MULTI FACTOR AUTHENTICATION SETTINGS IN THE FUSION CONNECT MICROSOFT VOICE PORTAL

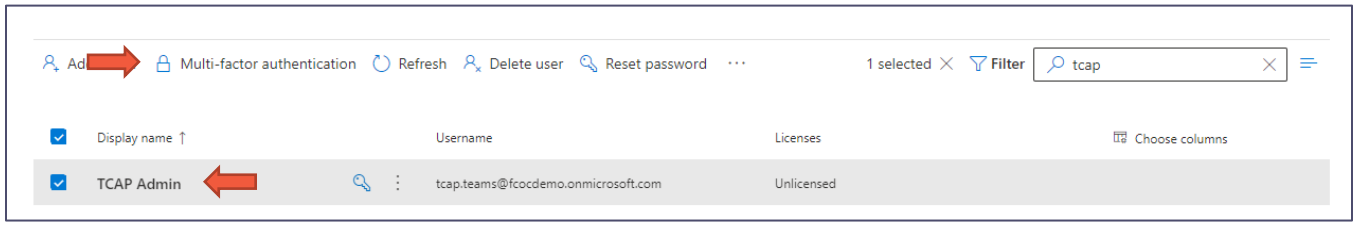
Document Summary

To ensure that the Teams Calling Automation Platform (TCAP) has access to your Microsoft 365 tenancy, we need to ensure that the TCAP platform IP Addresses are excluded from your organizations Multifactor Authentication (MFA) policies.

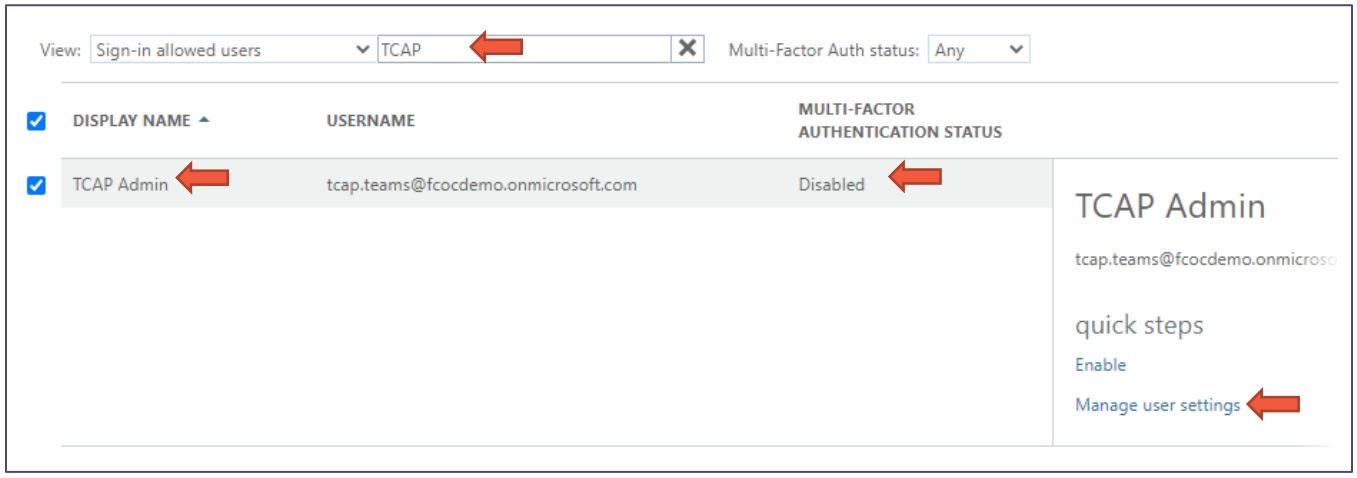
We do this in two main areas and - if you have Azure AD Premium - in a third policy-based area.
M365 Settings

