

Practical Task 1: Introduction to Microsoft Entra ID

Create a new Microsoft Entra ID tenant.

In Manage tenants I have found create a tenant

The screenshot shows the Microsoft Azure portal interface for creating a new tenant. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, 'Copilot' button, and user profile icon. Below it, the breadcrumb navigation shows 'Home > kpi.ua | Overview > Manage tenants > Create a tenant'. The main title is 'Create a tenant' with a close button. Underneath, there are three tabs: *** Basics** (underlined), *** Configuration**, and **Review + create**. A note below says: 'Microsoft Entra ID and Azure AD B2C enable users to access applications published by your organization, and share same administration experiences. [Learn more](#)'.

Tenant type

Select a tenant type *

Microsoft Entra ID
 Azure AD B2C
[Help me choose...](#)

Review + create < Previous Next : Configuration >

Microsoft Azure Search resources, services, and docs (G+/-) Copilot ...

Home > kpi.ua | Overview > Manage tenants >

Create a tenant

* Basics * Configuration Review + create

Directory details

Configure your new directory

Organization name * ⓘ Yakubyshyn org ✓

Initial domain name * ⓘ yakubyshyn ✓
yakubyshyn.onmicrosoft.com

Location ⓘ United States ✓
✓ Geographic location - United States

The location selected above will determine the geographic location where Microsoft Entra ID will store your Core Store data only. To determine where Microsoft will store or process your Microsoft Entra ID data, see [Microsoft Entra ID Data residency](#).

Review + create < Previous Next : Review + create >

Microsoft Azure Search resources, services, and docs (G+/-) Copilot ...

Home > **Yakubyshyn org | Overview** ...

+ Add ⓘ Manage tenants ⓘ What's new ⓘ Preview features ⓘ Got feedback? ⓘ

Overview Microsoft Entra has a simpler, integrated experience for managing all your identity and Access Management needs. Try the new Microsoft Entra admin center! ⓘ

Preview features Diagnose and solve problems

Manage Monitoring Properties Recommendations Setup guides

Search your tenant

Basic information

Name	Yakubyshyn org	Users	1
Tenant ID	be098e76-f2f0-41f0-8292-f151f67b6729	Groups	0
Primary domain	yakubyshyn.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Migrate to the converged Authentication methods policy
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

Learn more ⓘ

Tenant was created successfully

2. Add at least two users to the directory.

The screenshot shows the Microsoft Azure portal interface for creating a new user. The URL in the address bar is portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/CreateUser.ReactView. The page title is "Create new user". The "Identity" section is visible, showing the "User principal name" field set to "JoeDao" and the "Domain not listed?" link. Other fields include "Mail nickname" (set to "JoeDao" with the "Derive from user principal name" checkbox checked), "Display name" (set to "Joe Dao"), "Password" (a masked password), and "Account enabled" (checked). Navigation buttons at the bottom include "Review + create" (highlighted in blue), "< Previous", "Next: Properties >", and "Give feedback".

This screenshot shows the continuation of the user creation process. The "Identity" section is shown again with the "User principal name" field set to "BillieJean". The "Mail nickname" field is also set to "BillieJean" with the "Derive from user principal name" checkbox checked. Other fields like "Display name", "Password", and "Account enabled" are also present. The navigation buttons at the bottom are identical to the previous screen.

I left default options everywhere and just clicked Next

Microsoft Azure

Home > Yakubshyn.org | Users >

Users ...

Yakubshyn.org

Search

+ New user | Delete | Download users | Bulk operations | Refresh | Manage view | Per-user MFA | Got feedback?

All users

Audit logs

Sign-in logs

Diagnose and solve problems

Deleted users

Password reset

User settings

Bulk operation results

New support request

Search

Add filter

Azure Active Directory is now Microsoft Entra ID.

3 users found

	Display name ↑	User principal name ↑	User type	On-premises sync status	Identities	Company name	Creation type
<input type="checkbox"/>	BJ Billie Jean	BillieJean@yakubshyn.onmicrosoft.com	Member	No	yakubshyn.onmicrosoft.com		
<input type="checkbox"/>	JD Joe Dao	JoeDao@yakubshyn.onmicrosoft.com	Member	No	yakubshyn.onmicrosoft.com		
<input type="checkbox"/>	АЯ Анатолій Якубшин	goldykub_kpi.ua#EXT#@yakubshyn.org	Member	No	ExternalAzureAD		

users page

3. Create two groups named Developers and Admins.

Microsoft Azure

Home > Yakubshyn.org | Overview >

New Group ...

Got feedback?

Group type * Security

Group name * Developers

Group description Enter a description for the group

Membership type Assigned

Owners
No owners selected

Members
No members selected

Microsoft Azure

Home > Yakubshyn.org | Overview >

New Group ...

Got feedback?

Group type * Security

Group name * Admins

Group description Enter a description for the group

Membership type Assigned

Owners
No owners selected

Members
No members selected

Create

The screenshot shows the Microsoft Azure Groups | All groups page. The left sidebar has 'All groups' selected. The main area displays a table with two rows:

	Name	Object Id	Group type	Membership type	Email
A	Admins	986f676d-2c01-4b8c-ad69-1b248cb0631e	Security	Assigned	
D	Developers	b23e4820-3a75-449f-89ad-0bae70161de5	Security	Assigned	

All groups page

4. Assign the users to appropriate groups.

The screenshot shows the Microsoft Azure User | Groups page for 'Billie Jean'. The left sidebar has 'Groups' selected. The main area shows a table with one row:

Name	Object Id	Group Type	Membership Type	Email	Source
Not a member of any groups					

Clicking add memberships

Select groups

The screenshot shows a search interface for selecting groups. A search bar at the top contains the placeholder text "Try changing or adding filters if you don't see what you're looking for." Below the search bar, a message says "2 results found". Under the heading "All Groups", there is a table with two rows:

Name	Type	Details
Admins	Group	
Developers	Group	

A blue checkmark is next to the "Developers" row, indicating it is selected. At the bottom right of the table area is a "Select" button.

