MULTI FACTOR AUTHENTICATION SETTINGS FOR THE FUSION CONNECT MICROSOFT VOICE PORTAL

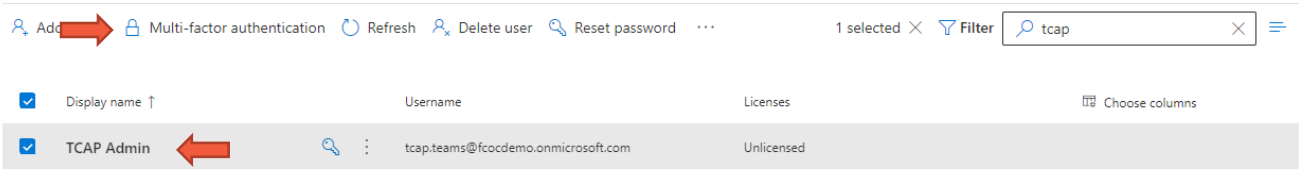
Document Summary

To ensure that the Fusion Connect Microsoft voice portal has access to your Microsoft 365 tenancy, we need to ensure that the portal's IP Addresses are excluded from your organizations Multifactor Authentication (MFA) policies.

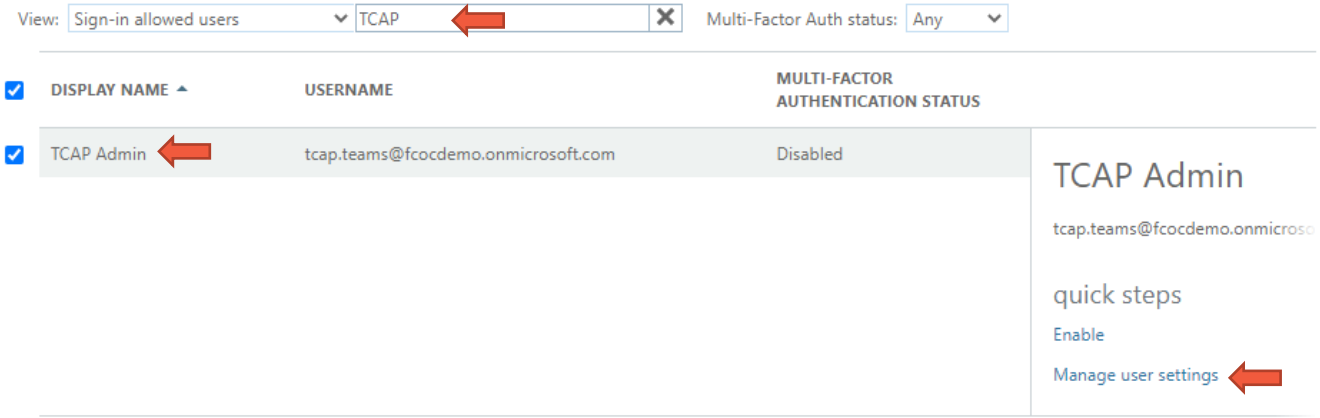
We do this in two main areas: Microsoft 365 settings and if you have Azure AD Premium, in a third policy-based area.

Microsoft 365 Portal

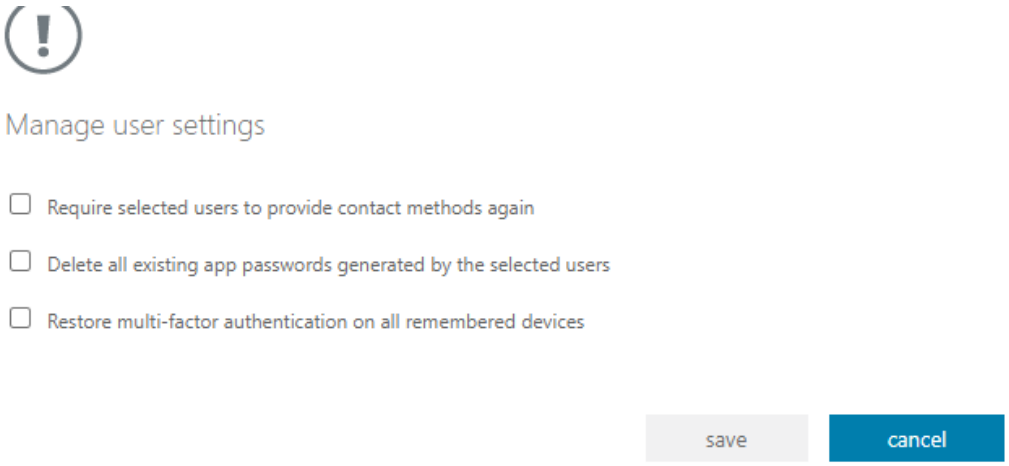
1. Login to your M365 Admin portal and go to Users > Active Users
2. Find the TCAP Admin user in your users list and click on Multi Factor Authentication Settings.



