3 - Use Custom Security Attributes to apply an exception policy for Azure Conditional Access for Jamf Connect

Overview

Because the Jamf Connect app registration in Microsoft Azure Active Directory is designed to be a “desktop/mobile” application, it does not normally appear in the list of applications that can be exempted from an Azure Active Directory Conditional Access policy.

In this article, we will use the Jamf Connect app as an example, however these steps can be used for any application registration in Microsoft Azure Active Directory.

By applying a Custom Security Attribute to the Jamf Connect app, we can use the Filters option to exempt Jamf Connect from Azure Active Directory Conditional Access policies.

When would you exempt Jamf Connect from Conditional Access policies

Jamf Connect is designed to create user accounts on individual client macOS devices, manage the access rights on that client, and keep that local user account password in sync with a cloud identity provider (IdP) password.

Microsoft Azure Active Directory Conditional Access policies can cause conflicts with the needs of an individual client computer versus a cloud resource. For example, a restriction to log into Jamf Connect on a device marked non-compliant may result in the user being locked out of the device and unable to get the device back into a compliant state by updating an operating system, applying a patch to installed software, or simply getting a user account password back in sync with the IdP.

Conditional Access policies that may cause issues with Jamf Connect

- Locations outside of a private network
- Enforcing device registration in Azure Active Directory
- Requiring multi-factor authentication for All cloud apps*
- Restricting logins to specific browser types

*Note: When Jamf Connect evaluates the user's local account password against the identity provider password, it uses a Resource Owner Password Grant (ROPG) non-interactive login against the identity provider. An ROPG authentication, being non-interactive, is unable to prompt the user to complete an MFA challenge and response. If MFA is required, the sign-in logs for that app will show "failure" when the MFA challenge is not completed. Exempting Jamf Connect from the MFA requirement will prevent these failures from appearing in logs and affecting the user risk score.

Procedure

- Create a custom security attribute in Microsoft Azure Active Directory
- Apply the custom security attribute to the Jamf Connect enterprise app registration
- Modify the Microsoft Azure Conditional Access policy to add an exemption to any app assigned with the custom security attribute

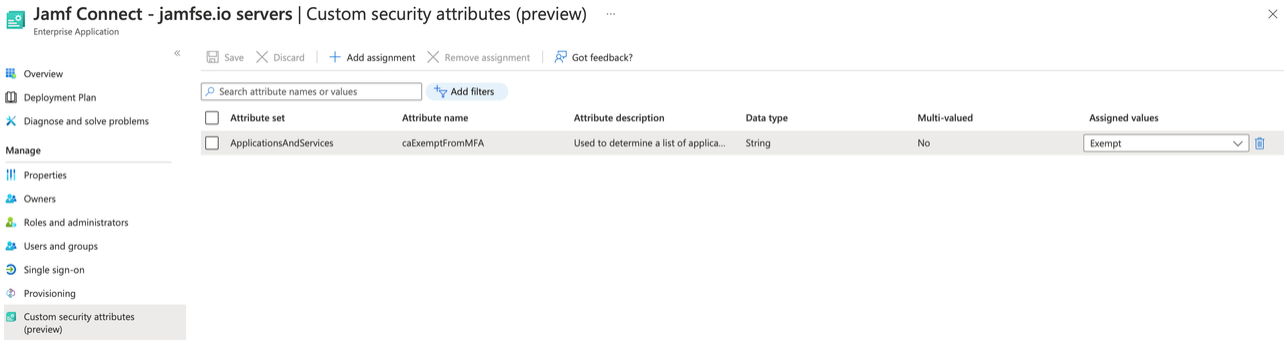
Create a custom security attribute

Follow the instructions in "https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/2_-_Creating_Custom_Security_Attributes_in_Microso.pdf" to create an attribute to assign to apps as exempt from a multi-factor authentication policy.

Apply the custom security attribute to Jamf Connect

Navigate to Azure Active Directory → Enterprise applications and find the name of the Jamf Connect application. Under the "Manage" section in the left hand toolbar,

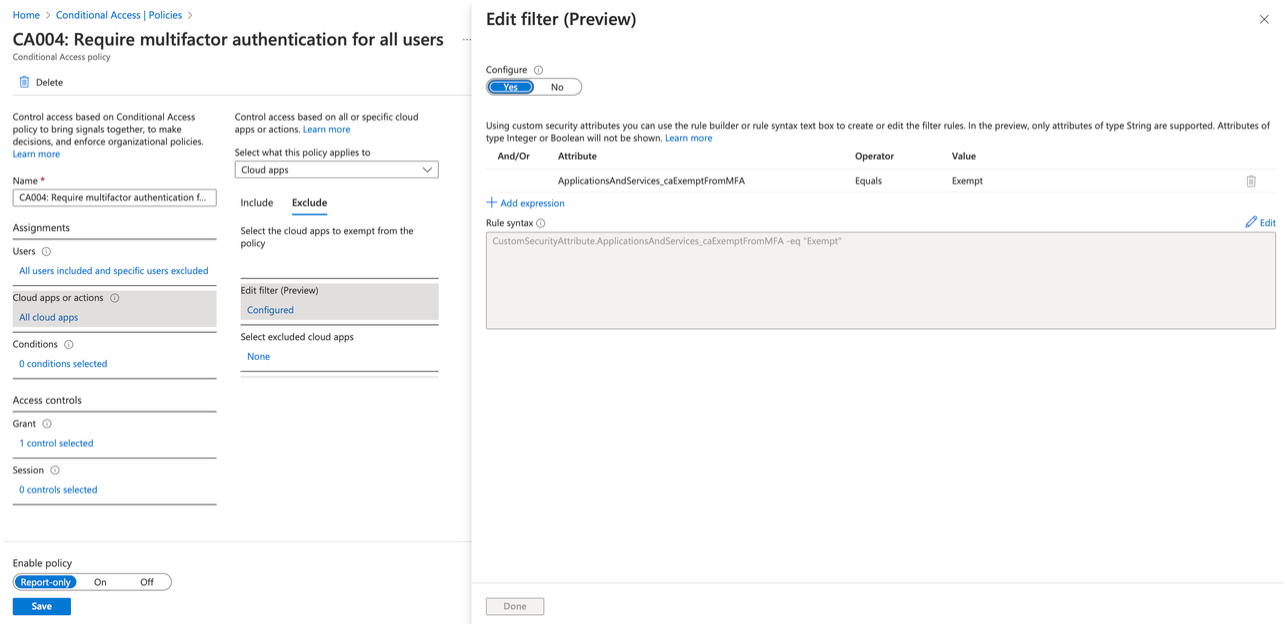
select the option for “Custom security attributes (Preview)”. Use the “+ Add assignment” button to assign the security attribute to be exempt from MFA to the Enterprise app. Select the “Save” option to save the assignment.



