4 - Modifying Jamf Connect to apply Azure Conditional Access Policies

Overview

Jamf Connect, being a desktop or native application, does not normally appear in the list of applications for Microsoft Azure Conditional Access policies. By adding a custom scope and a “private” application for Jamf Connect, we can apply a conditional access policy.

In this scenario, we want the non-interactive login (where Jamf Connect validates the user’s local password matches the Azure password) to be exempt from a conditional access policy that requires multi-factor authentication (MFA) but to enforce MFA at the *interactive* login of a user logging into a macOS client with the Azure web interface.

Net result: When a user logs in and sees a Microsoft login webpage, they’re asked to follow whatever conditional access rules the administrator has created. When Jamf Connect is simply checking the password silently in the background, the operation works without showing any errors in the login logs for the user, reducing the risk of marking a user’s login session as a medium or high risk.

Workflow overview:

- Create a “private endpoint” application registration with a custom API
    - With API permissions for “User.read”
    - With “Expose an API” scope created
- Create a “public endpoint” application registration for OIDC to call that custom API
    - Add API permission for “My APIs” for the name of the application created in first step and the scope created in first step
    - Define roles like “Admin” and “Standard” for elevating macOS account permissions
- Optional: Create an Azure Conditional Access policy to require multi-factor authentication

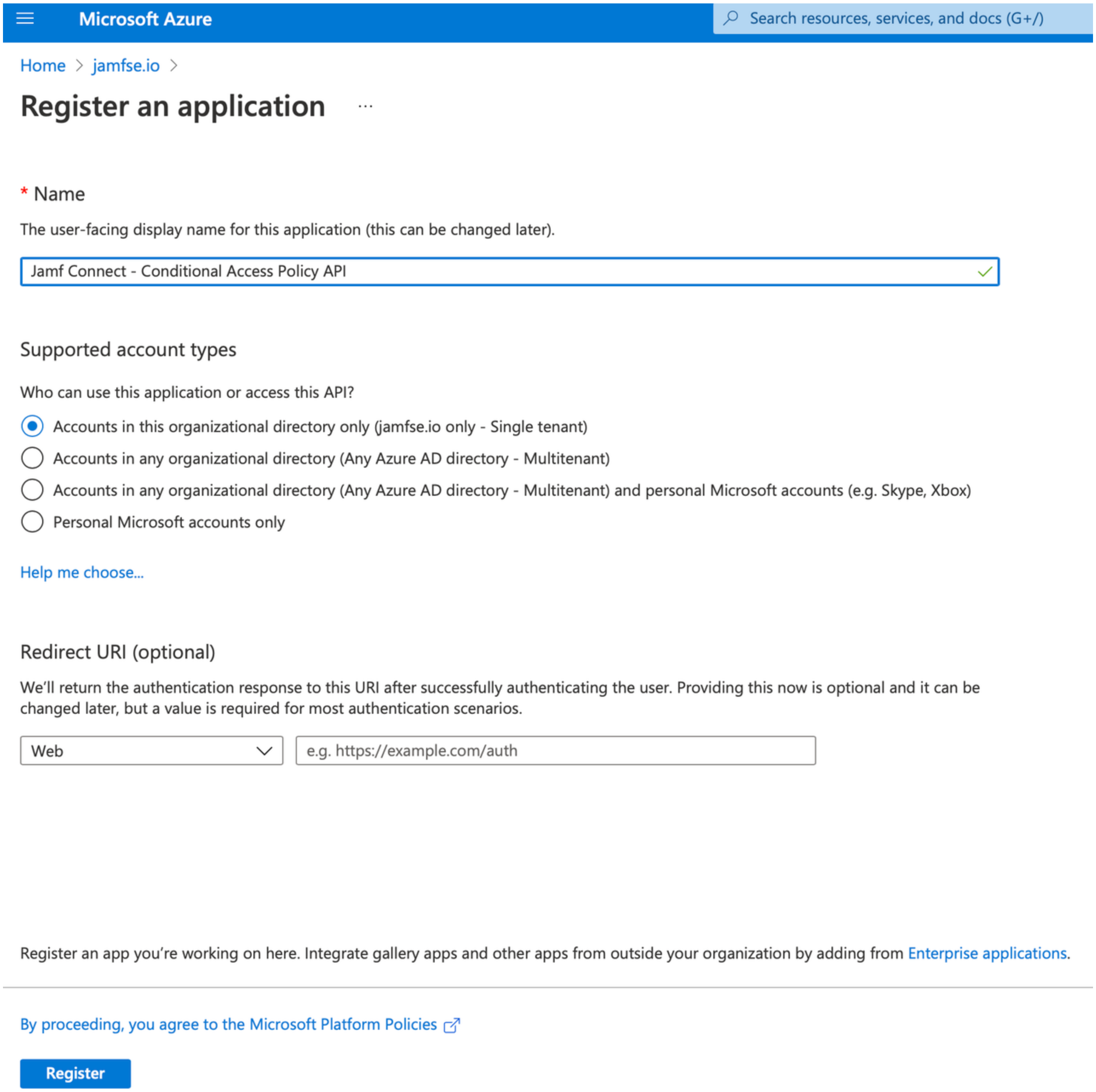
- Create an exception to Azure Conditional Access policies to exempt ROPG from requiring MFA
- Create a Jamf Connect Login configuration profile
    - Azure as Identity Provider
    - Define a custom scope
    - Test with Jamf Connect Configuration

Minimum system requirements

These instructions were written assuming you are using Jamf Connect version 2.17 or greater.

Step One: Create an application registration with a custom API

Navigate to portal.azure.com → Azure Active Directory → App Registrations. Create a new app registration. Name the application “Jamf Connect - Conditional Access Policy API”. Select the supported account types to “Accounts in this organizational directory only”. Leave Redirect URI section blank. Register the application.



Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Jamf Connect - Conditional Access Policy API ✓

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (jamfse.io only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

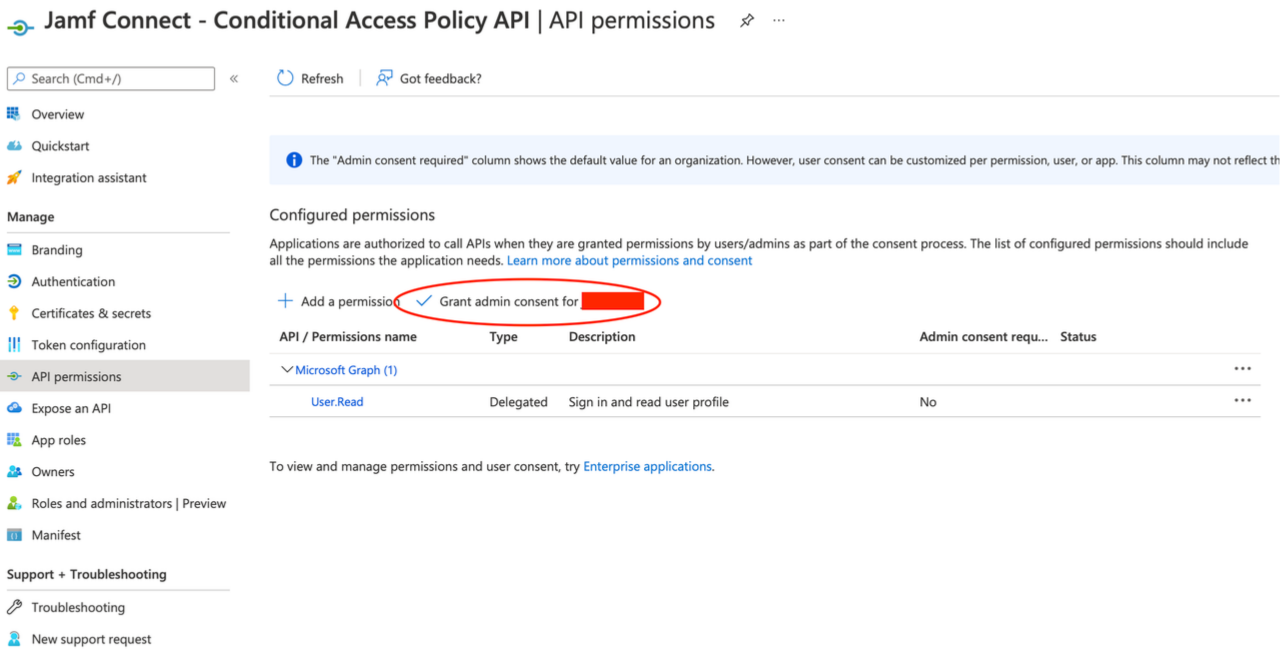
Web | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Application Registration Screen (as of 06DEC2021)

Navigate to API permissions on the left hand navigation bar. Grant admin consent for the organization.



Jamf Connect - Conditional Access Policy API | API permissions

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect th

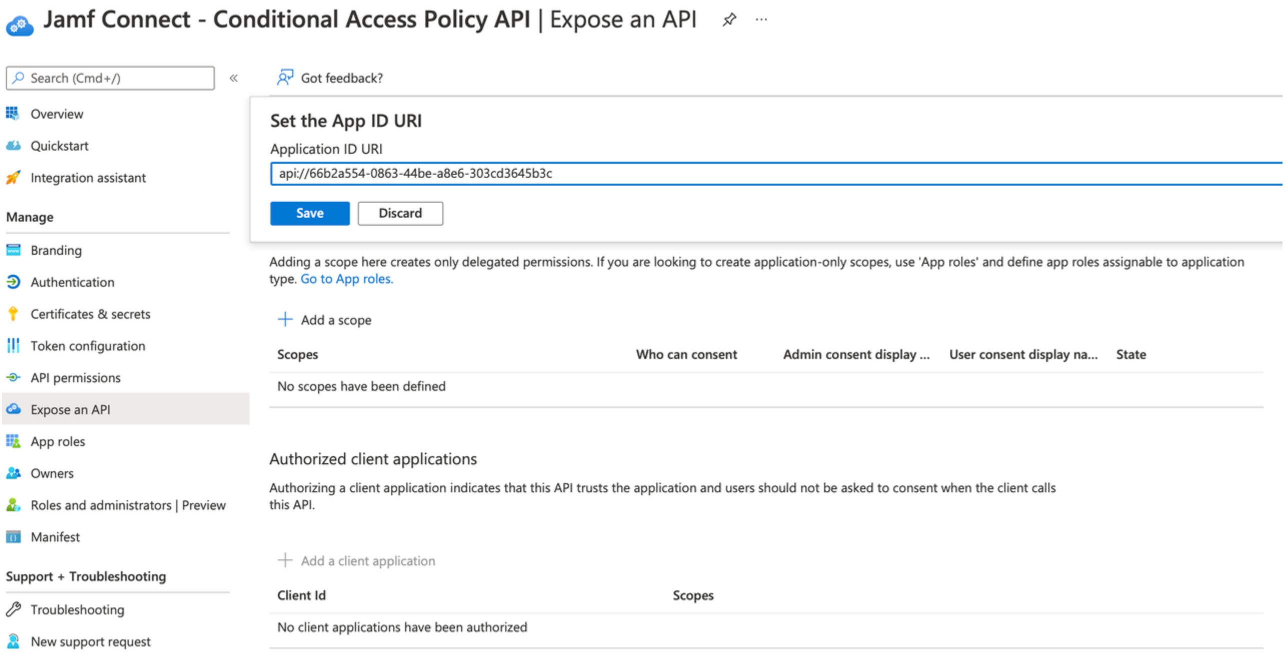
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.

