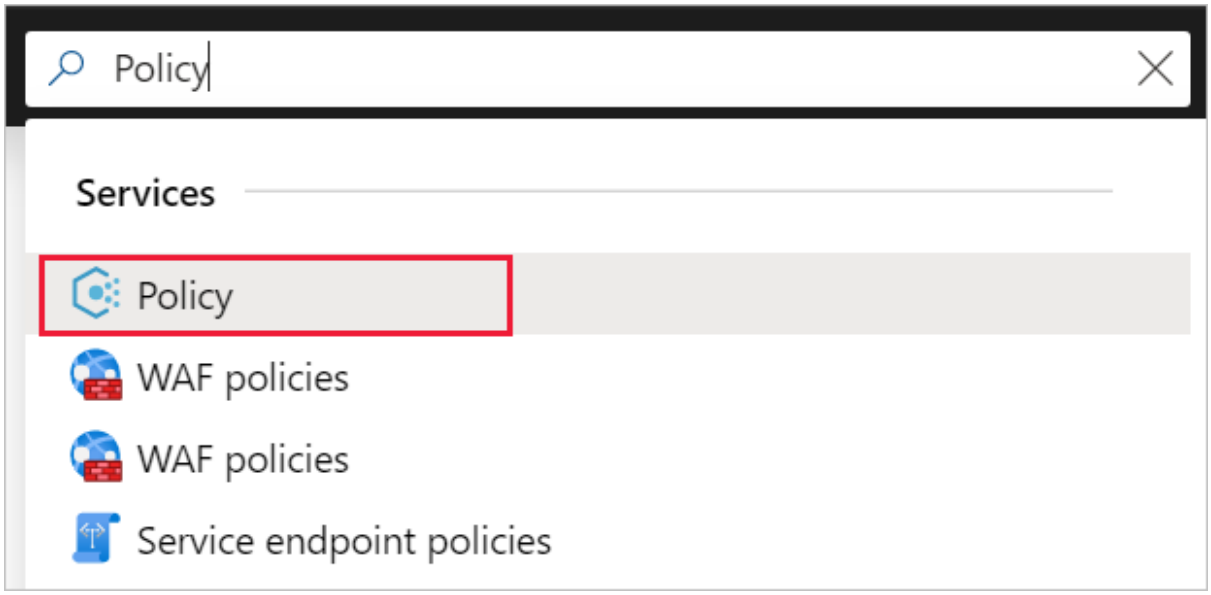
Azure Policy

The Azure Policy is a free Azure service that permits you to make policies, and assign them to resources, and receive alerts or take action in cases of non-compliance with these policies. The Azure Policy is a free Azure service that permits you to make policies, and assign them to resources, and receive alerts or take action in cases of non-compliance with these
policies.



Policy compliance

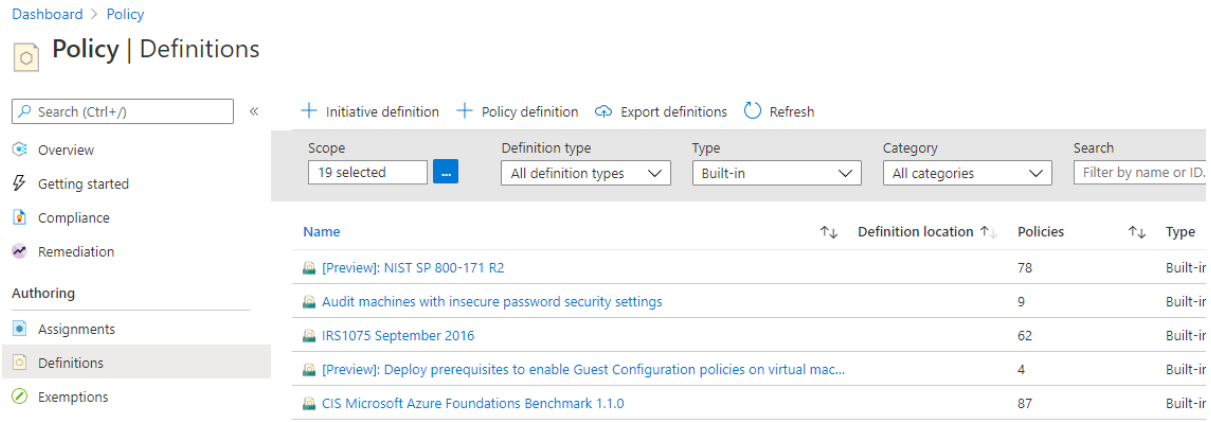
Policy **Compliance** means conforming to a rules course or principle of action adopted or proposed by an organization or individual. Or in other words, policy compliance is law which checks that all our resources are obeying attach rules and policies or not.

Built in default policies

Built-in policies/user flows are predefined for the most common identity tasks, such as sign-up, sign-in, and profile editing. Built in policies are for the common simple tasks required when authenticating users.

