



MULTI FACTOR AUTHENTICATION SETTINGS IN THE FUSION CONNECT MICROSOFT VOICE PORTAL

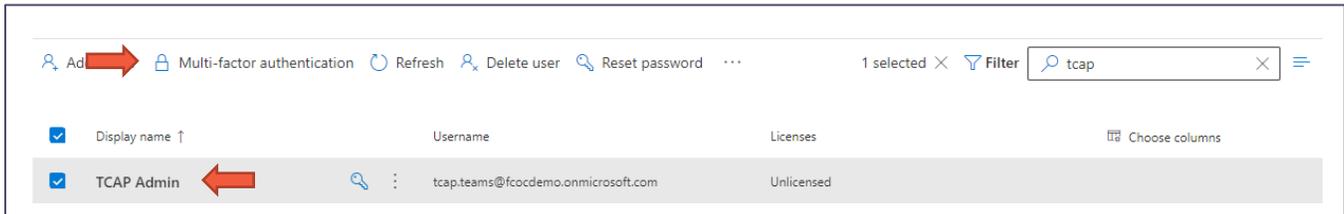
Document Summary

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.

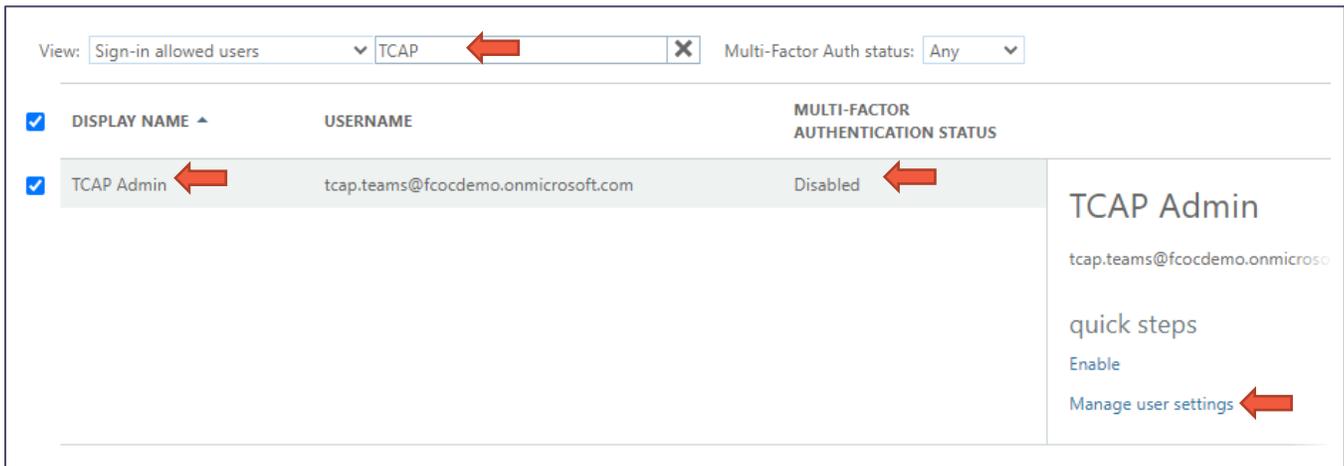
We do this in two main areas and - if you have Azure AD Premium - in a third policy-based area.
M365 Settings

Microsoft 365 Portal

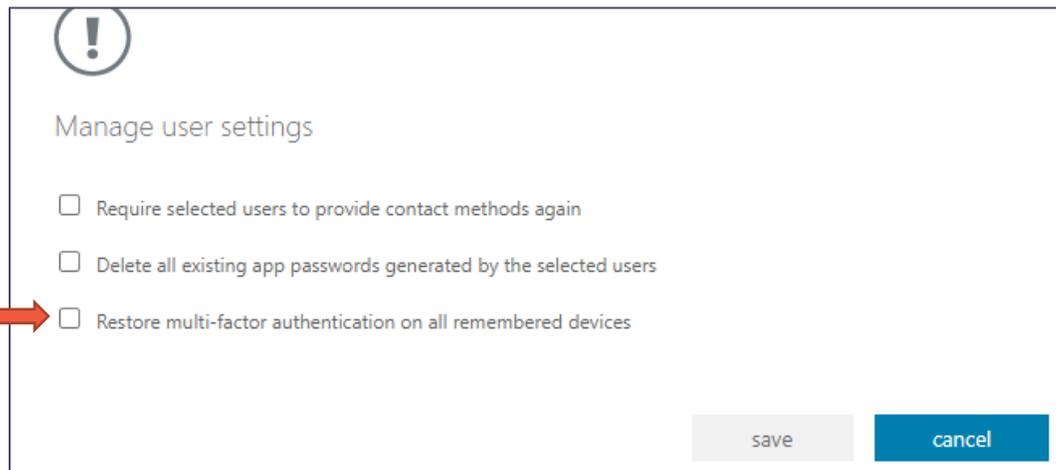
1. Login to your M365 Admin portal - <https://admin.microsoft.com/>
2. Find the **TCAP admin** user in your users list and click on **Multi Factor Authentication Settings**.