Using the left hand navigation bar, select “Expose an API”. Set the Application ID URI. A default entry will be created based on the pattern of `api://[application ID]`. This may be modified if desired but default entry is acceptable.



Jamf Connect - Conditional Access Policy API | Expose an API

Set the App ID URI

Application ID URI: api://66b2a554-0863-44be-a8e6-303cd3645b3c

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

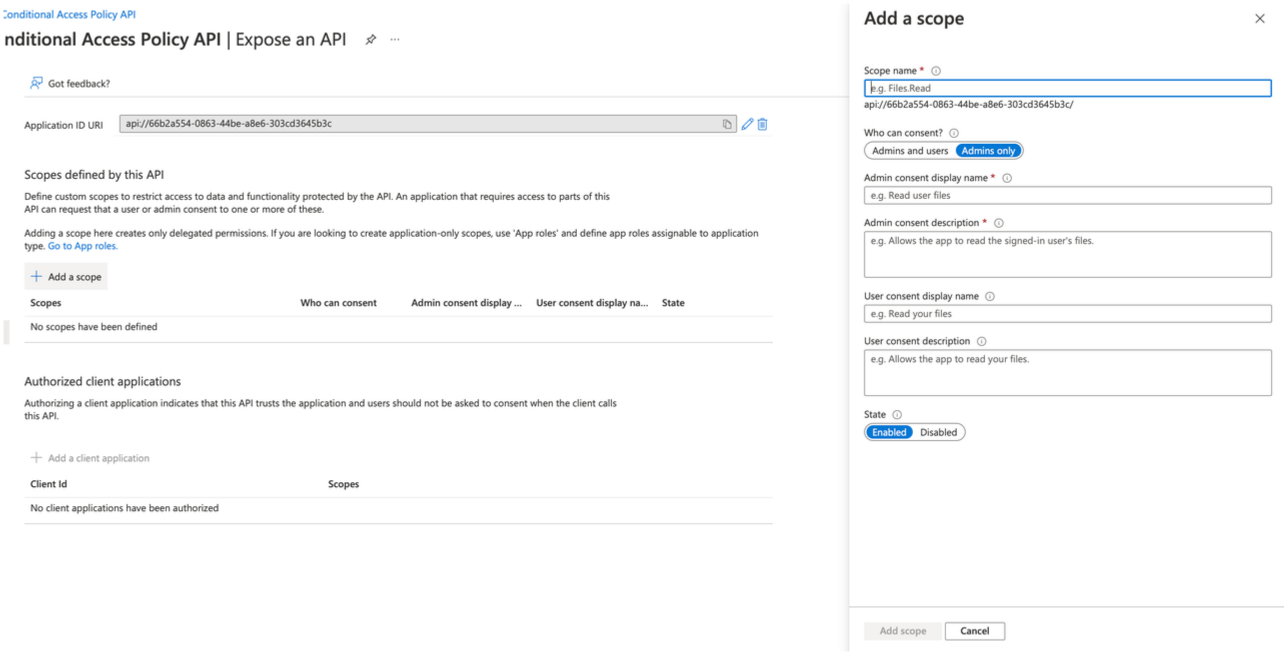
Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

Client Id	Scopes
No client applications have been authorized	

Select the option for “Add a scope”



Conditional Access Policy API

nditional Access Policy API | Expose an API

Got feedback?

Application ID URI: api://66b2a554-0863-44be-a8e6-303cd3645b3c

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Add a scope

Scope name *: e.g. Files.Read
api://66b2a554-0863-44be-a8e6-303cd3645b3c/

Who can consent?: Admins and users [✓ Admins only]

Admin consent display name *: e.g. Read user files

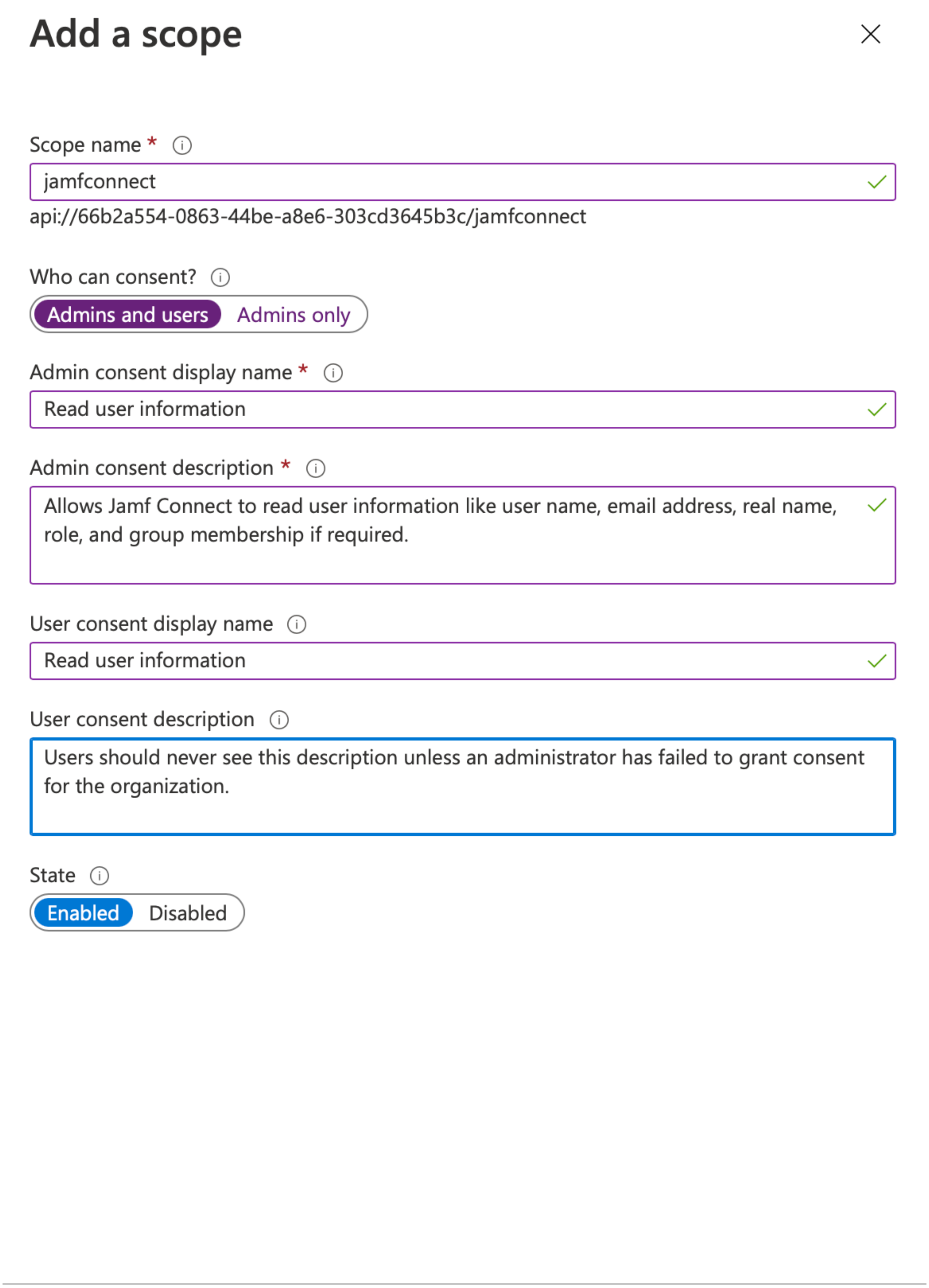
Admin consent description *: e.g. Allows the app to read the signed-in user's files.

User consent display name: e.g. Read your files

User consent description: e.g. Allows the app to read your files.

State: [✓ Enabled] Disabled

Set the scope name to `jamfconnect`. "Who can consent" will be set to the default option "Admins" - you will consent on behalf of the users in the next step so this can be set either to "Admins and users" or "Admins only." Enter information into the Admin consent display name and Admin consent description. Any text is acceptable - this will be accepted by the admin in the next step. Press "Add scope" to save.



Add a scope

Scope name *

jamfconnect

api://66b2a554-0863-44be-a8e6-303cd3645b3c/jamfconnect

Who can consent?

[✓ Admins and users] Admins only

Admin consent display name *

Read user information

Admin consent description *

Allows Jamf Connect to read user information like user name, email address, real name, role, and group membership if required.

User consent display name

Read user information

User consent description

Users should never see this description unless an administrator has failed to grant consent for the organization.