Custom policies

Custom policies are essentially build in default policies but provide developers with extra configurations. Custom policies can be fully edited by an identity developer to complete many different tasks.

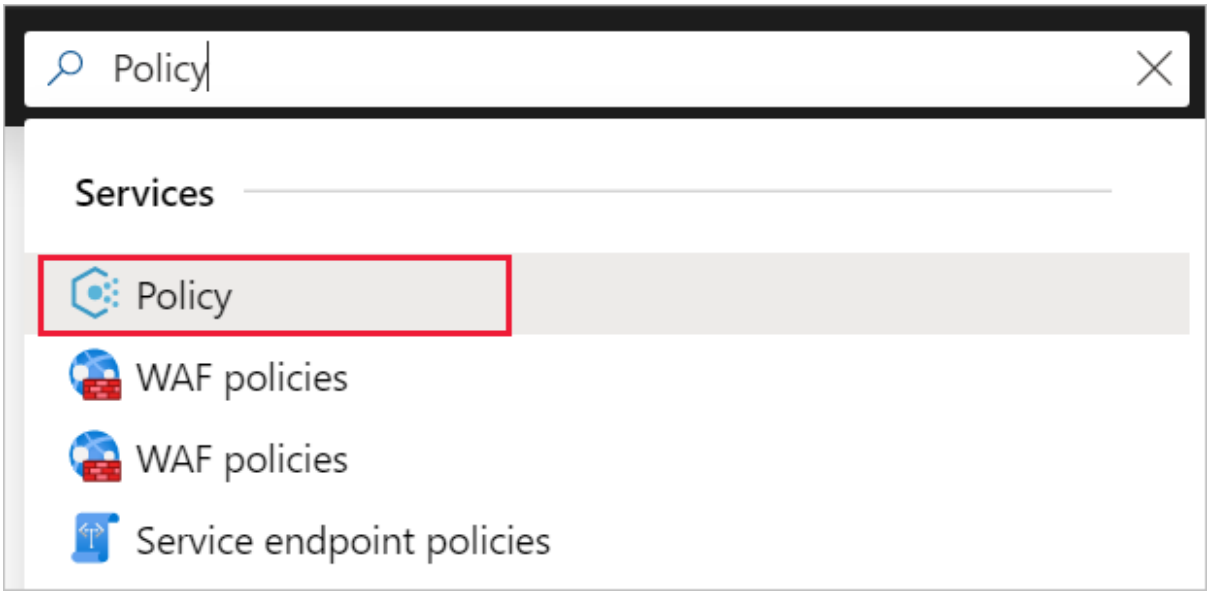


How can we remediate the policy

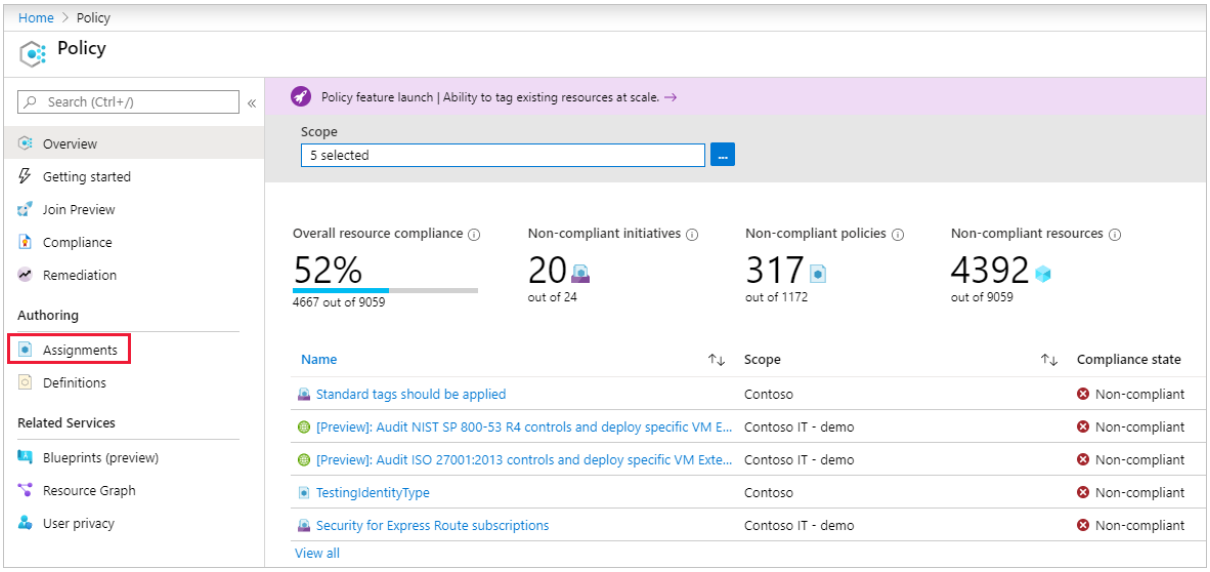
1. Launch the Azure Policy service in the Azure portal by selecting All services, then searching for and selecting Policy.
2. Select Compliance on the left side of the Azure Policy page.
3. Select a non-compliant policy or initiative assignment containing deploy If Not Exists or modify effects.
4. Select the Create Remediation Task button at the top of the page to open the New remediation task page.
5. Follow the steps to specify remediation task details.

