Deploy multi-factor authentication to remote Microsoft Teams users

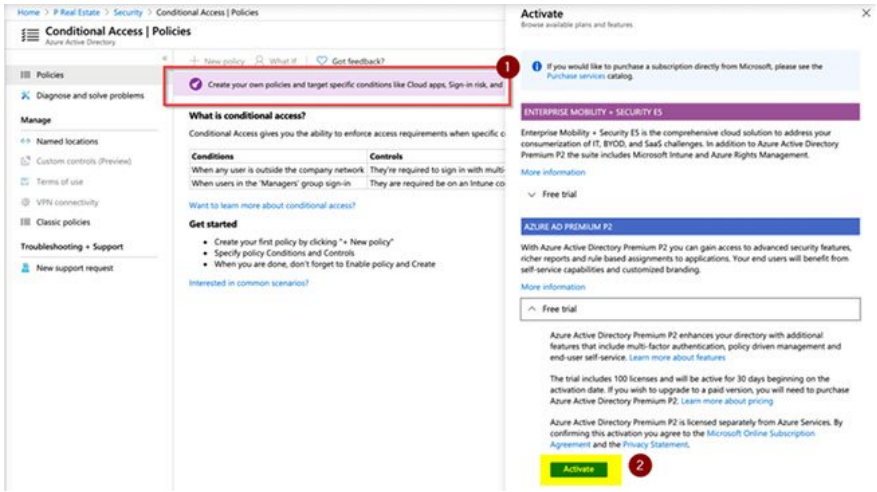
In this article, readers will learn how to apply multi-factor authentication to all remote users in Microsoft Teams. The same principle can be applied to any other application based on Azure Active Directory.

When planning remote access to any company application, the security element through authentication must be designed and implemented.

In previous posts, **TipsMake.com** covered the basics for starting to collaborate and communicate effectively in Microsoft Teams. In this article, readers will learn how to apply multi-factor authentication to all remote users in Microsoft Teams. The same principle can be applied to any other application based on Azure Active Directory.

Activate Azure AD Premium

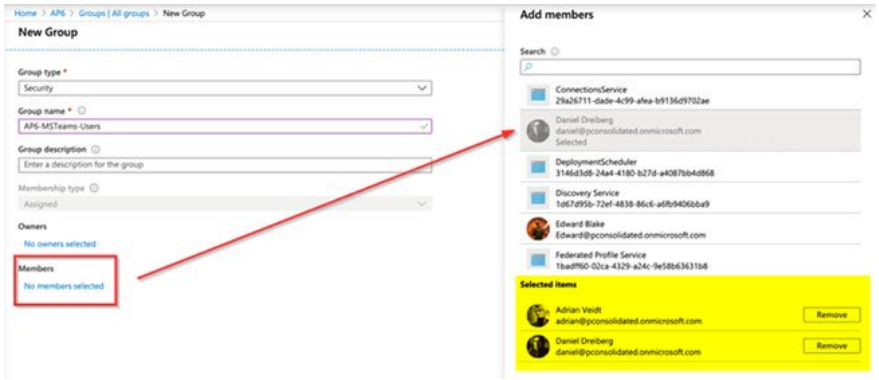
The first step to deploy multi-factor authentication to remote users with Microsoft Teams is activating **Active Azure AD Premium** . Go to **Azure Active Directory** , click **Security,** and then click **Conditional Access.** A banner on the right will be displayed, notifying users who activate Azure Premium to gain access to all resources. Click it, then select **Activate** in **Azure AD Premium P2** .



Select Activate in Azure AD Premium P2

The first step is to create at least a few groups, and then use those groups to deploy services and features to users. These new groups can be created on Active Directory on-premises (if you are syncing) or in Azure Active Directory.

To create Azure AD Group, click **Azure Active Directory> Groups> New Group** . Fill in the required information and select the desired user, then click **Create** to complete the process.