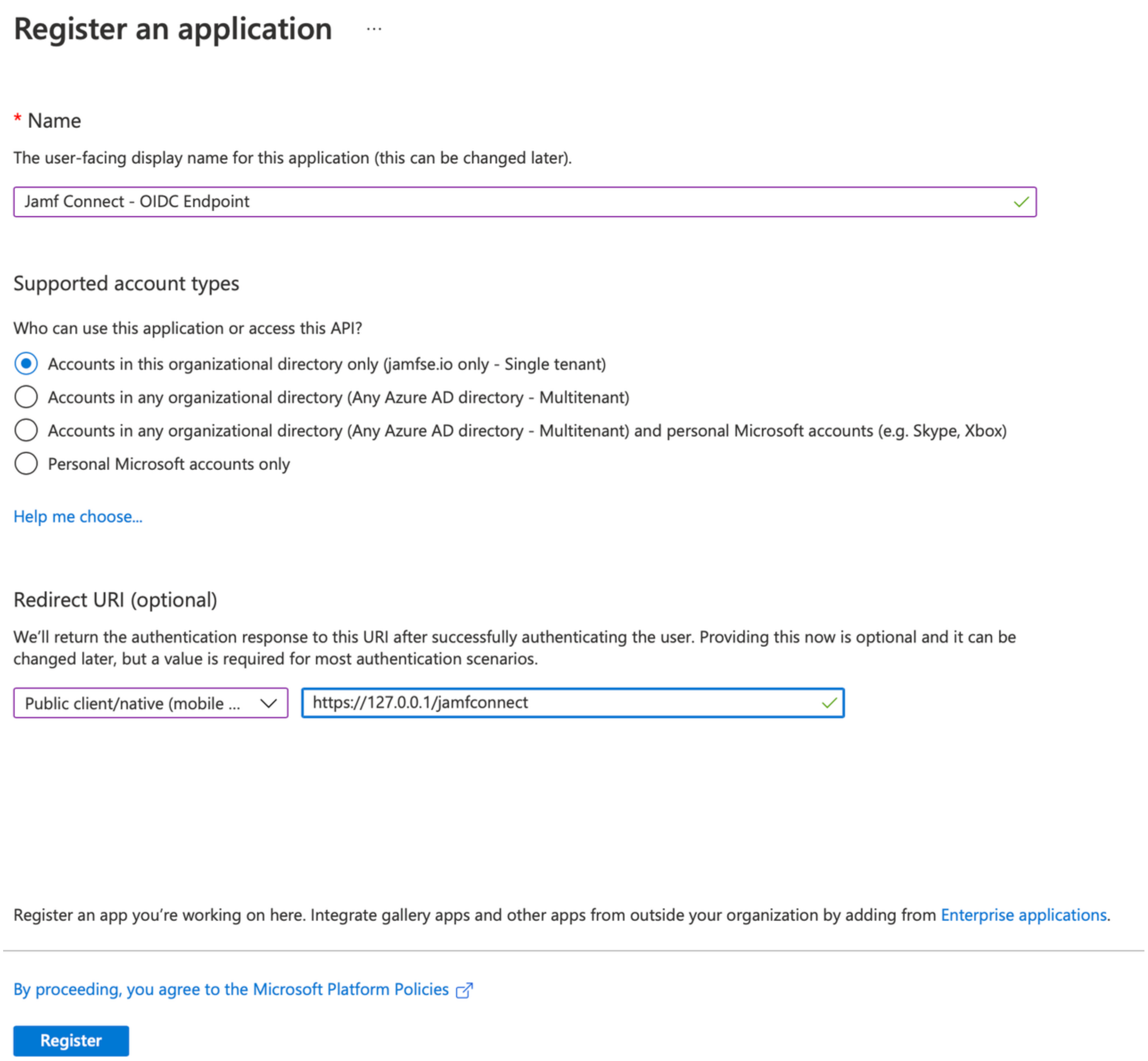
State

[✓ Enabled] Disabled

Copy the scope with the Copy button and save it for later. This will be used as the `OIDCScopes` later in Jamf Connect Configuration.

Step Two: Create an application registration that calls the custom scope

Return to Azure Active Directory → App Registrations. Create a new app registration. Name the app "Jamf Connect - OIDC Endpoint". Set Supported account types to "Accounts in this organizational directory only". Set Redirect URI to "Public client/native (mobile & desktop)" with the value `https://127.0.0.1/jamfconnect`. Register the application.



Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

Jamf Connect - OIDC Endpoint ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (jamfse.io only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

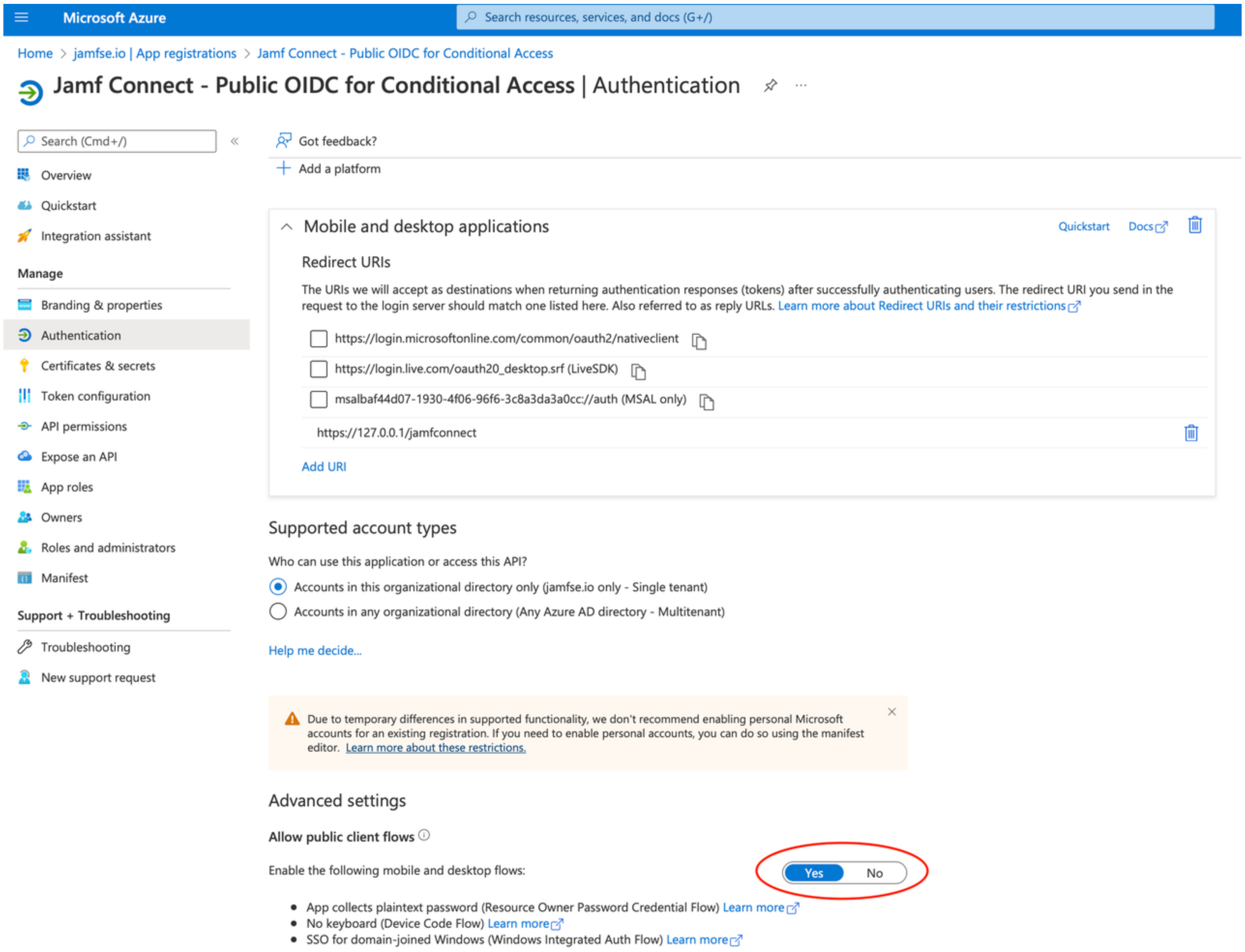
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | https://127.0.0.1/jamfconnect ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Navigate to Authentication on the left hand navigation bar. Set "Allow public client flows" to "Yes." (This feature enables Resource Owner Password Grant or ROPG to validate passwords.)



Jamf Connect - Public OIDC for Conditional Access | Authentication

Mobile and desktop applications

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

- ☐ https://login.microsoftonline.com/common/oauth2/nativeclient
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)
- ☐ msalbaf44d07-1930-4f06-96f6-3c8a3da3a0cc://auth (MSAL only)
- https://127.0.0.1/jamfconnect

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (jamfse.io only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

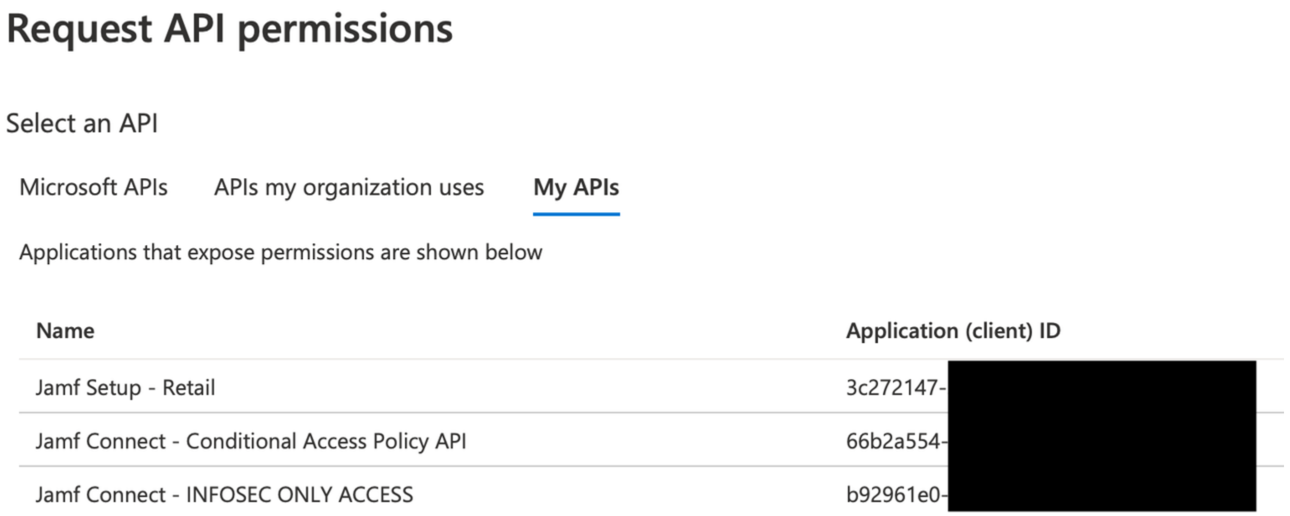
Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Authentication page for an App registration (25AUG2022)

Navigate to API permissions. By default, the Microsoft Graph → User.Read permission is added. Use the “Grant admin consent for [domain]” button to grant permission to read the user information on behalf of the user.