3. This will take you to the MFA auth settings section of Microsoft.



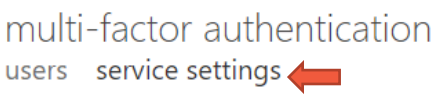
4. Search for the TCAP Admin user account and ensure the MFA status is set to Disabled. If it is not, disable it.



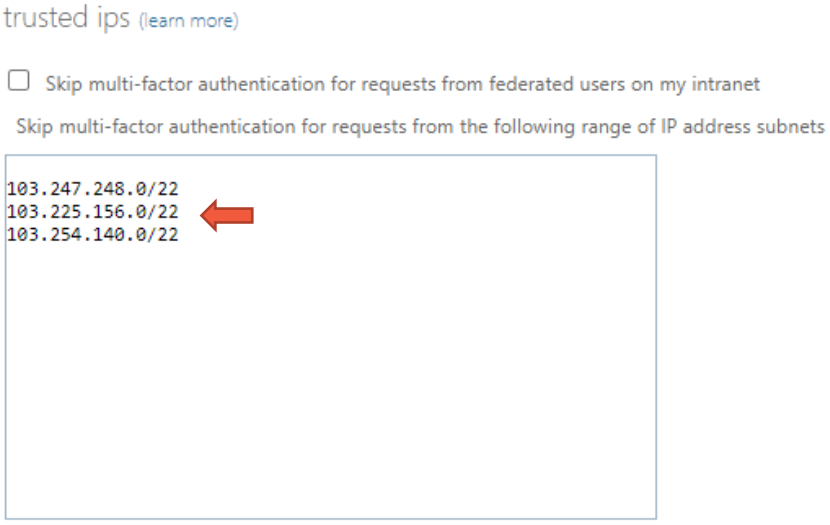
5. Add the following IP Ranges to the Whitelist IP's for Multi Factor Authentication. This will ensure all the portal worker engines and processes are excluded from M365 MFA.

a. An up-to-date list of exclude IP's is available at www.pingco.com.au/TCAP/IPRanges.txt

b. Click on Service Settings



c. Add the IP's from the above list in step (a) to the trusted IPs list



d. Click save

Azure AD Premium Users

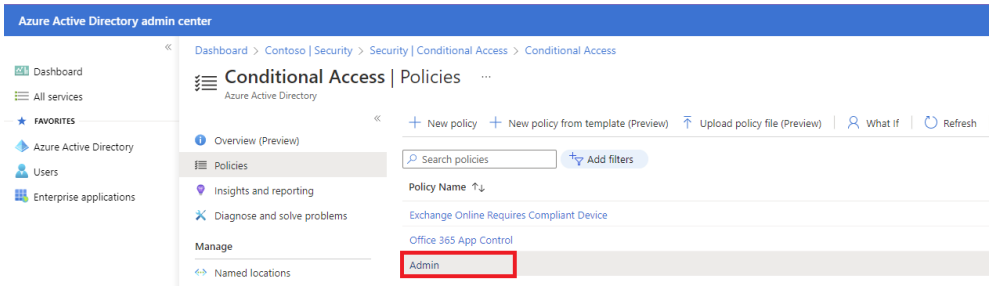
If you are using Azure AD premium, you will need to ensure that Conditional Access Policies are excluded for the TCAP Admin account.

