

Creating a Custom Scope for Jamf Connect and Conditional Access policies

Change log:

24 AUG 2022 - Initial release. See notes of minimum system requirements for minimum version of Jamf Connect to use for these instructions.

25 AUG 2022 - Added additional screen shot to enable ROPG in public client app. Mirrors instructions in official documentation.

30 AUG 2022 - Fixed ROPG instructions - Allow public client flows needs to be enabled on the public application. Thank you, Paul Smith.

Workflow overview:

- Create a “private endpoint” application registration with a custom API
 - With API permissions for “User.read”
 - With “Expose an API” scope created
 - Define roles like “Admin” and “Standard” for elevating macOS account permissions
- 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
- Create an Azure Conditional Access policy to require multifactor authentication
 - Apply to application created in first step
- Remove any CA policy applied to “All cloud apps” that would require MFA
- Create a Jamf Connect Login configuration profile
 - Azure as Identity Provider
 - Define a custom scope
 - Define the Discovery URL for OIDC and ROPG
 - Test with Jamf Connect Configuration

Minimum system requirements

These instructions were written assuming you are using Jamf Connect version 2.14 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 something like “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.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [jamfse.io](#) >

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](#) ↗

Register

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

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

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](#)

+ Add a permission ☒ Grant admin consent for [redacted]

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

Search (Cmd+/) Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API**
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Set the App ID URI

Application ID URI

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

Save Discard

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	

Select the option for "Add a scope"

Conditional Access Policy API

Conditional 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 *

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

Who can consent?

☐ Admins and users ☒ Admins only

Admin consent display name *

Admin consent description *

User consent display name *

User consent description *

State

☒ Enabled ☐ Disabled

Set the scope name to `jamfconnect`. Set "Who can consent" to "Admins". 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 *

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

Who can consent?

☒ Admins and users ☐ Admins only

Admin consent display name *

Admin consent description *

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

[Add scope](#)[Cancel](#)

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

Step Two: Create an application registration using this new API permission

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](#) ↗

Register

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.)

Microsoft Azure

Home > jamfse.io | App registrations > Jamf Connect - Public OIDC for Conditional Access

Jamf Connect - Public OIDC for Conditional Access | Authentication

Search (Cmd+/) Got feedback? Add a platform

Overview Quickstart Docs

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

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)
- ☐ msalbf44d07-1930-4f06-96f6-3c8a3da3a0cc://auth (MSAL only)
- ☐ https://127.0.0.1/jamfconnect

Add URI

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)

[Help me decide...](#)

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. (The “public” app with the defaults scope of `openid` will still be used by the ROPG process to validate a user’s password, thus user.read permissions are required.)

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

Microsoft APIs

APIs my organization uses

My APIs

Applications that expose permissions are shown below

Name	Application (client) ID
Jamf Setup - Retail	3c272147- <div></div>
Jamf Connect - Conditional Access Policy API	66b2a554- <div></div>
Jamf Connect - INFOSEC ONLY ACCESS	b92961e0- <div></div>

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.

Request API permissions

[← All APIs](#)**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

[expand all](#)

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

[Add permissions](#)[Discard](#)

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/jamf-connect/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-

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.

H3: Step Three: Create an Azure Conditional Access policy

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

[Home](#) > [Conditional Access](#)

Conditional Access | Policies

Azure Active Directory

[+ New policy](#) ▾[What If](#)[Refresh](#)[Overview \(Preview\)](#)[Policies](#)[Insights and reporting](#)[Diagnose and solve problems](#)[Create new policy](#)[Create new policy from templates \(Preview\)](#)[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.

Create

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 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

- ☐ JC Jamf Connect - Conditional Access Policy API
- ☐ JC
- ☐ JC

Selected items

Select "Grant". Check the option for "Require multi-factor authentication". Set Enable policy to "On" and "Create" to save the policy.

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 Four: Remove any Conditional Access policies applied to All cloud apps

Preferred method

Navigate to portal.azure.com → Azure Conditional Access. Examine any application applied to the scope of “All cloud apps”. Either set “Enable policy” to “Off” for any application that has a Grant of “Require multi-factor authentication” or modify the “Cloud apps or actions” to specifically list resources that should have MFA applied.

Applying a policy to require MFA for “All cloud apps” will cause the ROPG application in the next step to inaccurately show failed logins in the Azure sign-in logs.

Alternative method

WARNING: Contains undocumented behavior, subject to change by Microsoft at any time. If you wish to keep “All cloud apps” as a definition, but you still want the policy to not be applied to the `openid` scope, create an unused Enterprise app registration for an unused SAML application, and then use that bogus app registration as an “Exclude” to the “All cloud apps” policy:

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 *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions 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

Select excluded cloud apps

[Microsoft Planner](#)



Microsoft Planner

09abbdfd-ed23-44ee-a2d9-a627aa1c90f3



This is undocumented behavior, but the application of an exclusion to the policy will break how the policy is applied to `openid` scope. As this is undocumented, the behavior may be unexpected and may change by Microsoft without notice.

Step Five: 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`

The screenshot shows the 'Configuration' window for Jamf Connect. It has tabs for 'Identity Provider', 'Login', and 'Connect'. The 'Identity Provider' tab is active. Below the tabs, there are sections for 'Required' and 'Advanced OIDC' settings.

Required Section:

- Identity Provider: Azure (dropdown menu)
- OIDC Client ID: a7c9d761-[Public app UUID]
- ROPG Client ID: a7c9d761-[Public app UUID]
- Tenant: f83fb0da-[Tenant UUID]

Advanced OIDC Section:

- OpenID Connect Scopes: api://[RANDOM_UUID]/jamfconnect+openid+profile+email
- Token Caching: ☐ Ignore cookies
- Client Secret: JCCyfVL7YWtP6gudLjBZRZV_N0dW4f3xETilxqtokEAZ6FAsBtgyIq0MpU1uQ7Jid
- OIDC Redirect URI: https://127.0.0.1/jamfconnect
- Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration

At the bottom, there is a 'Choose License...' button and a message: '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.

Test your configuration with the test user via ROPG. 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:

Basic info	Location	Device info	Authentication Details	Conditio
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.

Note: Administrators will still see a single MFA failure immediately after a user logs in using the Jamf Connect login window. As of Jamf Connect 2.14, the login window will use the scopes defined in the `OIDCScopes` key which will trigger the need for MFA for the ROPG process. This behavior is expected and harmless.

Copyright and Trademarks

© Copyright 2002-2022 Jamf. All rights reserved.

Jamf has made all efforts to ensure that this guide is accurate.

Jamf

100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of Jamf.

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, Jamf, the Jamf Logo, JAMF SOFTWARE®, the JAMF SOFTWARE Logo®, RECON®, and the RECON Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

Apple, the Apple logo, Apple Configurator 2, Apple Remote Desktop, Apple TV, AirPlay, Finder, FileVault, FireWire, iBeacon, iBooks, iPad, iPhone, iPod touch, iTunes, Keychain, Mac, MacBook, MacBook Pro, MacBook Air, macOS, OS X, and Safari are trademarks of Apple Inc., registered in the United States and other countries. AppleCare, App Store, iBooks Store, iCloud, and iTunes Store are service marks of Apple Inc., registered in the United States and other countries.

Microsoft, Microsoft Edge, Microsoft Intune, Active Directory, Azure, Excel, OneNote, Outlook, PowerPoint, Silverlight, Windows, Windows Server, and all references to Microsoft software are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.