Next, select “+ Add a permission”. Select the “My APIs” tab. Select the name of the application you created in step 1.



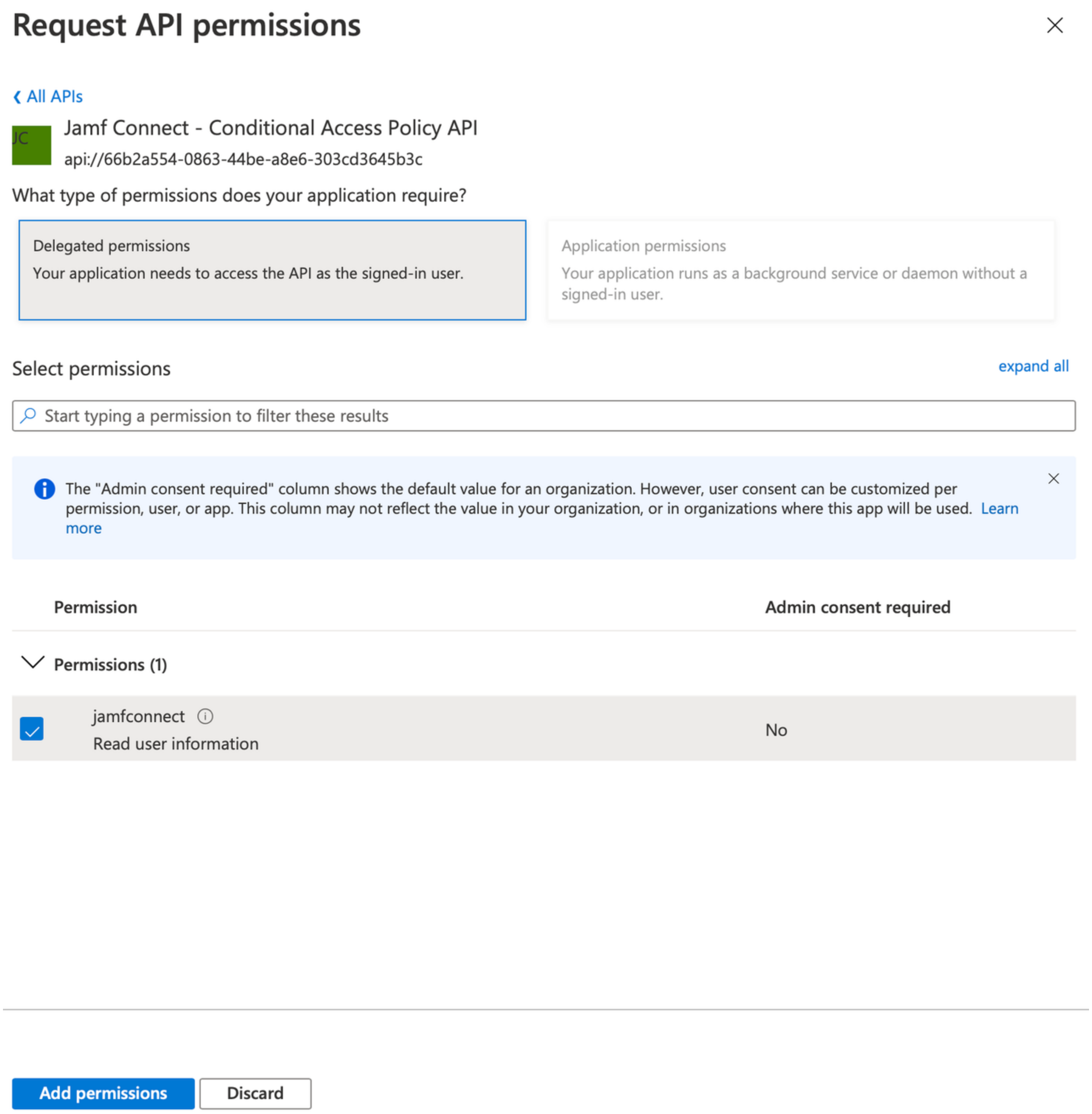
Request API permissions

Select an API

Applications that expose permissions are shown below

Name	Application (client) ID
Jamf Setup - Retail	3c272147-[redacted]
Jamf Connect - Conditional Access Policy API	66b2a554-[redacted]
Jamf Connect - INFOSEC ONLY ACCESS	b92961e0-[redacted]

Select the option for “Delegated permissions” and check the box for “jamfconnect” - the only permission listed in the application. Use the “Add permissions” button to close the window.



Jamf Connect - Conditional Access Policy API

api://66b2a554-0863-44be-a8e6-303cd3645b3c

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

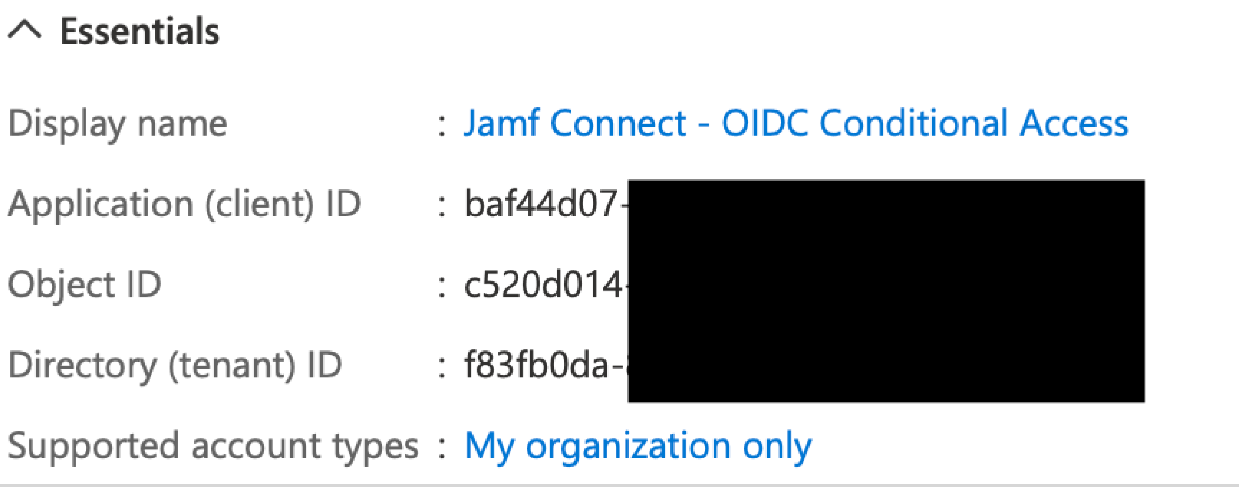
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Permission	Admin consent required
Permissions (1)	
☑ jamfconnect ⓘ Read user information	No

Use the "Grant admin consent for [domain]" to grant permission to access the API on behalf of users.

Optional: Use the "App roles" option to add a role for "Administrator" and "Standard". This will allow you to define users or groups of users directly in Azure who should have administrator rights on macOS client machines. "App roles" is located on the left hand navigation tool bar in the App registration - refer to https://docs.jamf.com/jamfconnect/documentation/Login_Window_Preferences.html for more details on the `OIDCAdminAttribute` and `OIDCAdmin` settings for Jamf Connect.

Navigate to Overview. Record the Application (client) ID and the Directory (tenant) ID for later use with Jamf Connect Configuration.



^ Essentials

Display name : Jamf Connect - OIDC Conditional Access

Application (client) ID : baf44d07- [redacted]

Object ID : c520d014

Directory (tenant) ID : f83fb0da-

Supported account types : My organization only

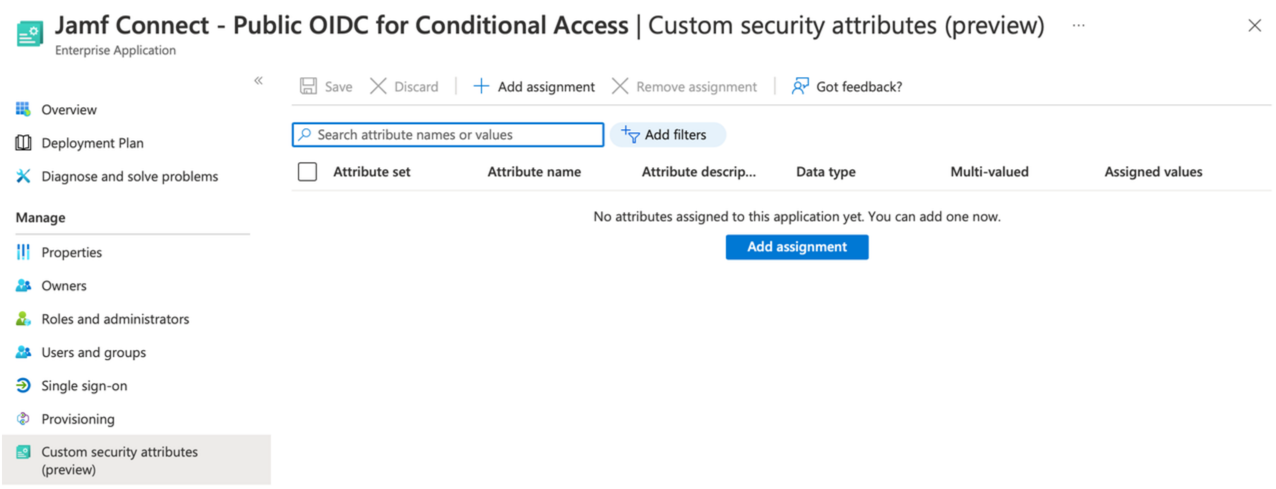
Navigate to Azure Active Directory → Enterprise Applications. Find the Jamf Connect - OIDC Endpoint application you created and assign users and roles to the application.

Step Three: Apply a custom security attribute to the Jamf Connect - OIDC Endpoint application

Follow the instructions in https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/2_-_Creating_Custom_Security_Attributes_in_Microso.pdf to create a custom security attribute.