From Azure portal under Azure Active Directory > Security > Conditional Access

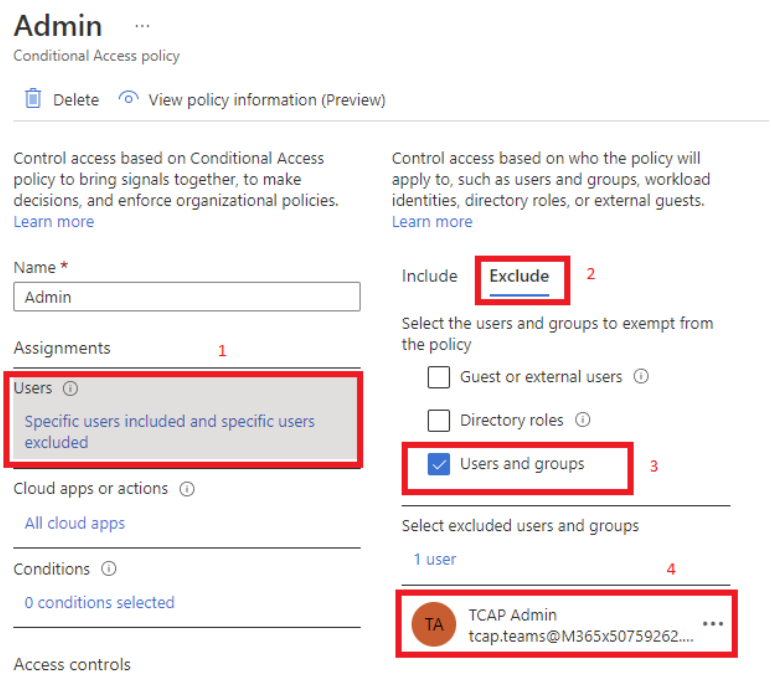
1. On every policy that you have existing, that requires Multi Factor Authentication, include the TCAP Admin account in the Excluded list.

2. Make sure you only modify existing policies, there is no need to create a new one.

3. Click on the existing policy you want to modify.



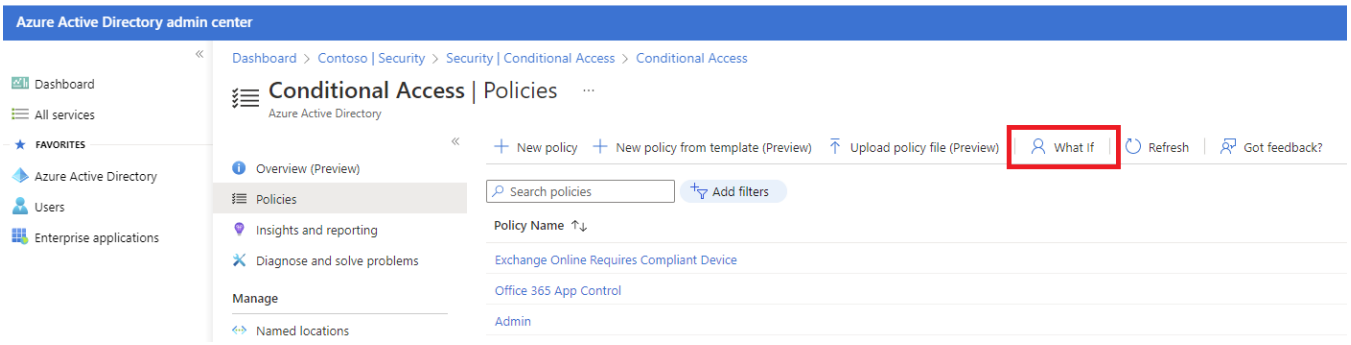
4. Click on the Specific users included then click on Exclude and select Users and groups, search for TCAP Admin in from the right pop-out bar then select TCAP admin user and save.



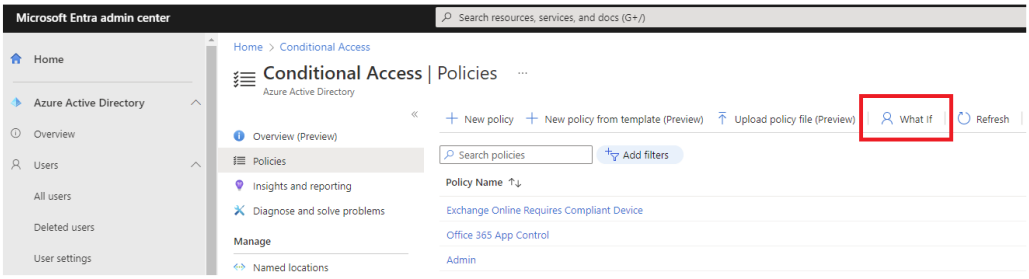
Troubleshooting Steps

Using What If tool to validate Conditional Access policies that is applied to a user.