The screenshot shows the Microsoft Azure portal interface for a user named "Billie Jean". The left sidebar has a "Groups" section selected. The main content area displays the "Groups" page for "Billie Jean". The "Overview" section on the left includes links for "Audit logs", "Sign-in logs", "Diagnose and solve problems", "Custom security attributes", "Assigned roles", and "Administrative units". The "Groups" section lists one group:

Name	Object Id	Group Type	Membership Type	Email	Source
Developers	b23e4820-3a75-449f-89ad-0ba...	Security	Assigned		Cloud

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/Groups/userId/0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8/hidePreviewBanner~/true

Microsoft Azure

Home > Yakubshyn.org | Users > Users > Joe Dao

Joe Dao | Groups

User

Search Add membership

Overview Audit logs Sign-in logs Diagnose and solve problems Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods New support request

Select groups

Try changing or adding filters if you don't see what you're looking for.

Search Name Not a member of any group

All Groups

Name	Type	Details
Admins	Group	<input checked="" type="checkbox"/>
Developers	Group	<input type="checkbox"/>

Selected groups (1)

Reset

Admins

Select

The screenshot shows the 'Select groups' dialog box. On the left, there's a sidebar with navigation links like Home, Overview, Audit logs, etc. The main area has a search bar and a table listing two groups: 'Admins' and 'Developers'. The 'Admins' group is selected, indicated by a checked checkbox. On the right, a panel titled 'Selected groups (1)' shows the 'Admins' group with a 'Reset' link. At the bottom, a large blue 'Select' button is visible.

Microsoft Azure

Home > Yakubshyn.org | Users > Users > Joe Dao

Joe Dao | Groups

User

Search Add memberships Remove memberships Refresh Columns Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods New support request

Name	Object Id	Group Type	Membership Type	Email	Source
Admins	986f676d-2c01-4b8c-ad69-1b2...	Security	Assigned		Cloud

The screenshot shows the 'Groups' page for the user 'Joe Dao'. The sidebar includes links for Overview, Audit logs, etc. The main area displays a table with one row for the 'Admins' group. The table columns are: Name, Object Id, Group Type, Membership Type, Email, and Source. The 'Admins' group is listed with its object ID, security type, assigned membership type, and cloud source.

5. Assign the Global Reader role to the Admins group.

Firstly, I need to transfer subscription to a new tenant.

Microsoft Azure Search resources, services, and docs (G+) Copilot goldyakub@kpi.ua KPLUA

Home > Subscriptions >

Azure for Students

Subscription

Overview

Activity log Subscription ID 3a612e70-8e22-4425-b3ea-29f6acf32428

Access control (IAM) Directory kpi.ua (kpi.ua)

Tags My role Owner

Diagnose and solve problems Status Active

Security Plan Azure Plan

Events Parent management group 9fc329d0-d550-414e-8d1c-a71a3efd97e9

Secure Score Not available

Spending rate and forecast No data to display

Current cost 0.00 Forecast 0.00

Costs by resource No active resource emitted usage yet.

Top free services Used within limit 0

Service Azure Cosmos Data Stored

Azure Cosmos 100 RU/s

Storage, Files, Stored

Storage, Prem Blob, P6 Disks

Storage, Stanc Managed Disk Snapshots

Storage, Stanc Managed Disk Operations

View all free services

Top products by number of resources You don't have any resources in this subscription

Azure Defender coverage Azure Defender is not enabled for this subscription Upgrade coverage

Click change directory

Microsoft Azure Search resources, services, and docs (G+) Copilot goldyakub@kpi.ua KPLUA

Home > Subscriptions >

Azure for Students

Subscription

Overview

Activity log Subscription ID 3a612e70-8e22-4425-b3ea-29f6acf32428

Access control (IAM) Directory kpi.ua (kpi.ua)

Tags My role Owner

Diagnose and solve problems Status Active

Security Parent management group 9fc329d0-d550-414e-8d1c-a71a3efd97e9

Events

Cost Management

Billing

Settings

Help

Spending rate and forecast No data to display

Current cost 0.00 Forecast 0.00

Costs by resource

Top products by number of resources You don't have any resources in this subscription

Azure I

Change the directory

Cloud services (classic) deployment model is retiring on 31 August 2024. The service administrator role on this subscription would be replaced by Azure RBAC role in the new tenant. [Learn more](#)

Changing the directory doesn't change billing ownership for the subscription. You won't be able to delete the original directory until billing ownership is transferred to someone else. [Learn more](#)

From kpi.ua (kpi.ua)

To

I understand that changing directory does not transfer some resources, for example, all Azure role-based access control assignments are deleted ([See affected users](#)) and system/user assigned managed identities are invalidated and not transferred to target directory. [Learn more](#)

Change Cancel Give feedback

<https://portal.azure.com/?feature.msals=true#>

<https://portal.azure.com/?feature.msals=true#>

<https://portal.azure.com/?feature.msals=true#>

After that I clicked review and assign

The screenshot shows the Microsoft Azure 'Add role assignment' interface. The 'Review + assign' tab is selected. The 'Role' is set to 'Reader' and the 'Scope' is the current subscription. Under 'Members', there is one entry: 'Admins' (Object ID: 986f676d-2c01-4b8c-ad69-7a248ca0631e, Type: Group). A note says 'No description'.