Apply Custom Security Attribute to Enterprise application

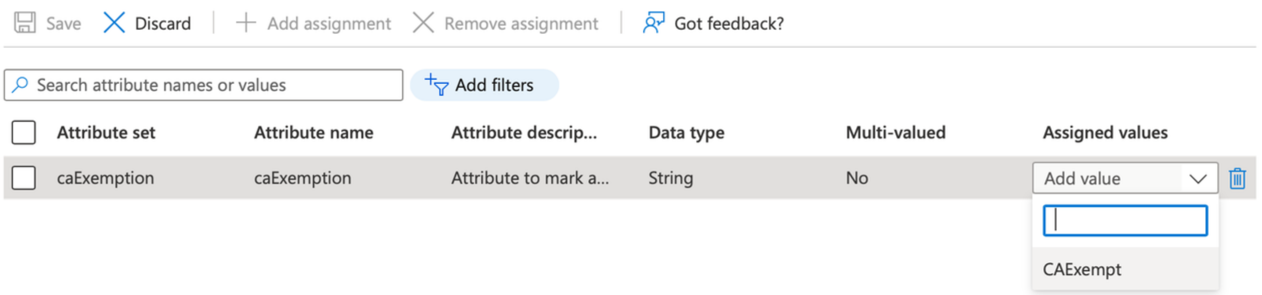
Navigate to Azure Active Directory → Enterprise applications. Select the app you named “Jamf Connect - OIDC Endpoint” in step two. In the left hand navigation bar under the section “Manage”, select the option for “Custom security attributes (preview)”.



☐ Attribute set	Attribute name	Attribute descrip...	Data type	Multi-valued	Assigned values

No attributes assigned to this application yet. You can add one now.

Select the option to “Add assignment.”



☐ Attribute set	Attribute name	Attribute descrip...	Data type	Multi-valued	Assigned values
☐ caExemption	caExemption	Attribute to mark a...	String	No	Add value

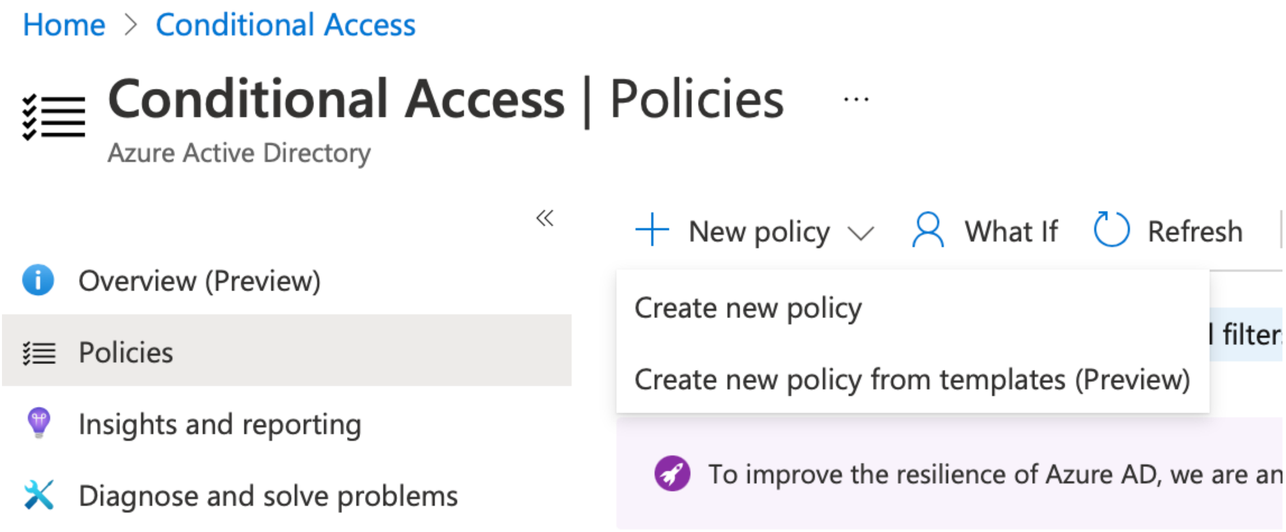
Select the options for the name of the attribute set you created and the attribute to mark the application exempt from Conditional Access policies.

Optional: Step Four: Create an Azure Conditional Access policy for Jamf Connect Login

If you already have a policy scoped to the “Cloud apps or actions” of “All cloud apps” to enforce the conditional access rules you wish to use, you can skip this step.

To make a conditional access policy for the Jamf Connect application, continue.

Navigate to portal.azure.com → Azure Conditional Access. Create a new policy.

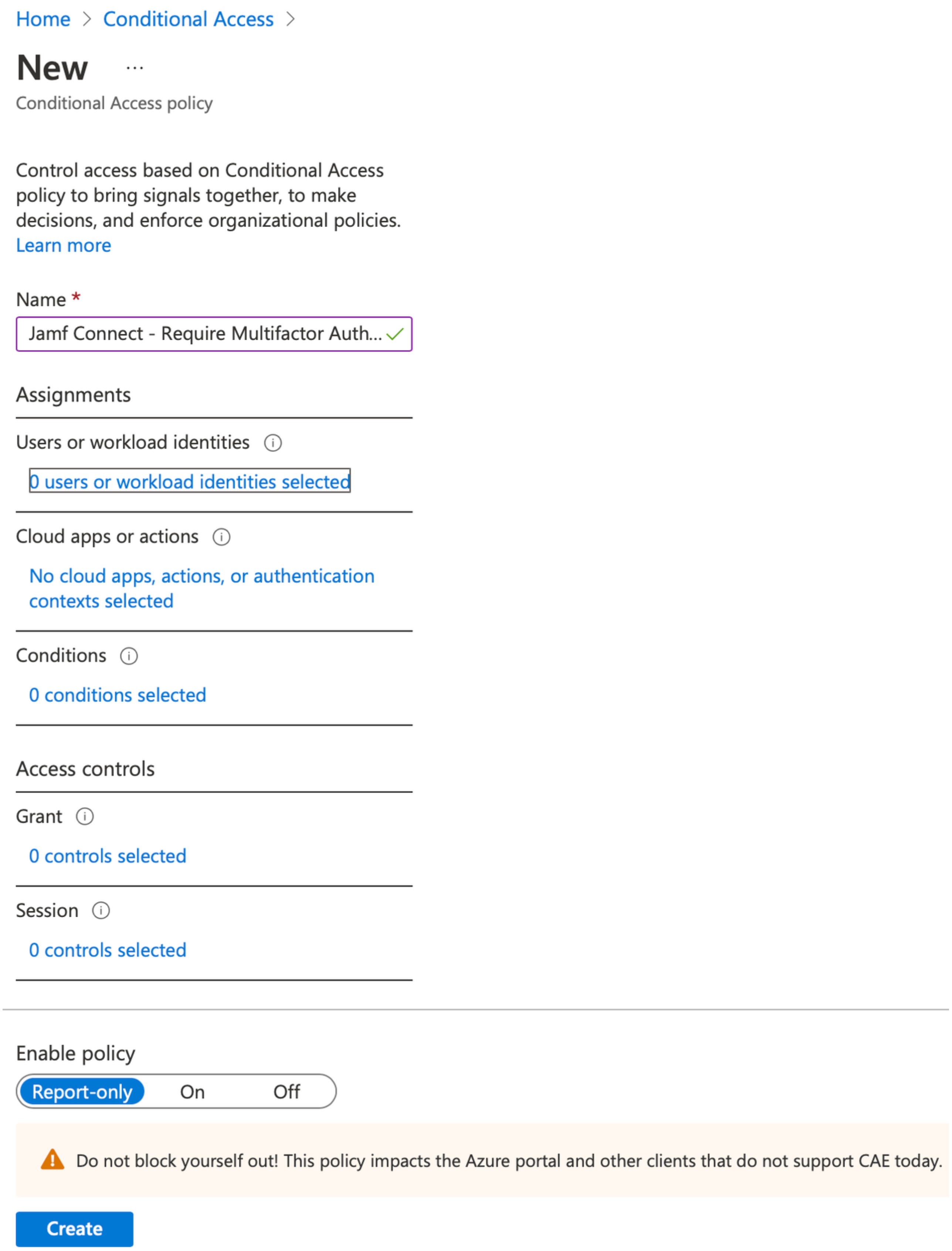

Home > Conditional Access

Conditional Access | Policies ...

Azure Active Directory

«
Overview (Preview)
Policies
Insights and reporting
Diagnose and solve problems
New policy
What If
Refresh
Create new policy
Create new policy from templates (Preview)
l filter
To improve the resilience of Azure AD, we are an

Name the policy as desired. The sample will name the policy “Jamf Connect - Require Multifactor Authentication”