From Azure portal under Azure Active Directory > Security > Conditional Access > What If.



From Microsoft Entra admin center under Azure Active Directory > Protect & Secure > Conditional Access



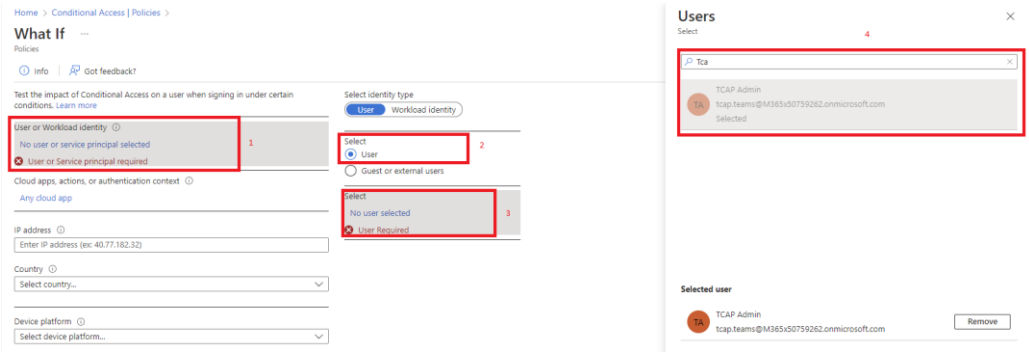
The only condition you must make is selecting a user or workload identity. All other conditions are optional.

Select the TCAP Admin user.

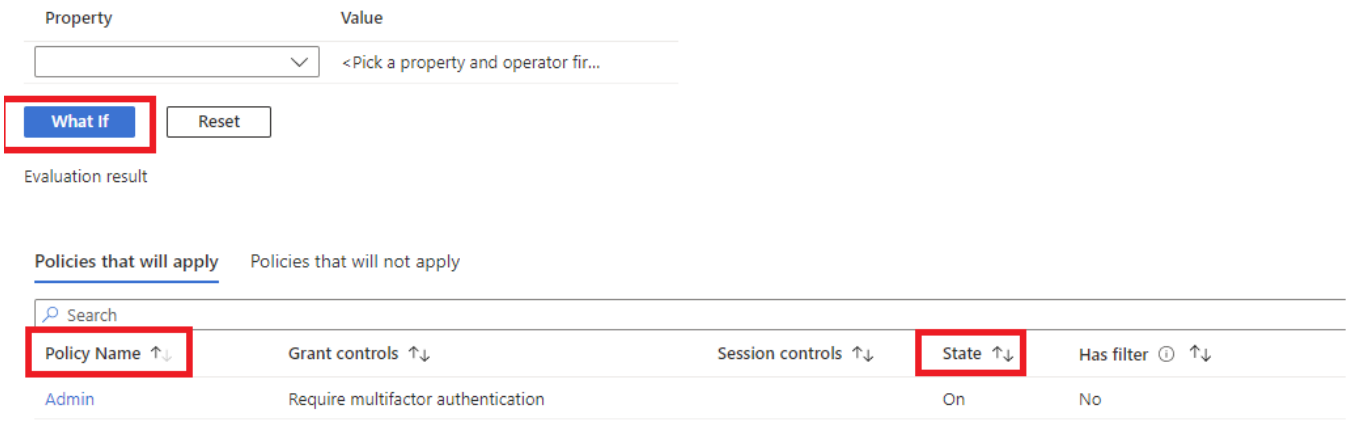
You can also make use of this IPs when testing:

103.247.248.0/22, 103.225.156.0/22, 103.254.140.0/22

Location: Australia



Scroll down and click on What If to evaluate the user.



The evaluation result provides you with a report that consists of:

- An indicator whether classic policies exist in your environment.
- Policies that will apply to your user or workload identity.
- Policies that don't apply to your user or workload identity.

Finally, if all settings are in place and MFA is still not being bypassed it may be required to perform the following:

1. Remove the TCAP Admin from any exemption policy
2. License the TCAP Admin user profile
3. Add back under exemption policy

The license may be removed after this, however isolated cases have been experienced in the past where the above may be necessary. Please allow up to 24 hours following any changes made to take effect.