A Copilot AI window is overlaid on the page, displaying two error messages about JSON validation. The first message states: 'Make sure that the "properties" property is included and contains valid key-value pairs. If the "properties" property is missing or its value is null, the JSON will be considered malformed.' It includes a code example: `{"properties": { "exampleKey": "exampleValue" }}`. The second message is similar, reiterating the requirement for a non-null 'properties' object.

The Copilot AI window shows a success message: 'Added Role assignment' with a green checkmark. It also displays the JSON object: `"properties": { "exampleKey": "exampleValue" }`.

6. Assign the Application Developer role to the Developers group

The screenshot shows the 'Add role assignment' interface again. The 'Review + assign' tab is selected. The 'Role' dropdown is set to 'Job function roles'. The search bar shows 'App Service Environment Contributor'. The results table shows one result: 'App Service Environment Contributor' (Type: All, Category: All, Description: Manage App Service Environments but not the App Service Plans or Websites that it hosts, Details: BuiltinRole, Category: None). A note at the bottom says 'Showing 1 - 1 of 1 results.'

Microsoft Azure

Home > Subscriptions > Azure for Students | Access control (IAM) > Add role assignment ...

Role Members Conditions Review + assign

Selected role App Service Environment Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name Object ID Type

No members selected

Description

Select members

Search by name or email address

Selected members:

Developers b23e4020-3a75-449f-89ad-0bae70161de5

Review + assign Previous Next Select Close

Microsoft Azure

Home > Subscriptions > Azure for Students | Access control (IAM) > Add role assignment ...

Role Members Conditions Review + assign

Role App Service Environment Contributor

Scope /subscriptions/3a612e70-8e22-4425-b3ea-29f6ecf32428

Members Name Object ID Type

Developers b23e4020-3a75-449f-89ad-0bae70161de5 Group

Description No description

Review + assign Previous Next Feedback

Notifications

More events in the activity log → Dismiss all ▾

✓ Added Role assignment ×

Developers was added as App Service Environment Contributor for Azure for Students.

a few seconds ago

✓ Added Role assignment ×

Admins was added as Reader for Azure for Students.

4 minutes ago

7. Verify that the role assignments function as expected for both groups.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes 'Overview', 'Diagnose and solve problems', 'Manage' (with sub-options like Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, and Licenses), and 'Azure role assignments' (which is selected and highlighted in grey). Below this is an 'Activity' section and a 'Troubleshooting + Support' link. The main content area displays a table titled 'Azure role assignments' for the 'Admins' group. The table has columns for 'Role', 'Resource Name', 'Resource Type', 'Assigned To', and 'Condition'. A single row is shown: 'Reader' role assigned to 'Azure for Students' resource type, under 'Subscription' (Azure for Students), 'Assigned To' 'Admins', and 'Condition' 'None'. A note at the top of the table says, 'If this identity has role assignments that you don't have permission to read, they won't be shown in the list.' Below the table is a 'Notifications' sidebar with several items: 'Added Role assignment' (Developers was added as App Service Environment Contributor for Azure for Students, a minute ago), 'Added Role assignment' (Admins was added as Reader for Azure for Students, 5 minutes ago), 'Upload Completed for GlobalReader.json' (509 B | "Streaming upload", 12 minutes ago), 'File validation' (Valid JSON content, 12 minutes ago), 'Upload Completed for GlobalReader.json' (253 B | "Streaming upload", 17 minutes ago), and 'File validation' (Invalid JSON content - Malformed JSON: "properties" property not present or value is null, 17 minutes ago). There is also a 'Help me troubleshoot' button.

This screenshot shows the Microsoft Azure portal interface for the 'Developers' group. The left sidebar navigation bar is identical to the previous screenshot. The main content area displays a table titled 'Azure role assignments' for the 'Developers' group. The table has columns for 'Role', 'Resource Name', 'Resource Type', 'Assigned To', and 'Condition'. A single row is shown: 'App Service Environment Contributor' role assigned to 'Azure for Students' resource type, under 'Subscription' (Azure for Students), 'Assigned To' 'Developers', and 'Condition' 'None'. A note at the top of the table says, 'If this identity has role assignments that you don't have permission to read, they won't be shown in the list.' The 'Notifications' sidebar is visible on the right, showing the same log entries as the previous screenshot.

Practical Task 2: Enabling Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

1. Enable Single Sign-On (SSO) for your Microsoft Entra ID tenant

The screenshot shows the Microsoft Azure App Gallery interface. In the search bar at the top left, 'zoom' is typed. Below the search bar, there are filters: 'Single Sign-on : All', 'User Account Management : All', and 'Categories : All'. Underneath these filters, there are two additional buttons: 'Federated SSO' and 'Provisioning'. On the right side of the screen, the 'Zoom' application page is displayed. It includes a logo for Zoom, a name field containing 'Zoom', a publisher field for 'Zoom Video Communications, Inc.', and a provisioning field indicating 'Automatic provisioning supported'. Below this information, it says 'Single Sign-On Mode' and lists 'Password-based Sign-on', 'SAML-based Sign-on', and 'Linked Sign-on'. At the bottom right of the app page, there is a blue 'Create' button.

Create zoom app

The screenshot shows the 'Zoom | Overview' page in the Microsoft Azure Enterprise Applications section. On the left, there is a sidebar with various management options like Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes), Security, Activity, and Troubleshooting + Support. The main area is titled 'Properties' and shows the application's name as 'Zoom', application ID as 'b6c1ac52-9dza-4307-be0a...', and object ID as 'acd7b3b3-d8f8-4c6b-80fd...'. Below the properties, there is a 'Getting Started' section with five numbered steps: 1. Assign users and groups, 2. Set up single sign on, 3. Provision User Accounts, 4. Conditional Access, and 5. Self service. Each step has a brief description and a 'Get started' button.