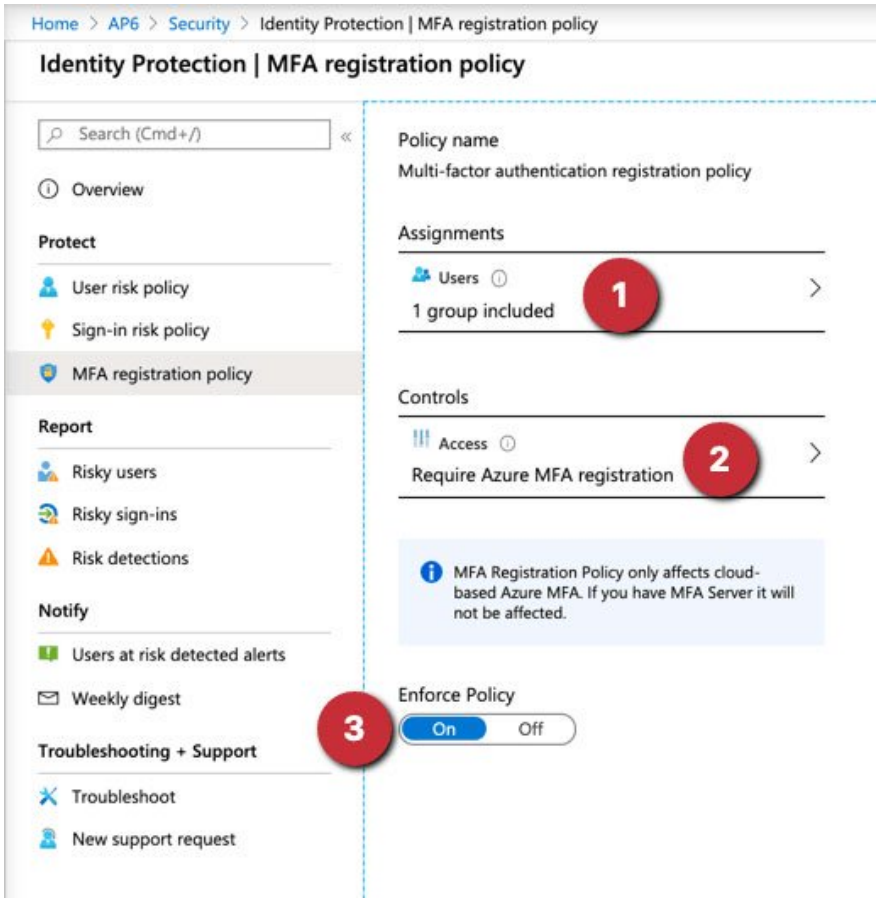
Click Create to complete the process

Manage Azure AD Premium

Using Azure Premium activates many of your environmental protection features. This section will focus on some of the features that address the goal of the article, which is to enable multi-factor authentication for all users using Microsoft Teams.

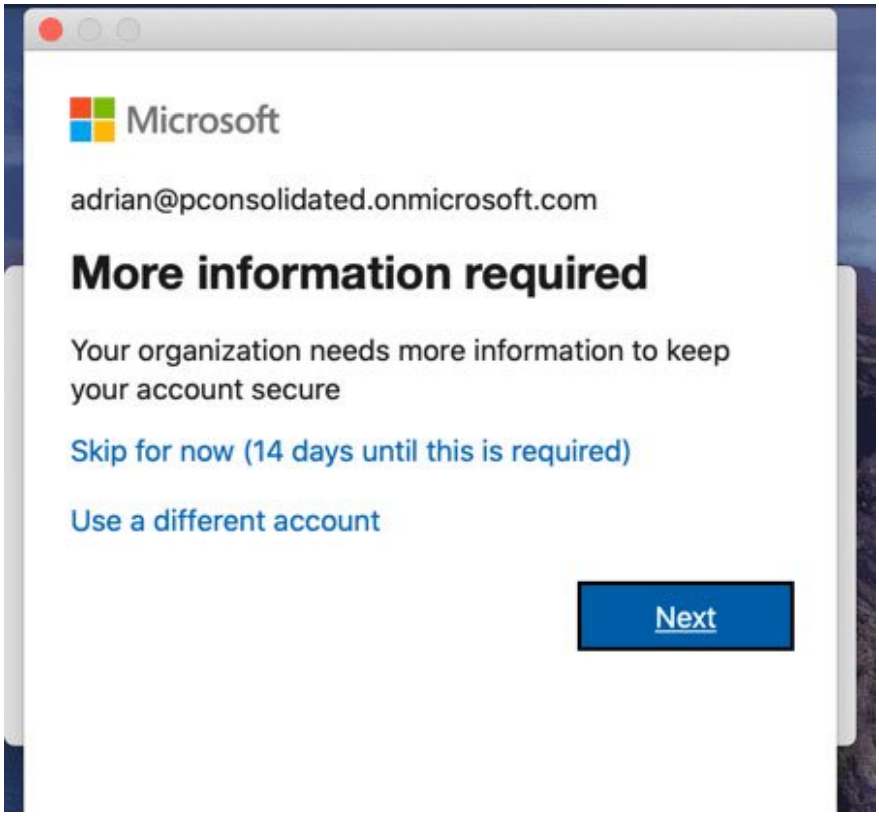
The first step is to manage the **MFA registration policy** . Determine how to deploy MFA to end users by asking them to register and this process can be done before releasing a service, such as Microsoft Teams.