How can we assign the policy to another user?

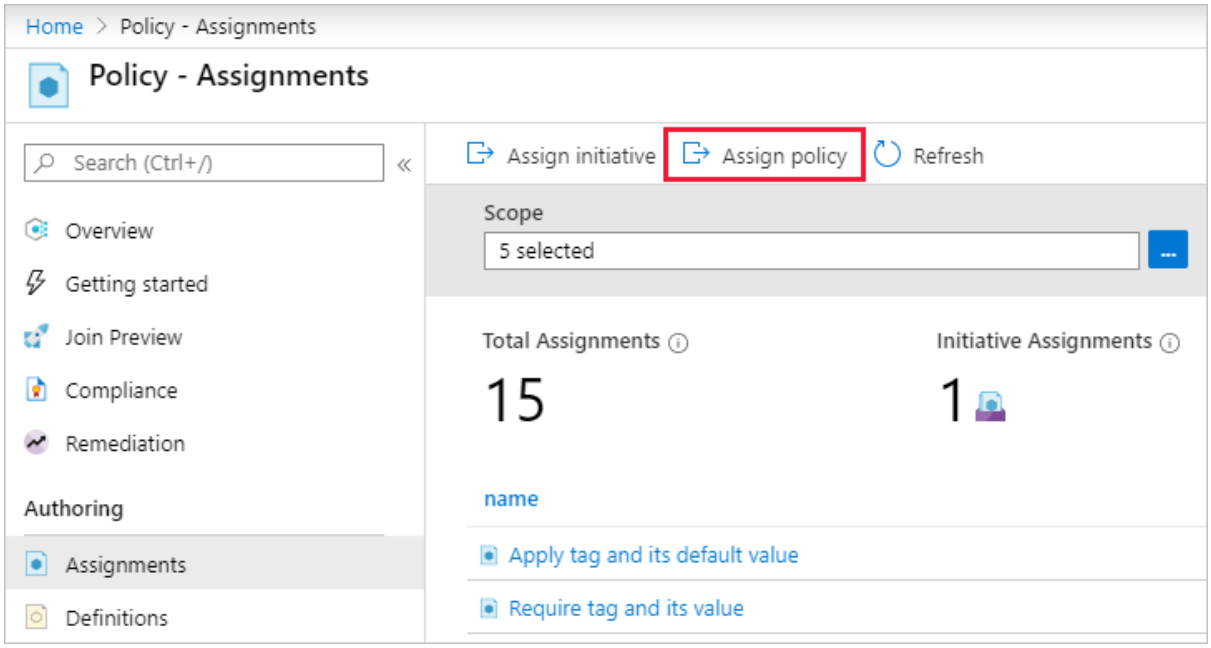
1. Go to the Azure portal to assign policies. Search for and select **Policy**.



2. Select **Assignments** on the left side of the Azure Policy page. An assignment is a policy that has been assigned to take place within a specific scope.



3. Select **Assign Policy** from the top of the **Policy - Assignments** page.



4. On the **Assign Policy** page and **Basics** tab, select the **Scope** by selecting the ellipsis and selecting either a management group or subscription.

5. Resources can be excluded based on the **Scope**. **Exclusions** start at one level lower than the level of the **Scope**.

6. Select the **Policy definition** ellipsis to open the list of available definitions. You can filter the policy definition **Type** to Built-in to view all and read their descriptions.
7. Select **Inherit a tag from the resource group if missing**.
8. The **Assignment name** is automatically populated with the policy name you selected, but you can change it. You can also add an optional **Description**. The description provides details about this policy assignment.
9. Leave **Policy enforcement** as Enabled. When Disabled, this setting allows testing the outcome of the policy without triggering the effect.

10. **Assigned by** is automatically filled based on who is logged in. This field is optional, so custom values can be entered.
11. Select the **Parameters** tab at the top of the wizard.
12. Select the **Remediation** tab at the top of the wizard.
13. Leave **Create a remediation task** unchecked.
14. **Create a Managed Identity** is automatically checked since this policy definition uses the modify effect.

15. Select the **Non-compliance messages** tab at the top of the wizard.
16. Select the **Review + create** tab at the top of the wizard.
17. Review your selections, then select **Create** at the bottom of the page.