Setup single sign on

Microsoft Azure

Home > Enterprise applications | All applications > Zoom

Zoom | Single sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Roles and administrators Users and groups

Single sign-on

Provisioning Self-service Custom security attributes

Security Activity Troubleshooting + Support

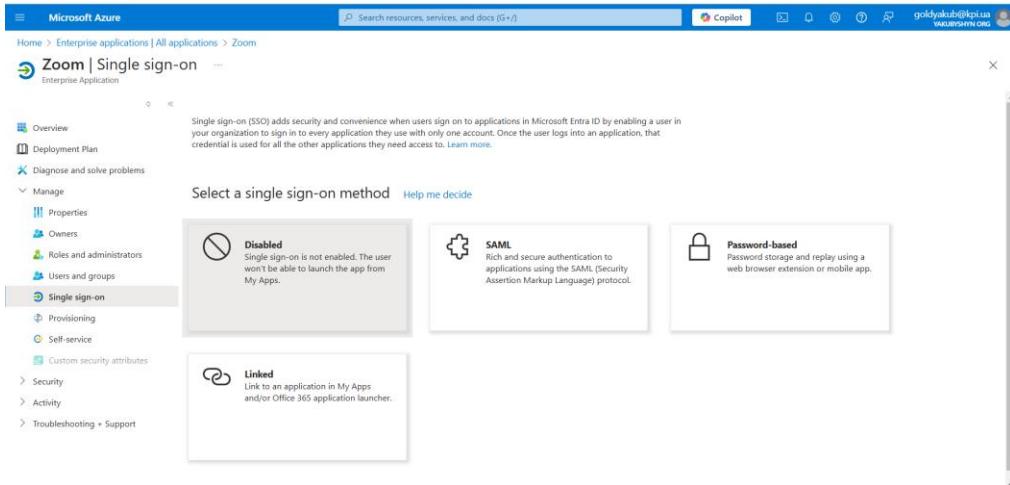
Select a single sign-on method [Help me decide](#)

Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.



Password-based

Microsoft Azure

Home > Enterprise applications | All applications > Zoom

Zoom

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Roles and administrators Users and groups

Single sign-on

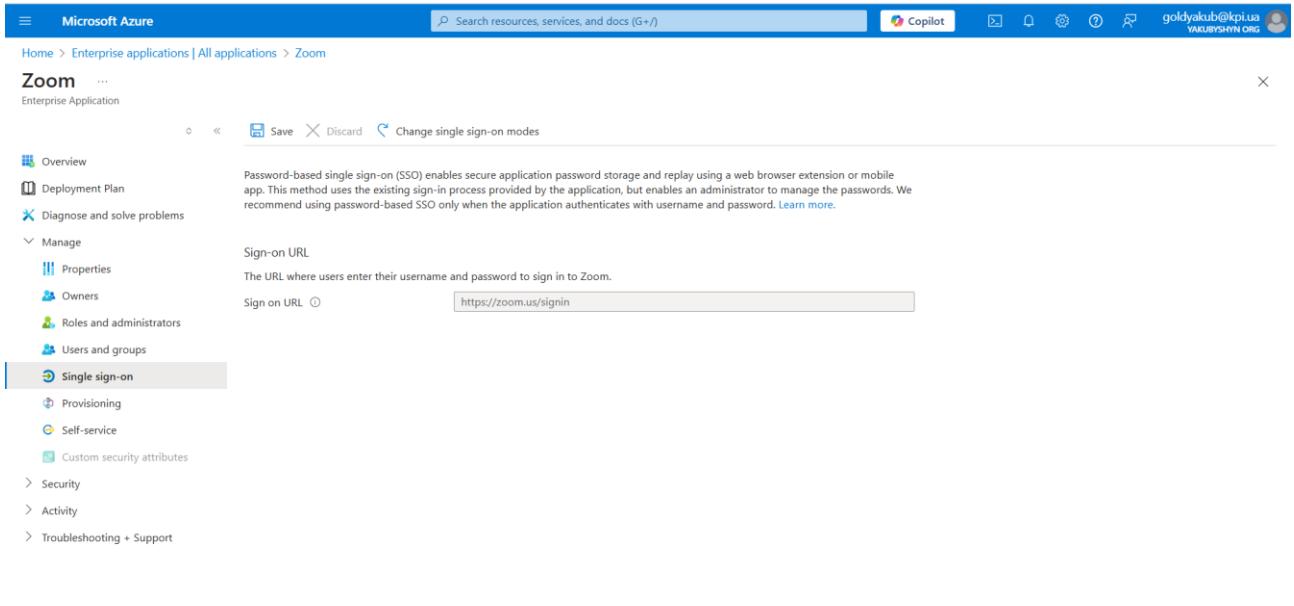
Provisioning Self-service Custom security attributes

Sign-on URL

The URL where users enter their username and password to sign in to Zoom.

Sign on URL

Save Discard Change single sign-on modes



Microsoft Azure

Home > Enterprise applications | All applications > Zoom | Us

Add Assignment

Yakubshyn.org

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

None Selected

Select a role *

None Selected

Search

Try changing or adding filters if you don't see what you're looking for.

3 results found

All Users

Name	Type	Details
Анатолій Якубшин	User	goldyakub@kpi.ua
Billie Jean	User	BillieJean@yakubshyn.onmicrosoft.com
Joe Dao	User	JoeDao@yakubshyn.onmicrosoft.com

Selected (2)

Reset

Billie Jean BillieJean@yakubshyn.onmicrosoft.com

Joe Dao JoeDao@yakubshyn.onmicrosoft.com

Assign Select

Microsoft Azure

Home > Enterprise applications | All applications > Zoom | Users and groups >

Add Assignment

Yakubshyn.org

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

2 users selected.