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

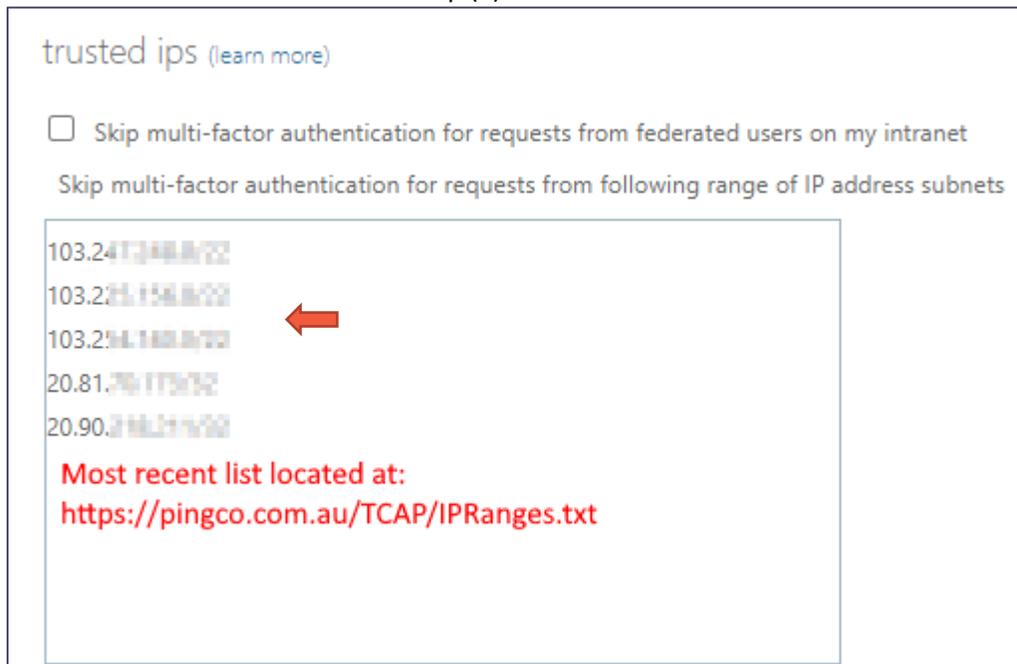
trusted ips ([learn more](#))

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

103.24.134.0/22
103.25.156.0/22
103.25.188.0/22
20.81.76.175/32
20.90.218.214/32

Most recent list located at:
<https://pingco.com.au/TCAP/IPRanges.txt>



- 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.

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

The screenshot shows the Microsoft Azure portal interface for creating a new Conditional Access policy. The breadcrumb navigation is: Home > Fusion OC Sandbox | Security > Security | Conditional Access > Conditional Access |. The page title is "New Conditional Access policy".

On the left side, there are several configuration sections:

- Name ***: A text input field containing "TCAP Policy" with a green checkmark.
- Assignments**: A section with a "Users" sub-section showing "0 users and groups selected".
- Target resources**: A section showing "No target resources selected".
- Conditions**: A section showing "0 conditions selected".
- Access controls**: A section with a red arrow pointing to the right.

On the right side, there are additional configuration options:

- Control access based on who the policy will apply to**: A section with a "Learn more" link.
- Include / Exclude**: Two radio buttons. The "Exclude" button is selected and has a red arrow pointing to it.
- Select the users and groups to exempt from the policy**: A list of options with checkboxes:
 - Guest or external users
 - Directory roles
 - Users and groups (has a red arrow pointing to it)
- Select excluded users and groups**: A section showing "1 user" selected, with a red circle icon and the text "TCAP Admin tcap.teams@fusionocsandbox...".