1 - Azure Conditional Access and All cloud apps

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#all-cloud-apps

What is Azure Conditional Access

Part of Microsoft Entra, Conditional Access policies add additional rules to apply to login authentication requests for applications that use Microsoft Azure Active Directory single sign-on services to gate access to resources. These rules could be used to allow or deny access to groups of users based on location, device state, user risk, etc. or to require additional authentication requirements like using a multi-factor based authentication method.

All cloud apps

Applying a Conditional Access policy to **All cloud apps** will result in the policy being enforced for all tokens issued to web sites and services. This option includes applications that aren't individually targetable in Conditional Access policy, such as Azure Active Directory.

In some cases, an All cloud apps policy could inadvertently block user access. These cases are excluded from policy enforcement and include:

- Services required to achieve the desired security posture. For example, device enrollment calls are excluded from compliant device policy targeted to All cloud apps.
- Calls to Azure AD Graph and MS Graph, to access user profile, group membership and relationship information that is commonly used by applications excluded from policy. The excluded scopes are listed here: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#all-cloud-apps

To exempt the above policies from an inadvertent block, at least one application must be exempted from the “All cloud apps” policy, either explicitly or via an app

filter.

Jamf Connect and “All cloud apps”

Jamf Connect uses Microsoft Graph via login to Azure Active Directory with the scope of “openid profile email”. To avoid an inadvertent application of conditional access policies to Jamf Connect, at least one application must be exempted from the “All cloud apps” policy, either explicitly or via an app filter. Administrators are recommended to use the Custom Security Attribute (Preview) feature to create a custom security attribute, apply the attribute to the Jamf Connect application, and use the attribute as a filter to exclude the MFA requirement from any Conditional Access policy.

Related topics:

- https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/2_-_Creating_Custom_Security_Attributes_in_Microso.pdf
- https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/3_-_Use_Custom_Security_Attributes_to_apply_an_exc.pdf
- https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/4_-_Modifying_Jamf_Connect_to_apply_Azure_Conditio.pdf