Select a role *

None Selected

Enter role name to filter items...

Basic

Corp

Licensed

On-Prem

Pro

Selected Role

Basic

Select

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users
2 users selected.
Select a role *
Basic

Assign

2. Enforce Multi-Factor Authentication (MFA) for all users in the directory.
3. Configure conditional access policies to require MFA for high-risk sign-ins.

Because I don't have *Microsoft Entra ID Premium*. I am doing some workaround

Name: Yakubshyn.org

Country or region: United States

Data location: United States datacenters

Notification language: English

Tenant ID: be098e76-f2f0-41f0-8292-f151f67b6729

Technical contact: goldiyakub@kpi.ua

Global privacy contact: [empty]

Privacy statement URL: [empty]

Access management for Azure resources

Анатолій Якубшин (goldiyakub@kpi.ua) can manage access to all Azure subscriptions and management groups in this tenant.

No

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.

Your organization is protected by security defaults.

Save Discard



Security defaults

X

Security defaults

Enabled (recommended)

Your organization is currently using security defaults.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

be

Save

Cancel

Enabled security defaults to use MFA

Microsoft Azure

Home > Users ...

All users

Audit logs Sign-in logs Diagnose and solve problems Deleted users Password reset User settings Bulk operation results New support request

Search (All users) Search Add filter

Azure Active Directory is now Microsoft Entra ID.

Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
Billie Jean	BillieJean@yakubshyn.onmicrosoft.com	Member	No	yakubshyn.onmicrosoft.com		
Joe Dao	JoeDao@yakubshyn.onmicrosoft.com	Member	No	yakubshyn.onmicrosoft.com		
Анатолий Якубшин	golyakub.kpi.ua#EXT#@yakubshyn.onmicrosoft.com	Member	No	ExternalAzureAD		

click per user MFA

Microsoft Azure

Home > Users >

Per-user multifactor authentication

Bulk update Got feedback?

Users Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the [multifactor authentication deployment guide](#).

Enable MFA Disable MFA Enforce MFA User MFA settings

Search Status : All View : Sign-in allowed users Reset filters

Name	UPN	Status
Billie Jean	BillieJean@yakubshyn.onmicrosoft.com	disabled
Анатолий Якубшин	golyakub.kpi.ua#EXT#@yakubshyn.onmicrosoft.com	disabled
Joe Dao	JoeDao@yakubshyn.onmicrosoft.com	disabled

Click enable MFA

Azure after refresh forced me to add MFA to my root account.

In result I have:

Microsoft Azure

Home >

Per-user multifactor authentication

Bulk update Got feedback?

Users Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

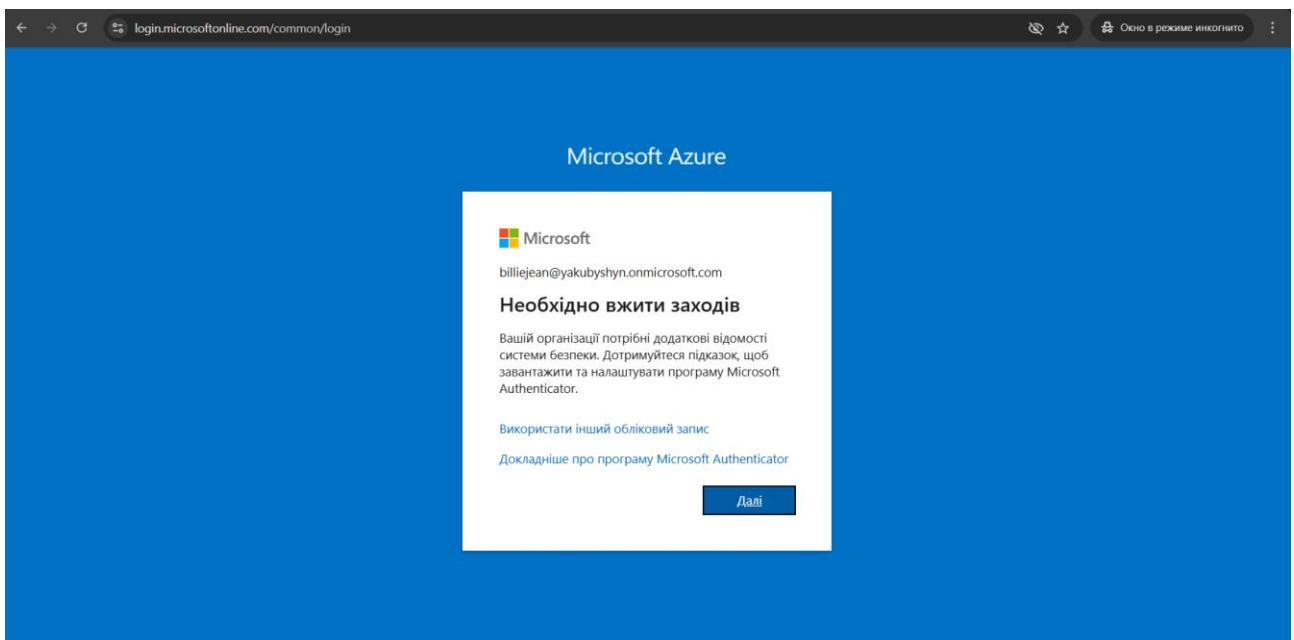
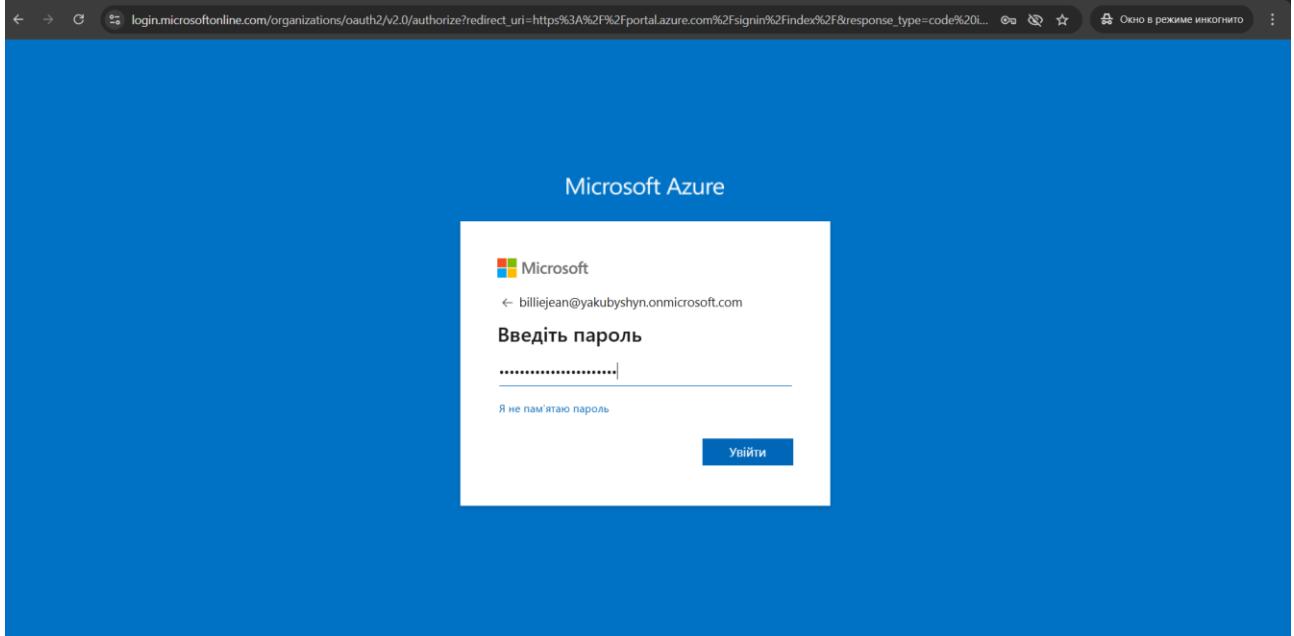
Before you begin, take a look at the [multifactor authentication deployment guide](#).

