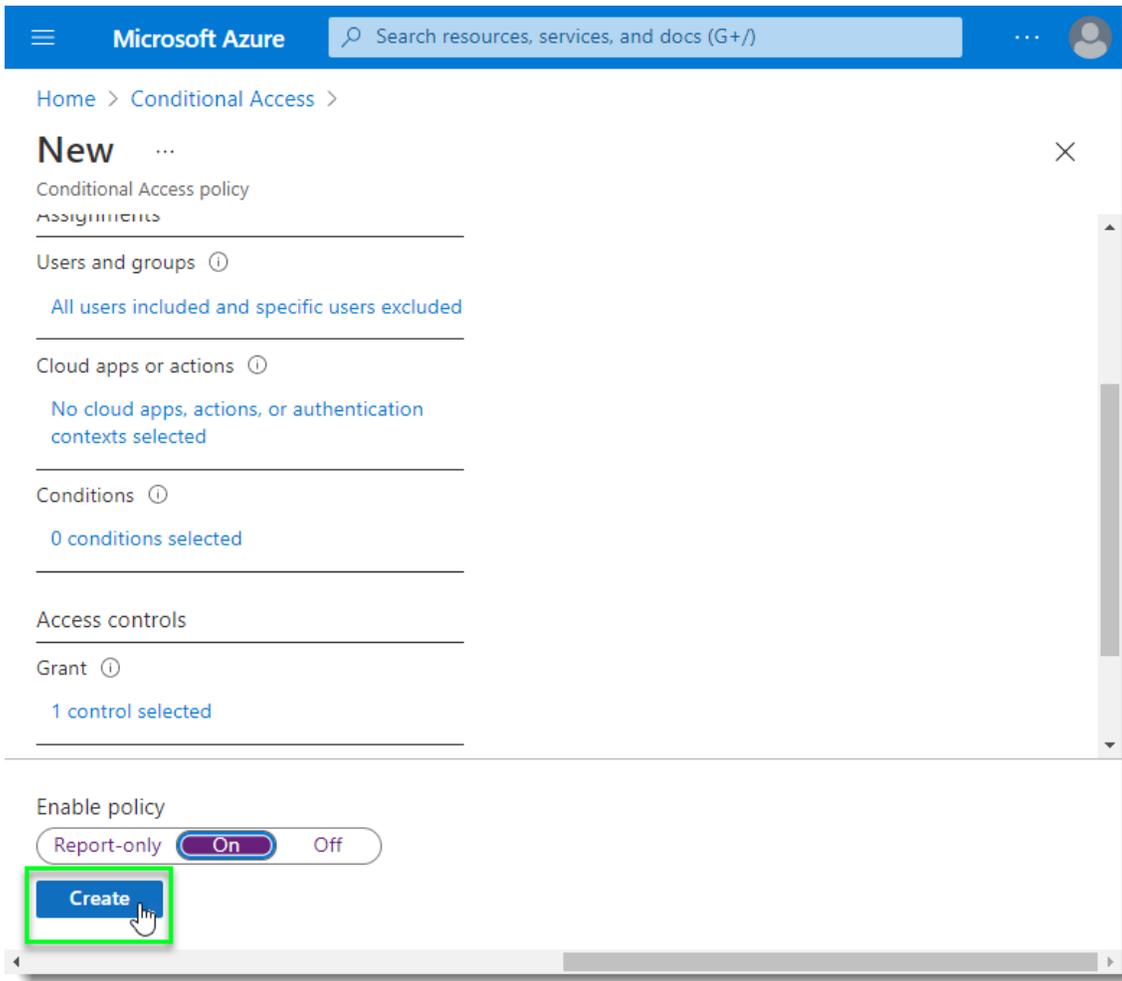


The screenshot shows the Microsoft Azure portal interface for creating a new Conditional Access policy. The breadcrumb navigation is "Home > Conditional Access >". The page title is "New" with a close button (X) in the top right corner. Below the title, the text "Conditional Access policy" and "ASSIGNMENTS" is displayed. The configuration steps are as follows:

- Users and groups:** "All users included and specific users excluded"
- Cloud apps or actions:** "No cloud apps, actions, or authentication contexts selected"
- Conditions:** "0 conditions selected"
- Access controls:** "Grant" with "1 control selected"

At the bottom of the configuration area, the "Enable policy" section is highlighted with a green border. It contains three radio button options: "Report-only" (selected), "On", and "Off". A mouse cursor is positioned over the "On" option. Below the radio buttons is a blue "Create" button.

22. Click on the “Create” button.

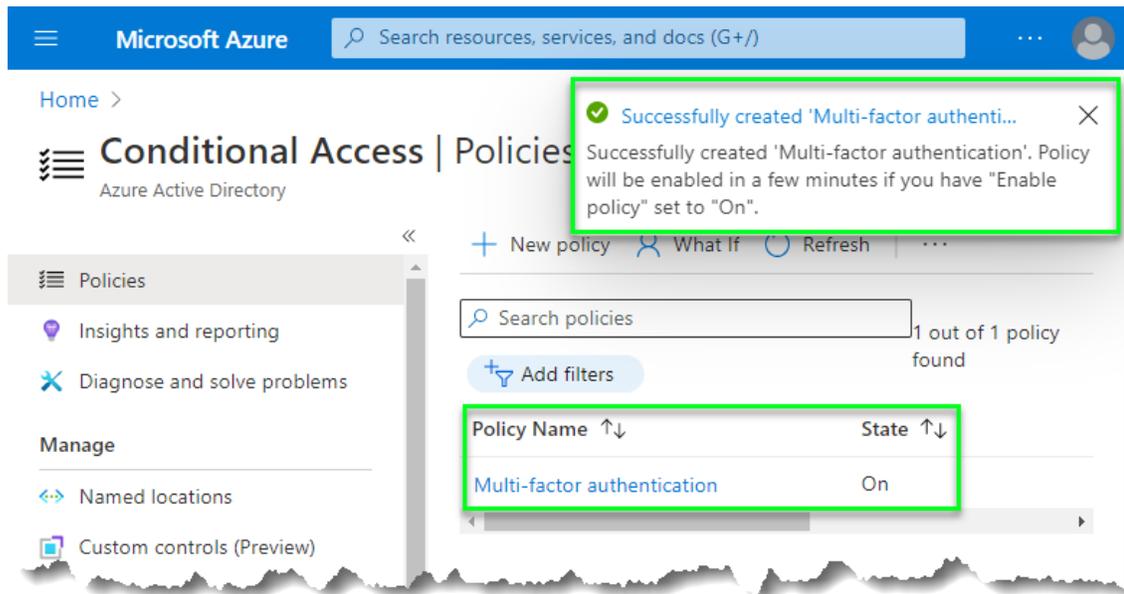


The screenshot shows the Microsoft Azure portal interface for creating a new Conditional Access policy. The breadcrumb navigation is "Home > Conditional Access >". The main heading is "New" with a close button (X) in the top right corner. Below the heading, the configuration is organized into sections:

- Users and groups**: "All users included and specific users excluded"
- Cloud apps or actions**: "No cloud apps, actions, or authentication contexts selected"
- Conditions**: "0 conditions selected"
- Access controls**: "Grant" section with "1 control selected"

At the bottom, the "Enable policy" section has a toggle set to "On" (with "Report-only" and "Off" as other options). A blue "Create" button is located at the bottom left of the configuration area, highlighted with a green rectangular box. A mouse cursor is positioned over 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?](#)