Microsoft 365 Portal

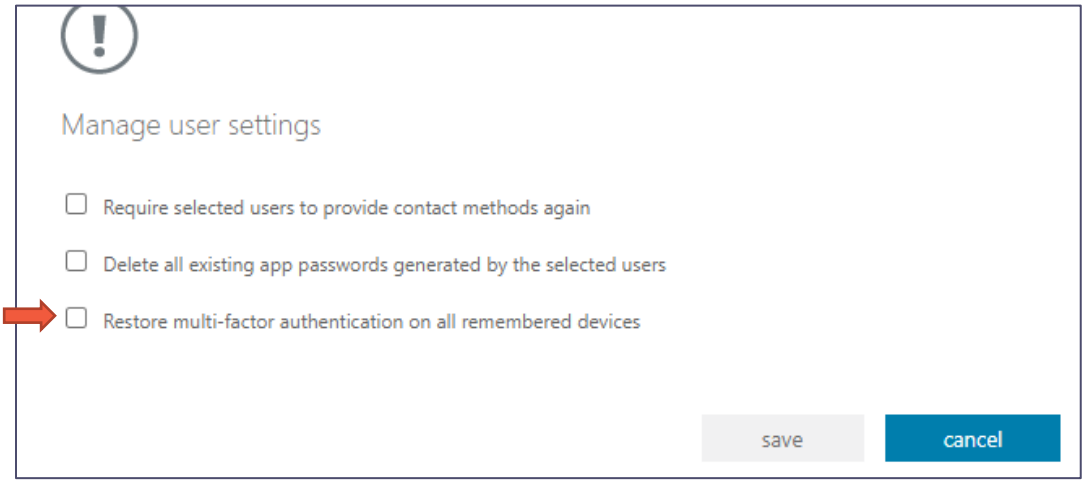
1. Login to your M365 Admin portal - https://admin.microsoft.com/
2. Find the ***TCAP admin*** user in your users list and click on ***Multi Factor Authentication*** **Settings**.



3. This will take you to the **MFA auth settings** section of Microsoft. Search for "***TCAP***" to find the ***TCAP Admin*** user. Ensure the MFA status is set to ***Disabled***. If it is not, disable it. To do this, Click on ***Manage user settings***.



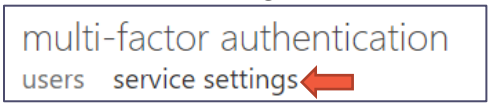
4. Remove the checkmark next to ***Restore multi-factor authentication on all remembered devices***, then Click ***Save***.



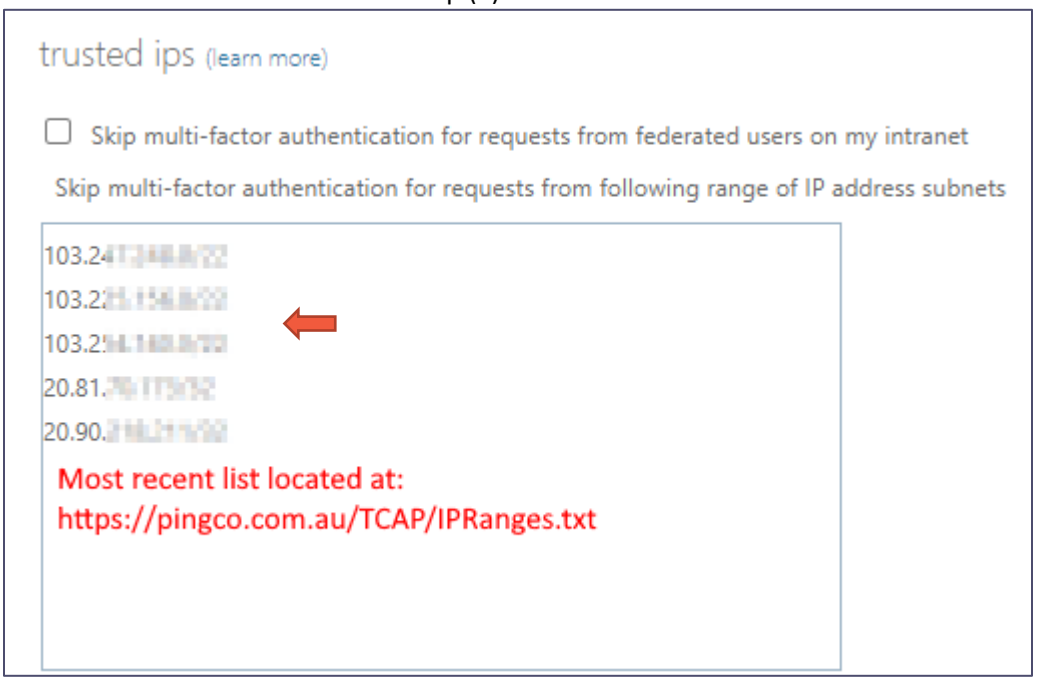
5. Add the following IP Ranges to the Whitelist IP's for Multi-Factor Authentication. This will ensure all the TCAP worker engines and processes are excluded from M365 MFA. This step requires Microsoft Entra ID P1 (formerly Azure Active Directory P2).