Enable MFA Disable MFA Enforce MFA User MFA settings

Search Status : All View : Sign-in allowed users Reset filters

Name	UPN	Status
Billie Jean	BillieJean@yakubshyn.onmicrosoft.com	enabled
Анатолий Якубшин	golyakub.kpi.ua#EXT#@yakubshyn.onmicrosoft.com	enforced
Joe Dao	JoeDao@yakubshyn.onmicrosoft.com	enabled

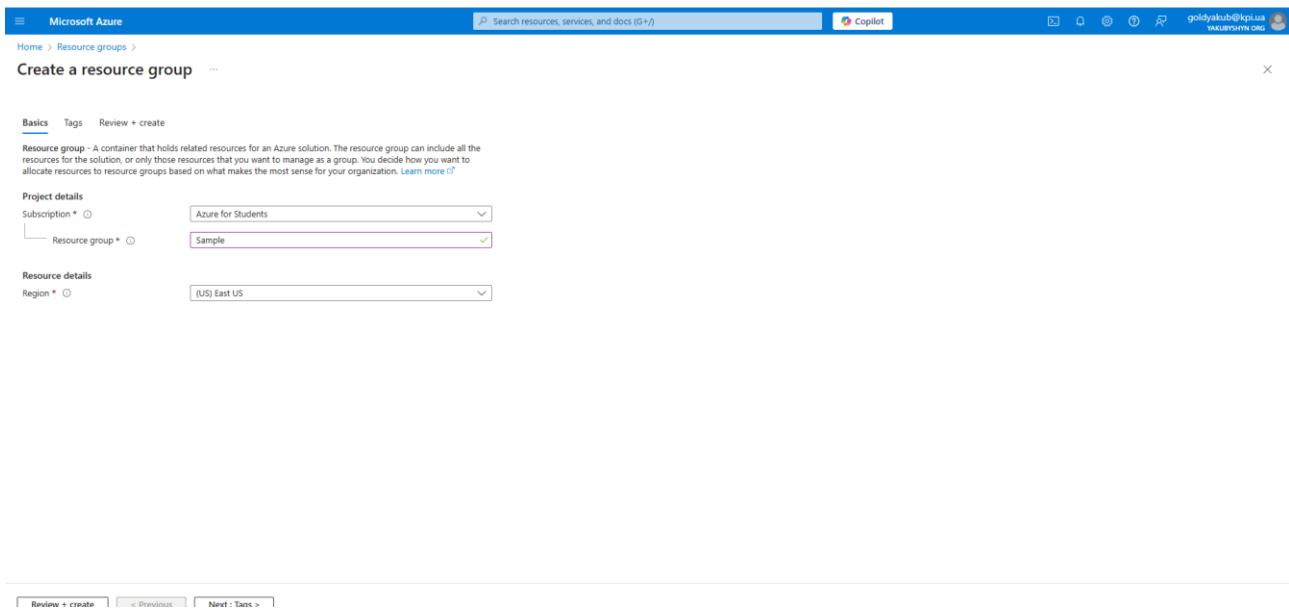
4. Verify that SSO and MFA settings are correctly applied for the users.