Open **Azure Active Directory** in **Azure Portal.** Click **Security> Identity Protection** and select **MFA registration policy** . All settings will be displayed in **Users.** Select a group (or even all users depending on the size of the company). The article will select the group created to support Microsoft Teams.



All settings will be displayed in Users

What is the impact of this setting? All users in the configuration will receive the dialog shown in the image below, which helps them configure their MFA.



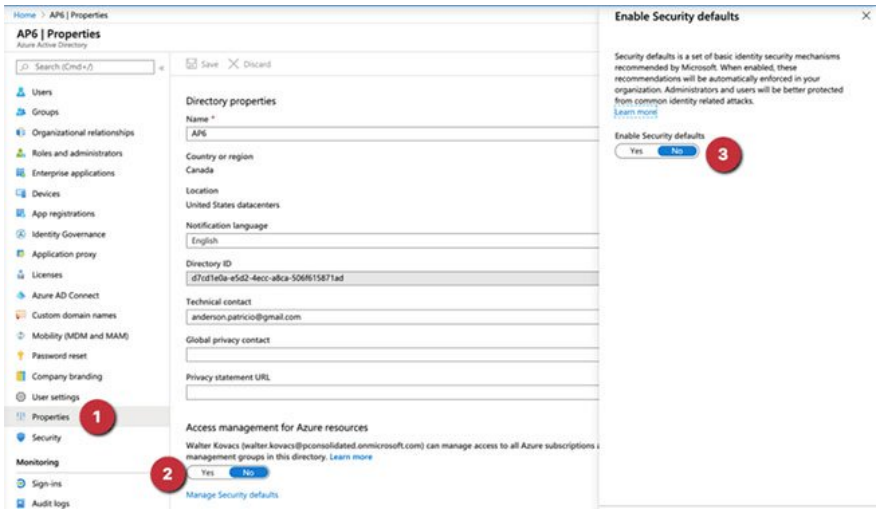
All users in the configuration will receive a MFA configuration help dialog

Only enforce multi-factor authentication on Microsoft Teams

Now it's time to configure conditional access, allowing flexibility when creating application access rules. By default, new subscriptions (after October 2019) are enabled for default security.

If you are planning to take advantage of conditional access, disable those security features and start control through conditional access. Unfortunately, both of these features cannot coexist.

Log in to **Azure Portal** , click on **Azure Active Directory** , select **Properties.** Next, click on the last link that says **Manage Security Defaults** and select **No.** Click on **Save.**

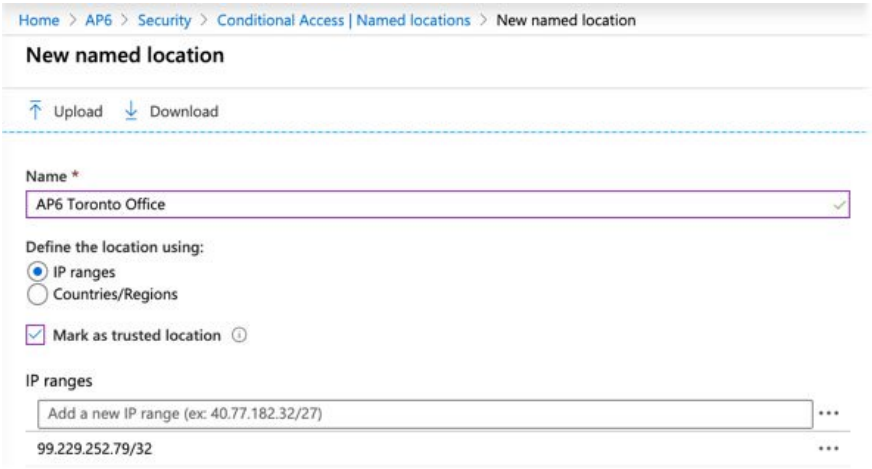


Click on Save
It's time to create the first policy to address multi-factor authentication requests for remote users with Microsoft Teams.