Home > Conditional Access >

New ···

Conditional Access policy

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

Name *

Jamf Connect - Require Multifactor Auth... ✓

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

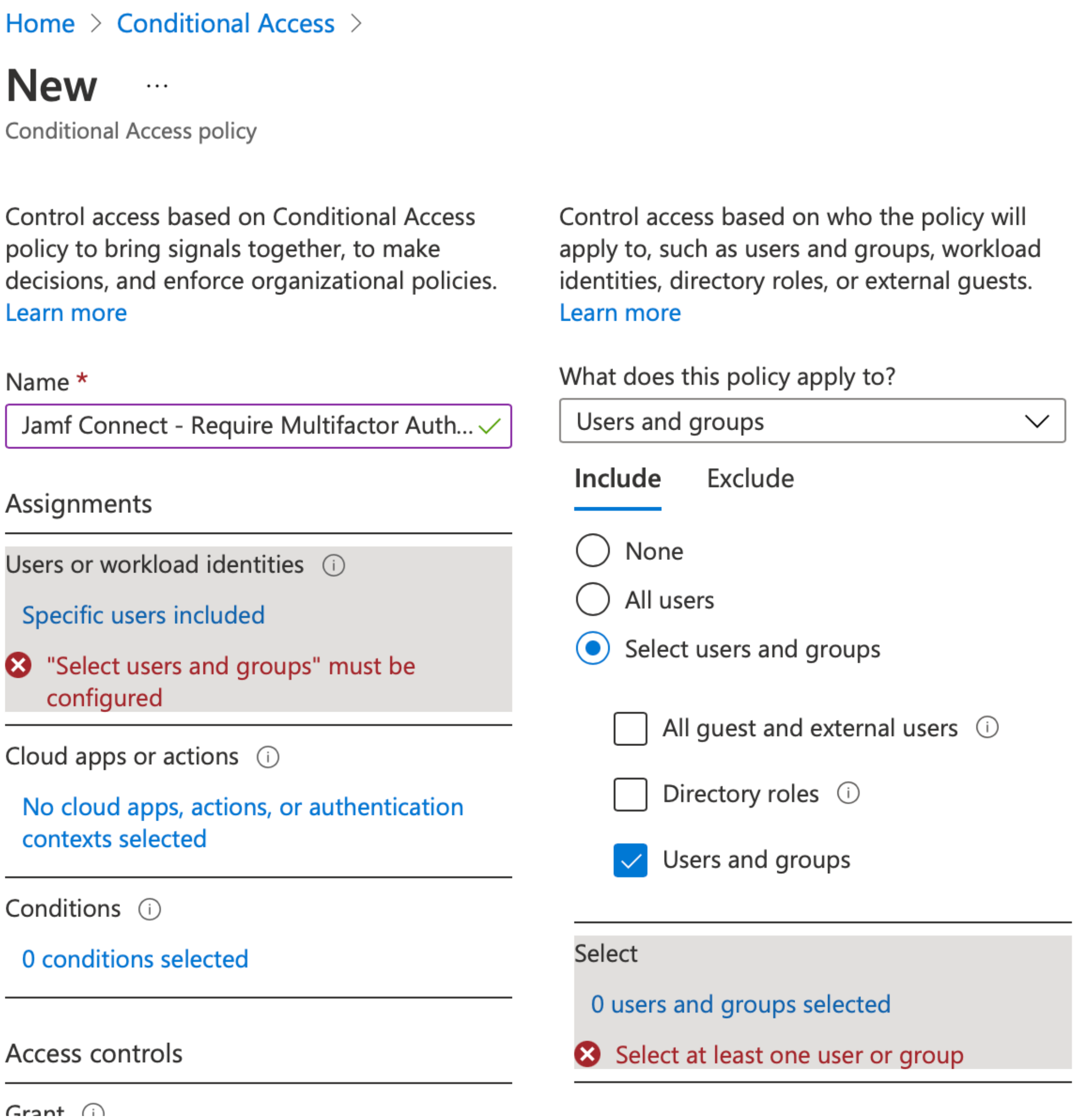
0 controls selected

Enable policy

[✓ Report-only] On Off

⚠ Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Select “Users or workload identities”. Select a test user to test your conditional access policy before applying to all users.



Home > Conditional Access >

New ...

Conditional Access policy

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

Name *

Jamf Connect - Require Multifactor Auth... ✓

Assignments

Users or workload identities ⓘ

Specific users included

☒ "Select users and groups" must be configured

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

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

What does this policy apply to?

Users and groups

Include | Exclude

○ None

○ All users

● Select users and groups

□ All guest and external users ⓘ

□ Directory roles ⓘ

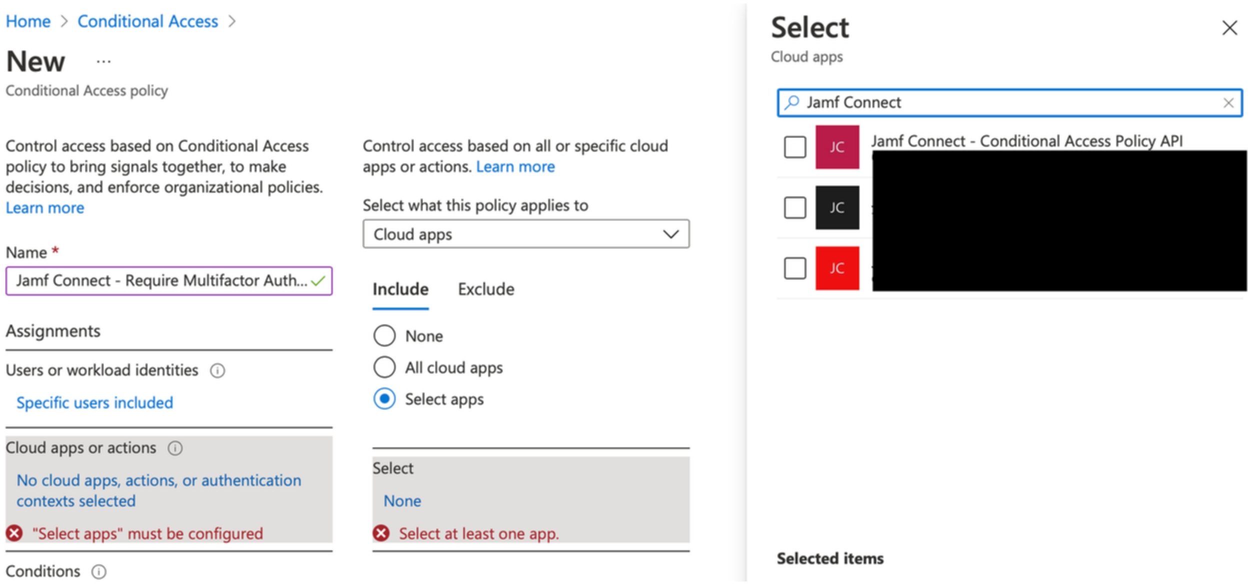
☑ Users and groups

Select

0 users and groups selected

☒ Select at least one user or group

Select “Cloud apps or actions”. Select the “Jamf Connect - Conditional Access Policy API” app registration you created in step one.



Home > Conditional Access >

New ...

Conditional Access policy

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

Name *

Jamf Connect - Require Multifactor Auth... ✓

Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

ⓧ "Select apps" must be configured

Conditions ⓘ

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include Exclude

○ None

○ All cloud apps

● Select apps

Select

None

ⓧ Select at least one app.

Select

Cloud apps

Jamf Connect

□ JC Jamf Connect - Conditional Access Policy API

□ JC

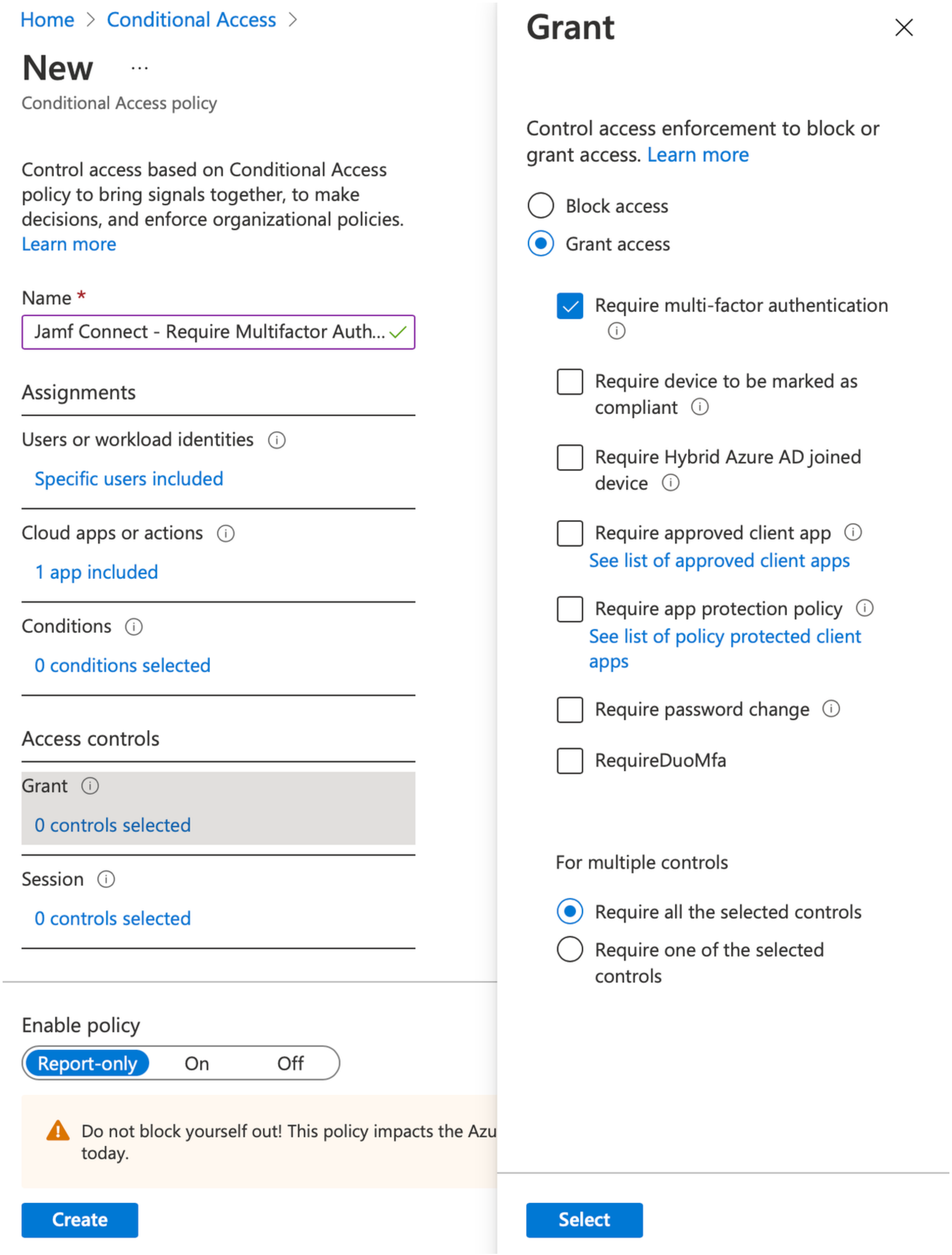
□ JC

[redacted]

Selected items

Select “Grant”. Check the options you wish to enforce as part of this policy. Set Enable policy to “On” and “Create” to save the policy.

Note: Some policies may lock users out of client macOS devices. It is not advised to apply a policy grant that requires a device to be marked as compliant or AD joined. If a device becomes non-compliant, it will be impossible to log into the device to bring it back into compliance. Similarly applying a “Condition” like being in a specific named IP address range may restrict users from logging into a macOS device to connect it to a specific network.



Home > Conditional Access >

New ···

Conditional Access policy

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

Name *

Jamf Connect - Require Multifactor Auth... ✓

Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

[✓ Report-only] On Off

⚠ Do not block yourself out! This policy impacts the Azu today.

