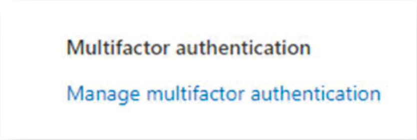
Multi-factor Authentication Settings for Teams Calling Automation Platform

To ensure that the Teams Calling Automation Platform has access to your Microsoft 365 tenancy, we need to ensure that the G12 platform IP Addresses are excluded from your organizations Multi-factor 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

1. Login to your M365 Admin portal

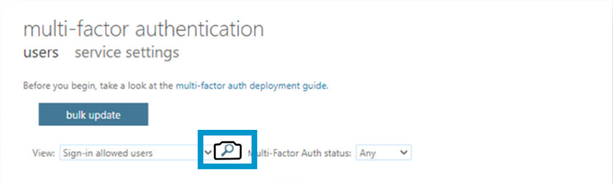
2. Find the G12 admin user in your users list and click on Multi-factor Authentication Settings.



Multifactor authentication

Manage multifactor authentication

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



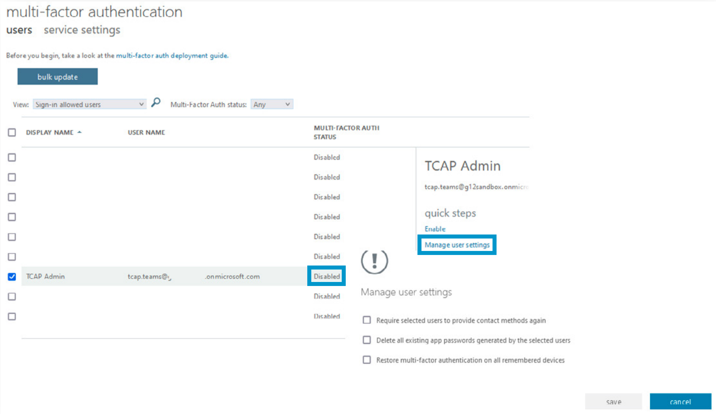
multi-factor authentication

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users

Multi-Factor Auth status: Any

4. Search for the G12 user account and ensure the MFA status is set to Disabled. If it is not, disable it.



multi-factor authentication

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users

Multi-Factor Auth status: Any

	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
□			Disabled
□			Disabled
□			Disabled
□			Disabled
□			Disabled
□			Disabled
☑	TCAP Admin	tcap.teams@ .onmicrosoft.com	Disabled
□			Disabled
□			Disabled

TCAP Admin

tcap.teams@g12sandbox.onmicr

Manage user settings

□ Require selected users to provide contact methods again

□ Delete all existing app passwords generated by the selected users

□ Restore multi-factor authentication on all remembered devices

G12
communications

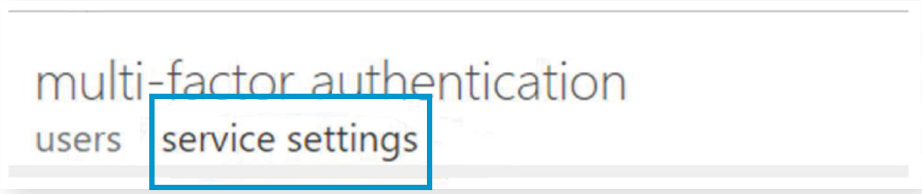
Multi-factor Authentication Settings for Teams Calling Automation Platform

5. Add the following IP Ranges to the Whitelist IP's for Multi-factor Authentication. This will ensure all the G12 worker engines and processes are excluded from M365 MFA.

a. Trusted IP Subnets to Add:

103.247.248.0/22
103.225.156.0/22
103.254.140.0/22

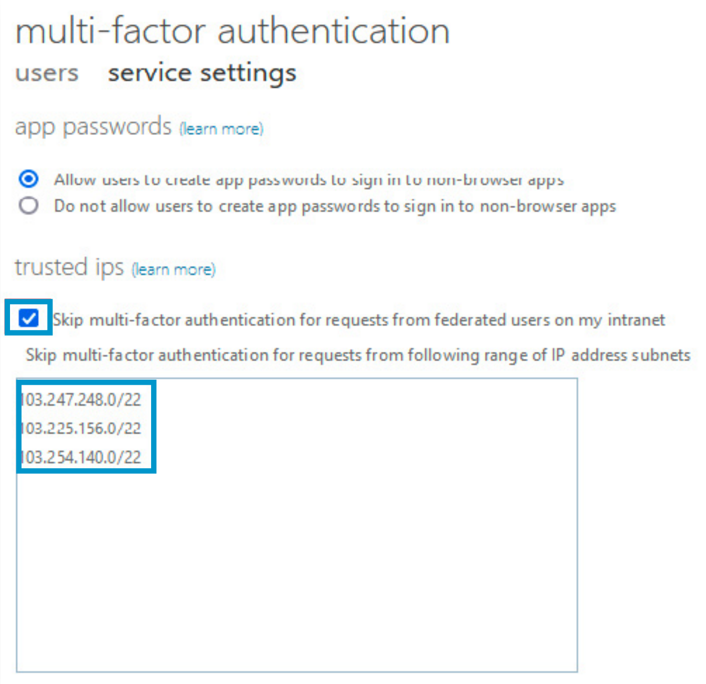
b. Click on Service Settings



multi-factor authentication

users service settings

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



multi-factor authentication

users **service settings**

app passwords (learn more)

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

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

```
103.247.248.0/22
103.225.156.0/22
103.254.140.0/22
```

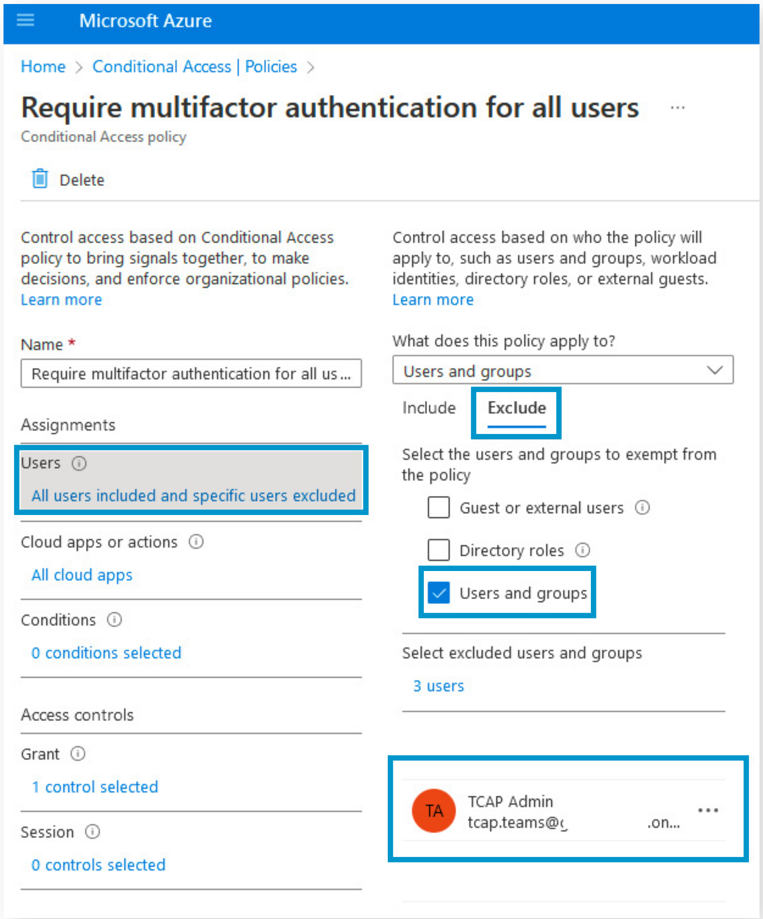
d. Click save

Multi-factor Authentication Settings for Teams Calling Automation Platform

Azure AD Premium Users

If you are using Azure AD premium, you will need to ensure that Conditional Access Policies are excluded for the G12 account.

e. Ensure any policy that requires Multi-factor Authentication includes the G12 account in the Excluded list



Microsoft Azure

Home > Conditional Access | Policies >

Require multifactor authentication for all users ...

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Require multifactor authentication for all us...

Assignments

Users ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

What does this policy apply to?

Users and groups

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

3 users

TA TCAP Admin
tcap.teams@[redacted].on... ...

f. Click Users and groups and specify the G12 account for exclusion from every policy.

G12 communications