The first is to determine the IP range being used by offices. MFA for remote users who are not in the corporate office will be required.

Click on **Azure Active Directory** in **Properties** , click on **Security.** Click on **Conditional Access** and all existing policies will appear on the right. Before going to the policies, click **Name locations> New location** .

Fill in the position of the office. You can even specify countries instead of IP addresses, in case you need easier access.



Fill in the position of the office
Back to the main point! Click **Policies.** There should not be any policies listed. Click on **New.**

At first, this process looks complicated and you need time to get used to. First, label the policy and handle two main parts, namely: **Assignments** and **Access Controls.**

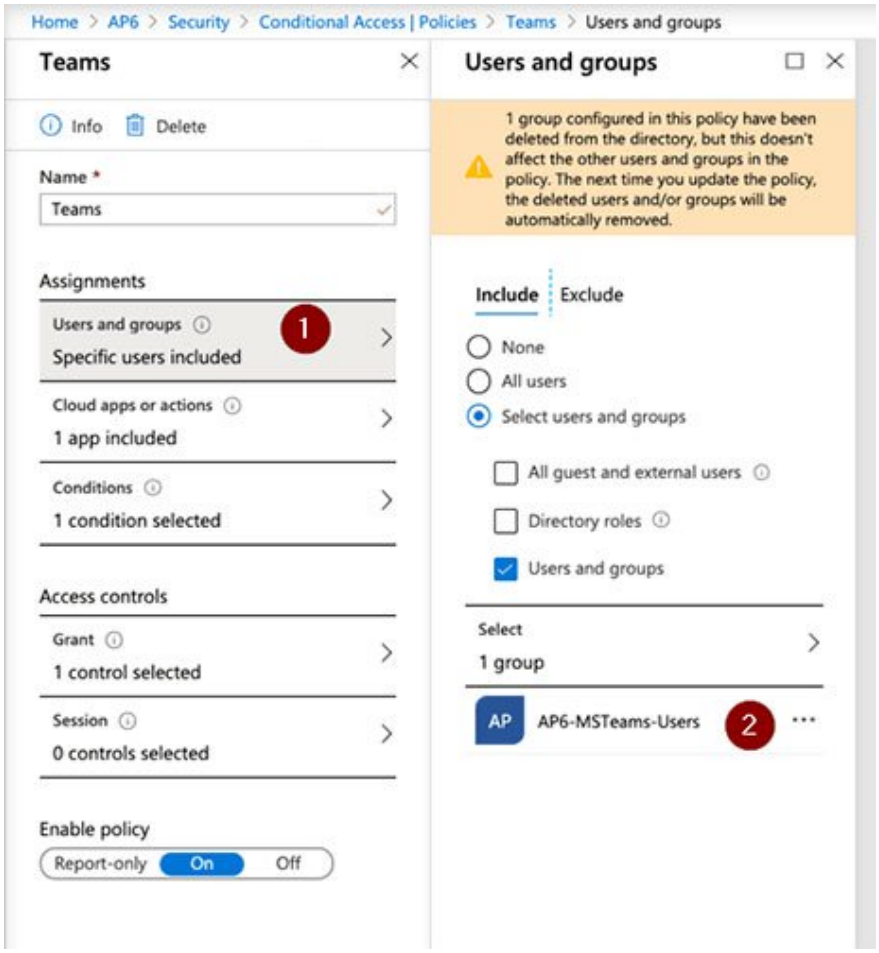
Think of **Assignments** like the 'if' clause. When any particular user is trying to authenticate, they must meet all policy requirements. Then an action, defined in **Access Control** , will occur.

In the **Assignments** section , the following settings will be configured:

1. **Users and Groups** : Only include AP6-MSTeam-Users.
2. **Cloud apps or actions** : Select Microsoft Teams from the list.
3. **Conditions** : Define **Locations** , configure **Include: Any** and **Exclude: All Trusted locations** .

In the **Access Controls** section , click **Grant** , select **Grant Access** and check the **Require multifactor authentication option** .

The final step is to enable the policy by selecting **On** in the final settings. Click **Create.**



Click Create

You finished reading the article "**Deploy multi-factor authentication to remote Microsoft Teams users**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.