For more information, refer to [INSERT LINK FOR BLOG ARTICLE AT LATER TIME WHEN POSTED].

Add an exemption to a conditional access policy

Navigate to Azure Conditional Access → Policies. Find the name of your policy that applies a requirement for Mutlifactor authentication.



Under “Assignments,” find the section for “Cloud apps or actions.” Select the Exclude tab and the option to configure a “Edit filter (preview).” Select “Configure” to Yes, and add the attribute that marks applications exempt from multi-factor authentication policies. Select “Done” to save the filter and the “Save” option to save the conditional access policy.

Note: Use the “Report-only” option to test that the policy is exempted properly before enforcing the policy.

Testing the exemption

First, wait about 5-15 minutes after creating or modifying the Azure Conditional Access policy before testing. Changes to policies take some time to propagate through the cloud identity provider service.

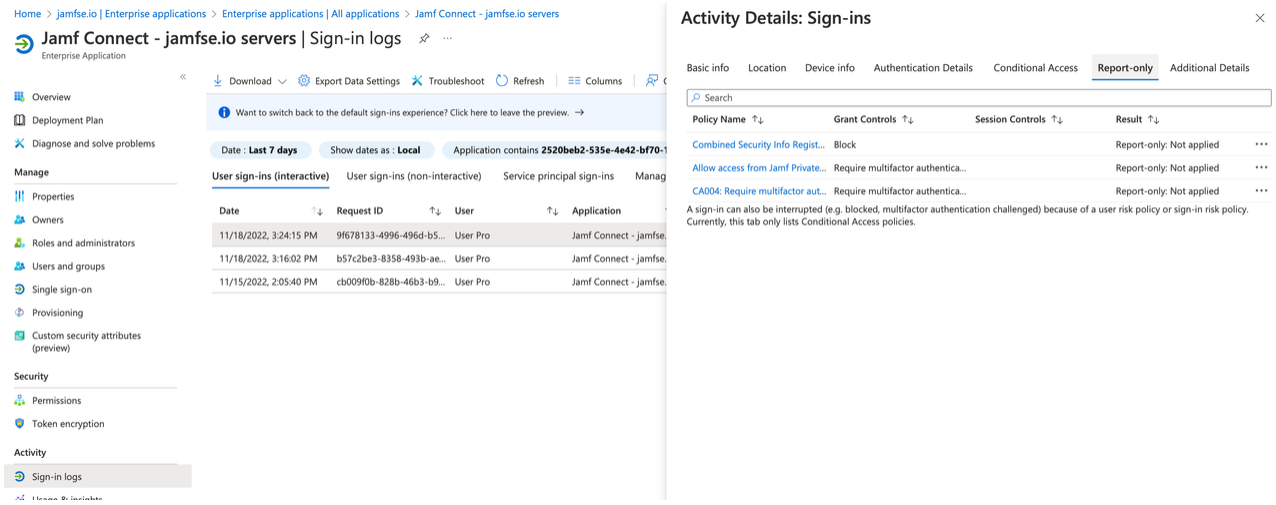
Next, use one of the following methods to log into the Jamf Connect application:

- Preferred - Jamf Connect Configuration - use the Test → ROPG button to test the password validation
- Jamf Connect menu bar application - Use the “Connect...” option to test the password validation

The following methods work but are not recommended as you may lock a user out of a client device without proper configuration:

- On a **NON-PRODUCTION** test machine, Jamf Connect login - Open the Terminal app and use the following command to trigger a login `security authorize -u system.login.console`
- On a **NON-PRODUCTION** test machine, Jamf Connect login - Use the → Sign out command and sign in as a test user.

After a successful login, wait about 2-5 minutes for sign-in logs to propagate through the Azure AD cloud service. Navigate to Azure Active Directory → Enterprise applications and search for the name of your Jamf Connect app. Use the Sign-in logs to examine the details of the authentication.



In the Activity Details: Sign-ins popup that opens when you select a specific authentication attempt, select the “Report-only” tab and verify that your conditional access policy result is “Not applied”.