Create

Grant ✕

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
See list of approved client apps

☐ Require app protection policy ⓘ
See list of policy protected client apps

☐ Require password change ⓘ

☐ RequireDuoMfa

For multiple controls

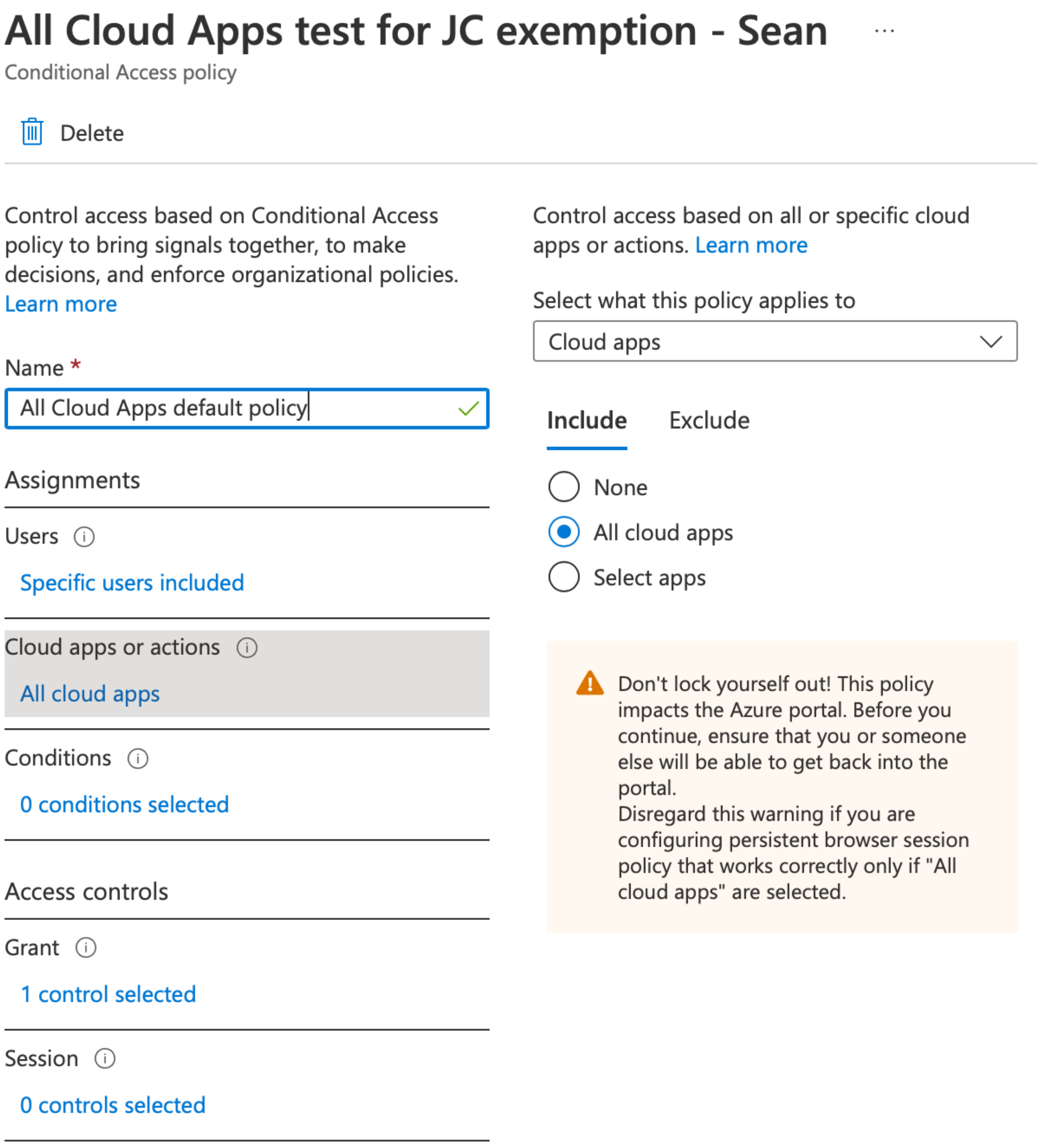
● Require all the selected controls

○ Require one of the selected controls

Select

Step Five: Apply exclusion policy to any Conditional Access policies scoped to All cloud apps

Search your Azure Conditional Access policy list for any policies that are scoped to "All cloud apps."



All Cloud Apps test for JC exemption - Sean ...

Conditional Access policy

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

Name *

All Cloud Apps default policy ✓

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

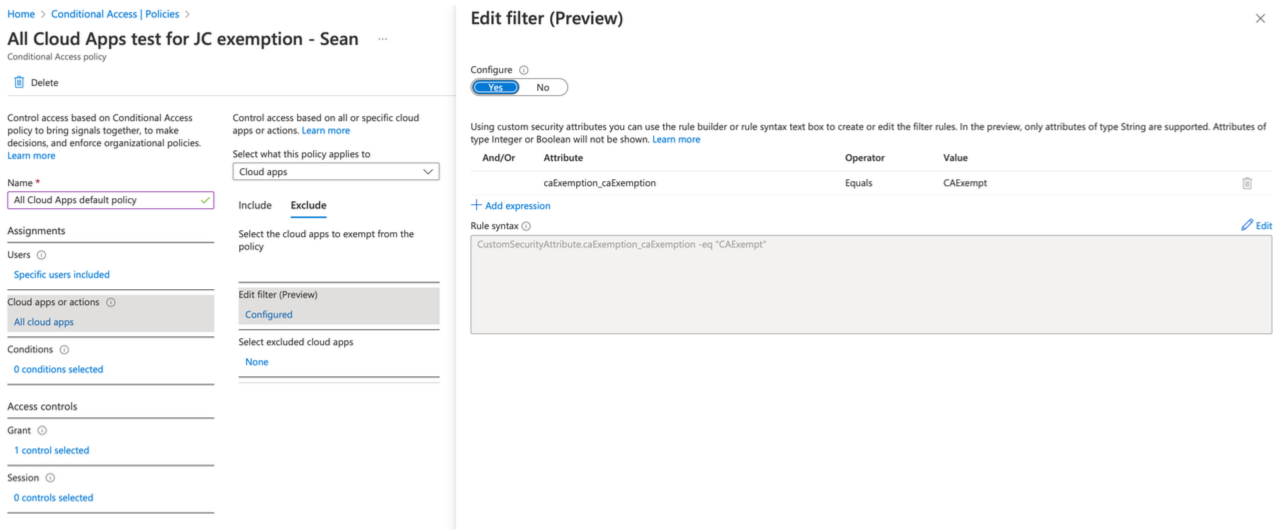
Include | Exclude

○ None
● All cloud apps
○ Select apps

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

When a policy is applied to “All cloud apps,” any login request using the `openid` scope will also be included in this policy. By adding an Exclude policy, we will eliminate the need for MFA and errors in logs for the ROPG portion of the Jamf Connect application.

Select the policy and select the section “Cloud apps or actions”. Select the option “Cloud apps” for the pulldown option “Select what this policy applies to”. Select the tab for “Exclude”



Home > Conditional Access | Policies >

All Cloud Apps test for JC exemption - Sean ···

Conditional Access policy

Delete

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

Name *

All Cloud Apps default policy

Assignments

Users: Specific users included

Cloud apps or actions: All cloud apps

Conditions: 0 conditions selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to: Cloud apps

Include | Exclude

Select the cloud apps to exempt from the policy

Edit filter (Preview): Configured

Select excluded cloud apps: None

Edit filter (Preview)

Configure: [✓ Yes] No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. Learn more

And/Or	Attribute	Operator	Value
	caExemption_caExemption	Equals	CAExempt

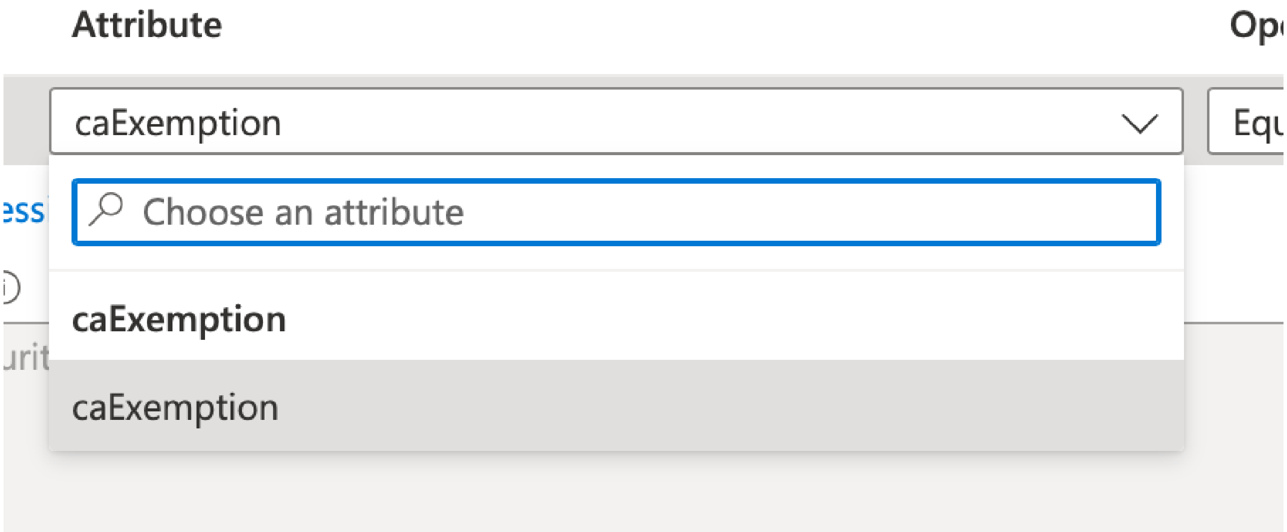
+ Add expression

Rule syntax

```
CustomSecurityAttribute.caExemption_caExemption -eq "CAExempt"
```

Edit

Select the option for “Edit filter (Preview)” and a new slideout window will appear. Select the option for “Configure” to “Yes”. In the Attribute column, select the custom security attribute you created to exempt an app from multi-factor authentication.