As a result, we see that MFA enforced for users (it is needed to add MS Authenticator).

Practical Task 3: Implementing Role-Based Access Control (RBAC)

Implement Role-Based Access Control (RBAC) in Azure to manage access to resources based on roles and ensure fine-grained access management.



Microsoft Azure

Home > Resource groups > Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * Resource group *

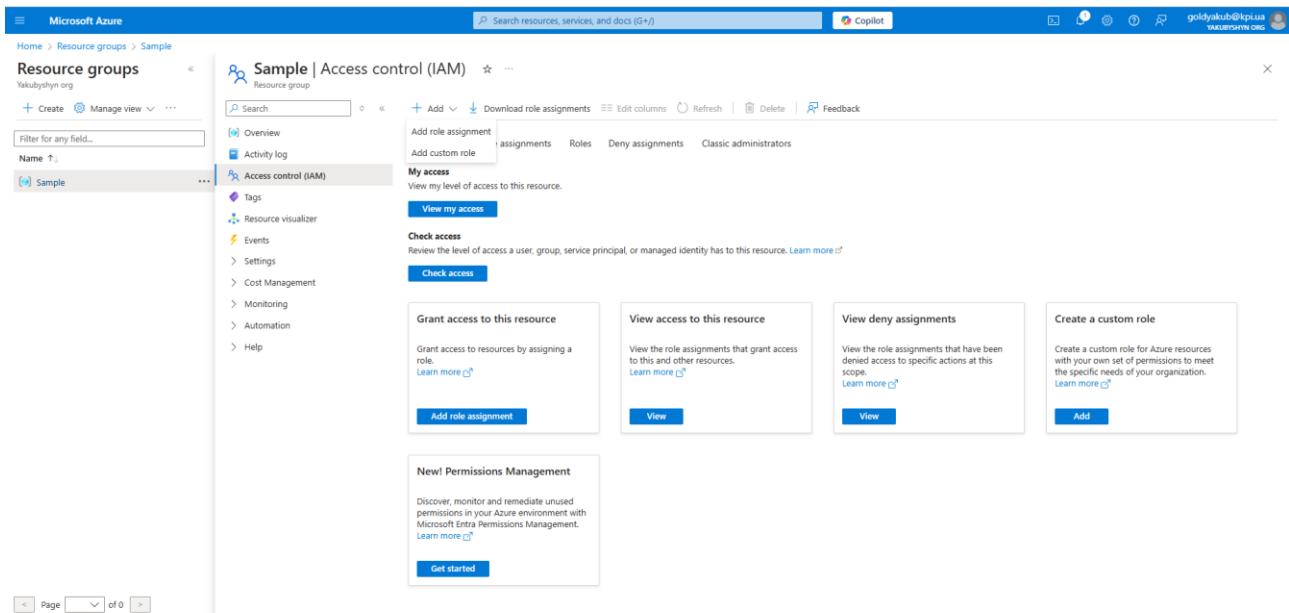
Resource details

Region *

Review + create < Previous Next : Tags >

Created ‘Sample’ resource group to proceed with tasks.

1. Create a custom role named Resource Viewer with read-only permissions for a specific resource group.



Microsoft Azure

Home > Resource groups > Sample

Resource groups

Sample | Access control (IAM)

Resource group

Search

+ Add Download role assignments Edit columns Refresh Delete Feedback

Add role assignment Assignments Roles Deny assignments Classic administrators

Add custom role

My access View my level of access to this resource.

View my access

Check access Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Check access

Grant access to this resource Grant access to resources by assigning a role. [Learn more](#)

Add role assignment

View access to this resource View the role assignments that grant access to this and other resources. [Learn more](#)

View

View deny assignments View the role assignments that have been denied access to specific actions at this scope. [Learn more](#)

View

Create a custom role

Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization. [Learn more](#)

Add

New! Permissions Management Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management. [Learn more](#)

Get started

Page of 0

Click add custom role

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Create a custom role

Basics Permissions * Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name * ✓

Description

Baseline permissions Clone a role Start from scratch Start from JSON

Review + create Previous Next https://portal.azure.com/# Feedback

Gave a name

Clicked Start from JSON

```
D:\> Azure > D:\Resource_viewer.json > {} properties > () o > [ ] permissions > () o > [ ] notDataActions
1  {
2    "properties": {
3      "roleName": "Resource Viewer",
4      "description": "Role with read permissions for resources in the Sample resource group.",
5      "assignableScopes": [
6        "/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample"
7      ],
8      "permissions": [
9        {
10          "actions": [
11            "Microsoft.Resources/subscriptions/resourceGroups/read",
12            "Microsoft.Resources/subscriptions/resourceGroups/resources/read"
13          ],
14          "notActions": [],
15          "dataActions": [],
16          "notDataActions": []
17        }
18      ]
19    }
20  }
```

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Create a custom role

Basics Permissions * Assignable scopes JSON Review + create

Basics

Role name

Role description Role with read permissions for resources in the Sample resource group.

Permissions

Action Microsoft.Resources/subscriptions/resourceGroups/read

Action Microsoft.Resources/subscriptions/resourceGroups/resources/read

Assignable Scopes

Scope

Create Previous https://portal.azure.com/# Feedback

2. Assign the Resource Viewer role to the Developers group created earlier

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment ...