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

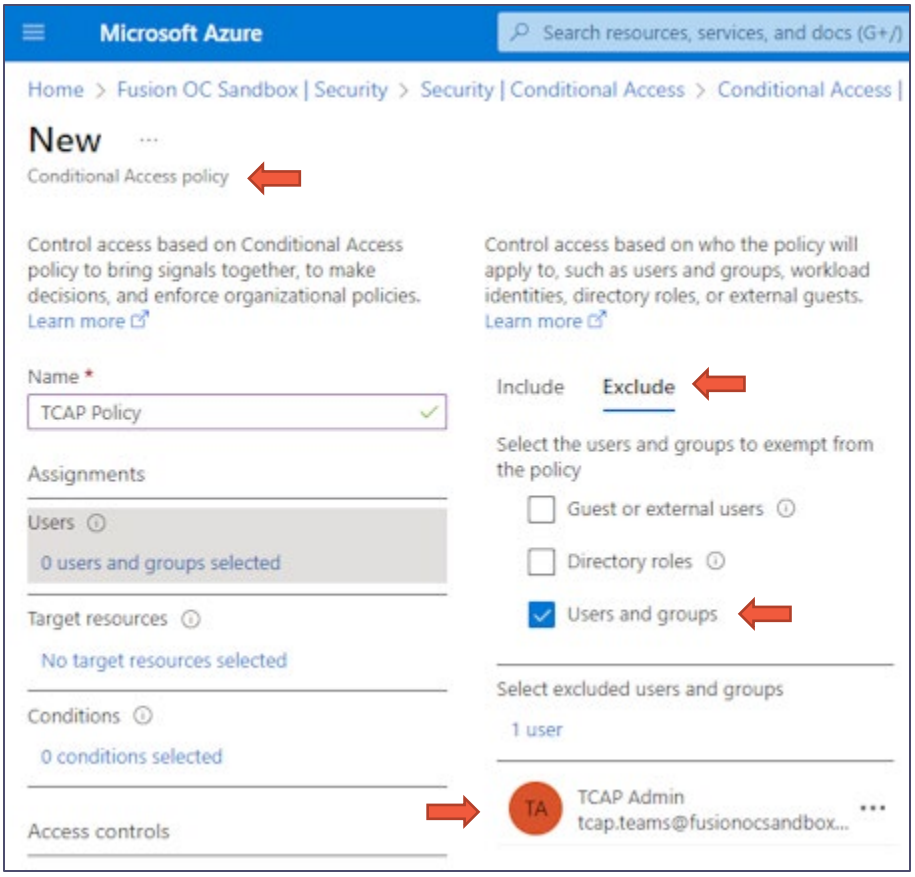


d. Click ***Save***.

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 account.

a. Ensure any policy that requires Multi Factor Authentication includes the TCAP account in the "**Exclude**" list.
b. Click ***Users and groups*** and specify the TCAP account for exclusion from every policy.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Fusion OC Sandbox | Security > Security | Conditional Access > 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 *
TCAP Policy
Assignments
Users
0 users and groups selected
Target resources
No target resources selected
Conditions
0 conditions selected
Access controls
Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
Learn more
Include
Exclude
Select the users and groups to exempt from the policy
Guest or external users
Directory roles
Users and groups
Select excluded users and groups
1 user
TA
TCAP Admin
tcap.teams@fusionocsandbox...