Attribute: caExemption

Op

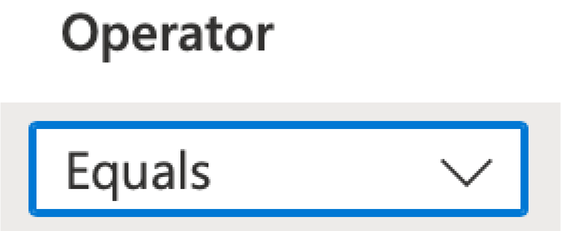
Equ

Choose an attribute

caExemption

caExemption

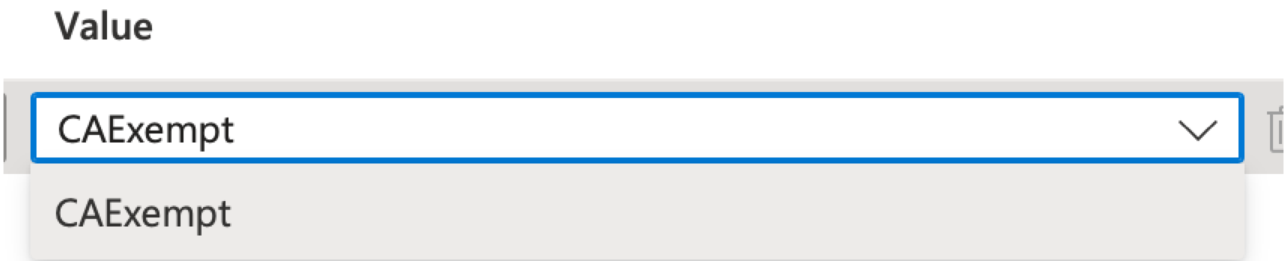
In the Operator column, select “Equals”.



Operator

Equals

In the Value column, select your attribute that marks an application as exempt from MFA.



Value

CAExempt

CAExempt

Select the “Done” option to close the slideout for Edit filter. Select the “Save” button to save the conditional access policy.

Repeat this process for any conditional access policy with “All cloud apps” as a target.

Step Six: Create a Jamf Connect Configuration Profile

Use the Jamf Connect Configuration app included in the Jamf Connect software distribution disk image which you can download from account.jamf.com with your Jamf Nation credentials.

On the Identity Provider tab, set:

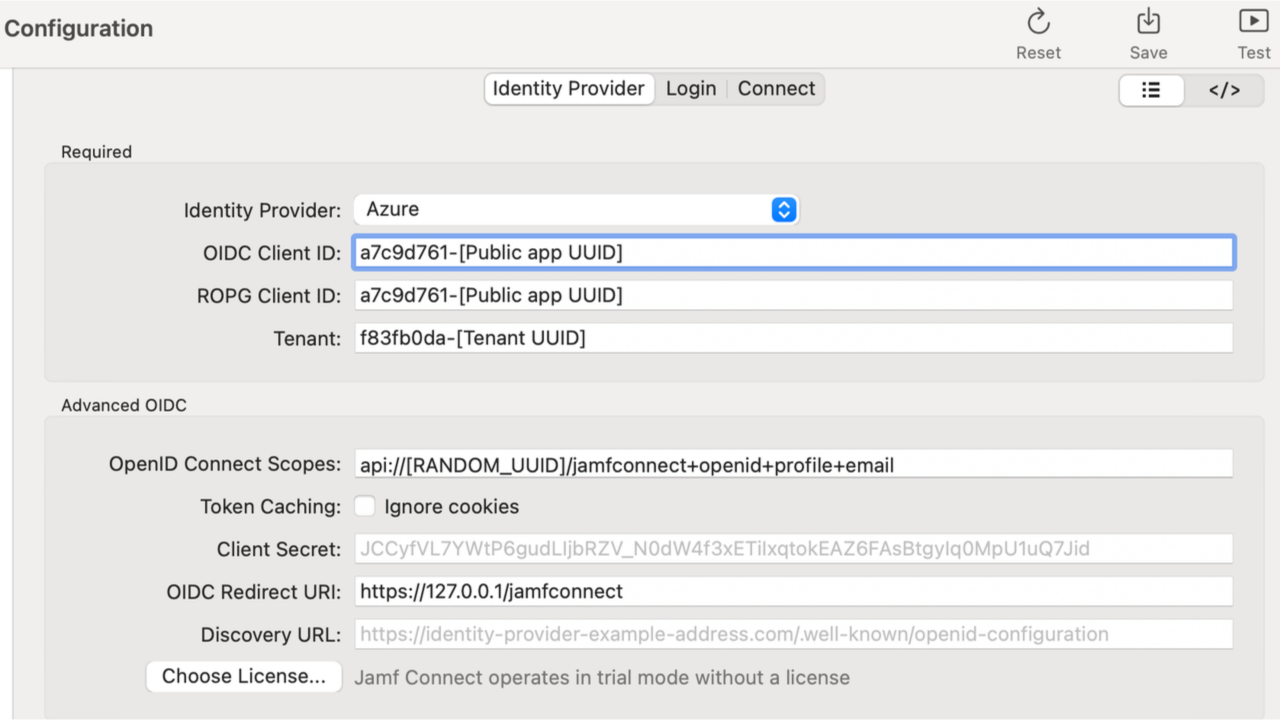
- Identity Provider: Azure
- OIDC Client ID: The application ID of the PUBLIC application you created in Step Two
- ROPG Client ID: The same application ID

- Scopes: Combine the scope you saved in Step One with `+openid+profile+email` to look similar to: `api://[RANDOM UUID STRING]/jamfconnect+openid+profile+email`
- Tenant: Enter the UUID of the tenant of your Azure instance. This can be found under the "Overview" tab of either of the App registrations made in Step One or Step Two.
- OIDC Redirect URI: (optional) Set to `https://127.0.0.1/jamfconnect`
- ROPGScopes: Set to `openid+email+profile`

Note: The following step is required for Jamf Connect version 2.17. Greater versions will have the ROPGScopes key in the GUI.

The configuration profile will need to be manually edited to include the following keys:

```
<key>ROPGScopes</key>
<string>openid+email+profile</string>
```



Configuration

Required

Identity Provider: Azure

OIDC Client ID: a7c9d761-[Public app UUID]

ROPG Client ID: a7c9d761-[Public app UUID]

Tenant: f83fb0da-[Tenant UUID]

Advanced OIDC

OpenID Connect Scopes: api://[RANDOM_UUID]/jamfconnect+openid+profile+email

Token Caching: □ Ignore cookies

Client Secret: JCCyfVL7YWtP6gudLljbRZV_N0dW4f3xETilxqtokEAZ6FAsBtgylq0MpU1uQ7Jid

OIDC Redirect URI: https://127.0.0.1/jamfconnect

Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration

Choose License... Jamf Connect operates in trial mode without a license

OPTIONAL: If you want to define a role for users to be made administrators on a macOS client device, on the Login tab, set:

- User Creation → Admin Roles: The value of the administrator App role you created in Step Two
- User Creation → Admin Attribute: `roles`

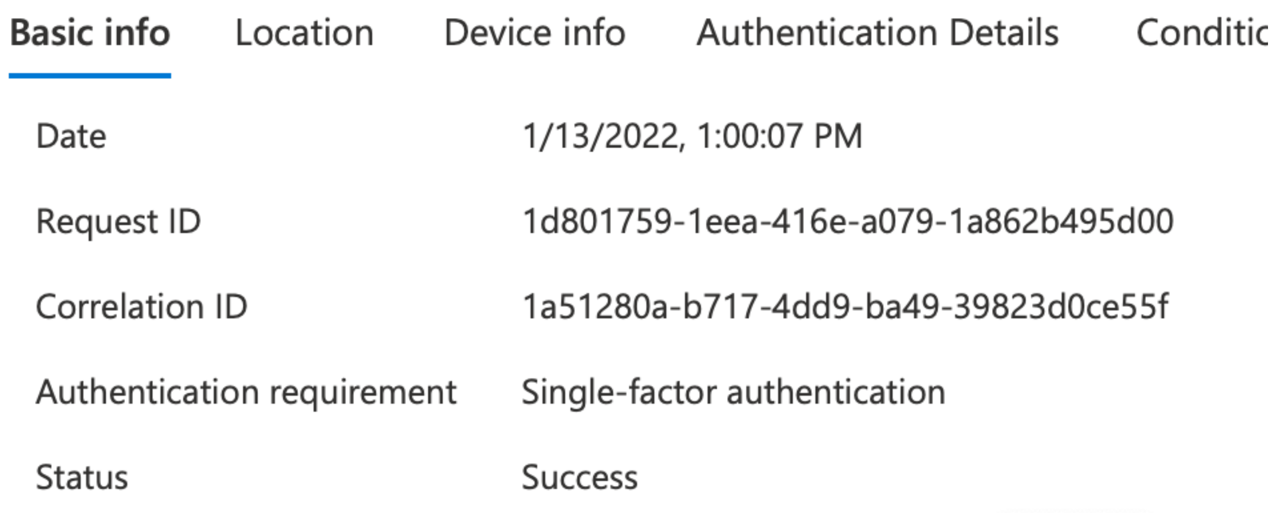
On the Connect tab, set:

- Authentication
  - ROPG Client ID: This should auto populate from your entry on the Identity Provider screen
  - ROPG Tenant: The UUID of the Azure tenant
  - ROPG Scopes: Set value to `openid+email+profile`

Test your configuration with the test user via OIDC. Make sure MFA was required. Validate the login in the Azure portal under Azure Active Directory → Sign-in logs. Note that there is a delay of 5-15 minutes between sign-in and the logs updating. Look for the Authentication Requirement to be “Multi-factor authentication”.

Testing ROPG will require installing the configuration on a non-production test machine. Save the Jamf Connect menu bar configuration as a .mobileconfig on a non-production test machine. Install the .mobileconfig manually into System Preferences. Install the JamfConnect.pkg from the Jamf Connect software distribution image (DMG). Log in to the Jamf Connect menu bar.

Validate in the Azure portal under Azure Active Directory → Sign-in logs that the authentication was successful. Look for the Authentication Requirement to be “Single-factor authentication”. The Basic tab will show something like:



Date	1/13/2022, 1:00:07 PM
Request ID	1d801759-1eea-416e-a079-1a862b495d00
Correlation ID	1a51280a-b717-4dd9-ba49-39823d0ce55f
Authentication requirement	Single-factor authentication
Status	Success

The Conditional Access tab should show that no policy was applied to the login.