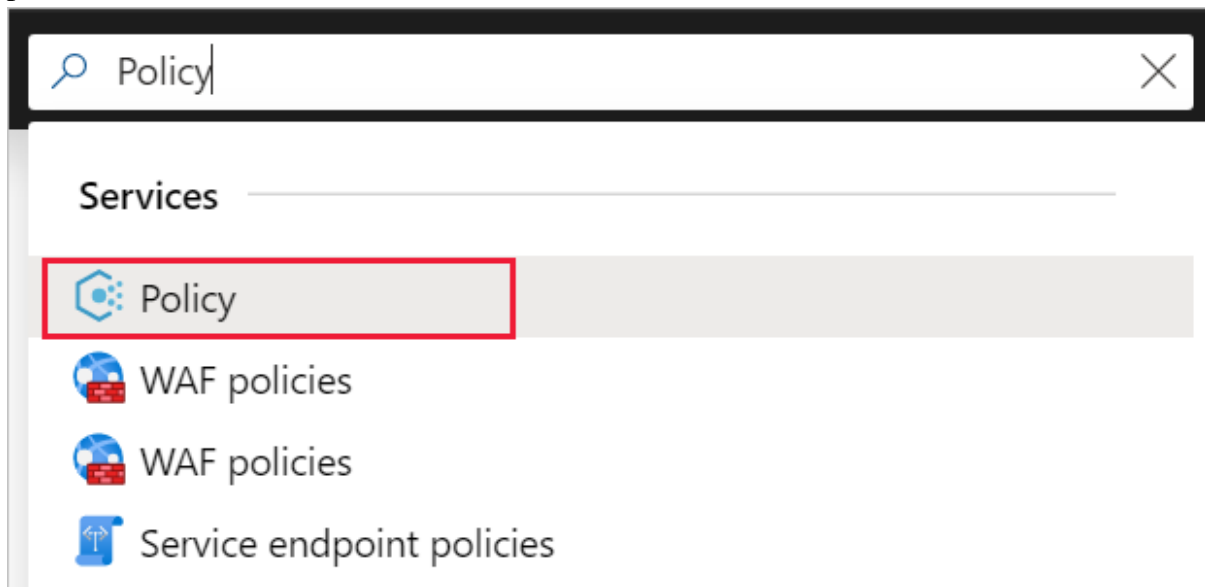


Azure Policy

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.

Policy | Definitions

Search (Ctrl+/)

<<

+ Initiative definition + Policy definition Export definitions Refresh

Overview

Getting started

Compliance

Remediation

Authoring

Assignments

Definitions

Exemptions

Scope

19 selected

Definition type

All definition types

Type

Built-in

Category

All categories

Search

Filter by name or ID.

Name

↑↓

Definition location

↑↓

Policies

↑↓

Type

[Preview]: NIST SP 800-171 R2

78

Built-in

Audit machines with insecure password security settings

9

Built-in

IRS1075 September 2016

62

Built-in

[Preview]: Deploy prerequisites to enable Guest Configuration policies on virtual mac...

4

Built-in

CIS Microsoft Azure Foundations Benchmark 1.1.0

87

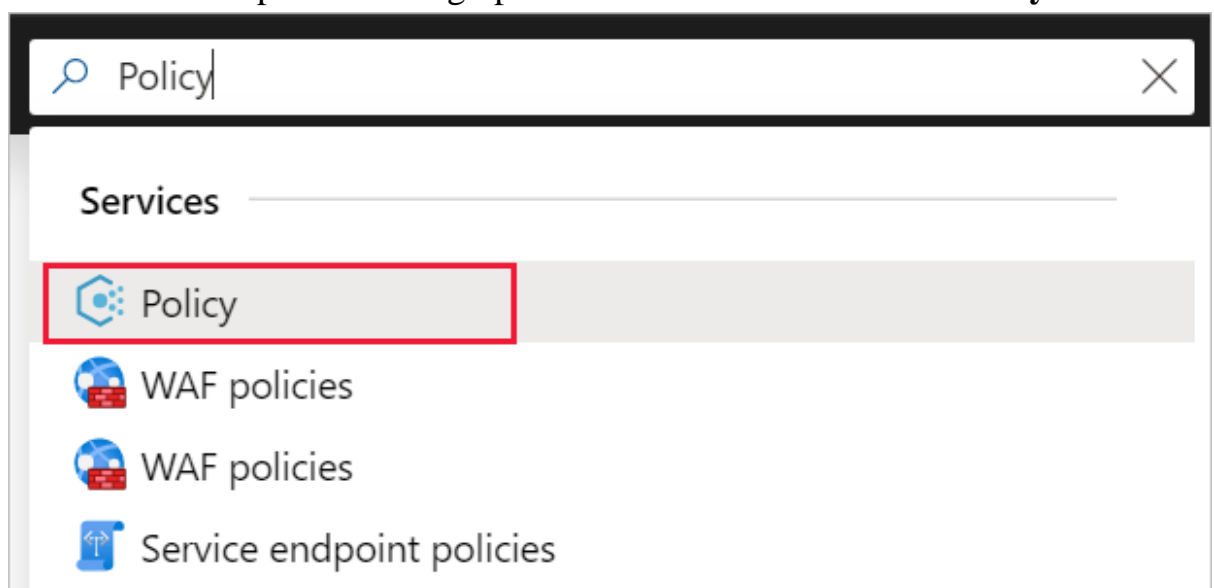
Built-in

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.

The screenshot shows the Azure Policy page. The left sidebar has a search bar and a list of navigation items: Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, Assignments (highlighted with a red box), Definitions, and Related Services. The main content area shows a 'Policy' header with a feature launch message. Below this is a 'Scope' dropdown set to '5 selected'. A summary section displays four metrics: Overall resource compliance at 52% (4667 out of 9059), 20 non-compliant initiatives out of 24, 317 non-compliant policies out of 1172, and 4392 non-compliant resources out of 9059. A table lists several policies, all marked as 'Non-compliant'.

Name	Scope	Compliance state
Standard tags should be applied	Contoso	Non-compliant
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM E...	Contoso IT - demo	Non-compliant
[Preview]: Audit ISO 27001:2013 controls and deploy specific VM Ext...	Contoso IT - demo	Non-compliant
TestingIdentityType	Contoso	Non-compliant
Security for Express Route subscriptions	Contoso IT - demo	Non-compliant

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

The screenshot shows the 'Policy - Assignments' page. The left sidebar is similar to the previous one, but 'Assignments' is now selected. The main content area has a header with 'Assign initiative', 'Assign policy' (highlighted with a red box), and 'Refresh' buttons. Below this is a 'Scope' dropdown set to '5 selected'. A summary section shows 'Total Assignments' as 15 and 'Initiative Assignments' as 1. A table lists two assignments: 'Apply tag and its default value' and 'Require tag and its value'.

name
Apply tag and its default value
Require tag and its value

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.