Role Members * Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name	Description	Type	Category	Details
Azure Arc Kubernetes Viewer	Lets you view all resources in cluster/namespace, except secrets.	BuiltInRole	Management + Governance	View
Resource Viewer	Role with read permissions for resources in the Sample resource group.	CustomRole	None	View
ToolchainOrchestrator Viewer Role	Grant access to view all Toolchain orchestrator resources.	BuiltInRole	None	View

Showing 1 - 3 of 3 results.

Review + assign Previous Next Feedback

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment ...

Role Members * Conditions Review + assign

Selected role Resource Viewer

Assign access to User, group, or service principal Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next Feedback

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment ...

Role **Members** Conditions Review + assign

Selected role Resource Viewer

Assign access to User, group, or service principal Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next Select Close

Select members

Search by name or email address

Axancilii Ilych@sample(Guest)	goldiyakub_kpi.us#EXT#@yakubshyn.onmicrosoft.com
Admins	98d6f76d-2c01-4b8c-ad69-1b248cb0631e
Billie Jean	BillieJean@yakubshyn.onmicrosoft.com
Developers	b23e4820-3a75-449f-89ad-0bae70161de5
Joe Dao	JoeDao@yakubshyn.onmicrosoft.com

Selected members:

Developers	b23e4820-3a75-449f-89ad-0bae70161de5
------------	--------------------------------------

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment ...

Role **Members** Conditions Review + assign

Selected role Resource Viewer

Assign access to User, group, or service principal Managed identity

Members + Select members

Name	Object ID	Type
Developers	b23e4820-3a75-449f-89ad-0bae70161de5	Group

Description Optional

Review + assign Previous Next Feedback

Click Review + assign

3. Assign the built-in Contributor role to the Admins group for the same resource group

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment

Role * **Members** * Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name	Description	Type	Category	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	View
AcrDelete	acr delete	BuiltinRole	Containers	View
AcrImageSigner	acr image signer	BuiltinRole	Containers	View
AcrPull	acr pull	BuiltinRole	Containers	View
AcrPush	acr push	BuiltinRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltinRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltinRole	Containers	View
Advisor Recommendations Contributor (Assessments and Re...	View assessment recommendations, accept review recommendations, and manage the recommendations lifecycle (mark recommendations as completed...)	BuiltinRole	None	View
Advisor Reviews Contributor	View reviews for a workload and triage recommendations linked to them.	BuiltinRole	None	View
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.	BuiltinRole	None	View
AgFood Platform Dataset Admin	Provides access to Dataset APIs	BuiltinRole	None	View
AgFood Platform Sensor Partner Contributor	Provides contribute access to manage sensor related entities in AgFood Platform Service	BuiltinRole	None	View
AgFood Platform Service Admin	Provides admin access to AgFood Platform Service	BuiltinRole	AI + Machine Learning	View
AgFood Platform Service Contributor	Provides contribute access to AgFood Platform Service	BuiltinRole	AI + Machine Learning	View

Review + assign Previous Next

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment

Role * **Members** * Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠️ Can a job function role with less access be used instead?

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltinRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image gal...	BuiltinRole	General	View
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.	BuiltinRole	None	View
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Policy.	BuiltinRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltinRole	General	View

Showing 1 - 5 of 5 results.

Review + assign Previous Next

Microsoft Azure

Home > Resource groups > Sample | Access control (IAM) >

Add role assignment

Role **Members** * Conditions Review + assign

Selected role Contributor

Assign access to User, group, or service principal Managed identity

Members + Select members

Name	Object ID	Type
Admins	986f576d-2c01-4b8c-ad69-1b248cb063...	Group

Description Optional

Review + assign Previous Next

<https://portal.azure.com/#>

Then Review + assign

4. Verify that members of the Developers group have only read access and members of the Admins group have full access to the resource group

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and a Copilot button. Below the search bar is a row of service icons: Create a resource, Quickstart Center, Azure AI services, Kubernetes services, Virtual machines, App Services, Storage accounts, SQL databases, Azure Cosmos DB, and More services. The main area is titled "Resources" with tabs for "Recent" and "Favorite". It displays a message: "No resources have been viewed recently" and a "View all resources" button. Below this is a "Navigate" section with links for Subscriptions, Resource groups, All resources, and Dashboard. Under "Tools", there are links for Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, and Cost Management.

Logged in as Developer

The screenshot shows the "Resource groups" page for a "Sample" resource group. The left sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main content area is titled "Overview" and shows the following details: Subscription (moved) : Azure for Students, Subscription ID : 3ab12e70-8e22-4425-b3ea-29f6acf32428, Tags (edit) : Add tags, Deployments : No deployments, Location : East US. Below this is a "Resources" section with a table header for Name, Type, and Location. A note says "Showing 0 to 0 of records." At the bottom, there are buttons for Create resources and Clear filters, and a link to Learn more. The footer includes navigation links for Page 1 of 1 and a Give feedback link.

Switched to a 'Sample' Resource group

Microsoft Azure

Home > Resource groups > Sample | Resource visualizer > Create a resource > Create a virtual machine ...

Create a virtual machine

⚠️ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure for Students

Resource group * Sample Create new

Instance details

Virtual machine name * Sample

Region * (Europe) Norway East

Availability options Availability zone

Zone options Self-selected zone (Choose up to 3 availability zones, one VM per zone)

Azure-selected zone (Preview) (Let Azure assign the best zone for your needs)

Availability zone * Zone 1 You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

< Previous Next : Disks > Review + create Give feedback

BillieJean@yakubshyn... YAKUBSHYN ORG (YAKUBSHY...)

Errors

Summary Raw Error

ERROR TYPE

Deployment failed with multiple errors: 'Authorization failed for template resource 'sample797_z1' of type 'Microsoft.Network/networkInterfaces'. The client 'BillieJean@yakubshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/networkInterfaces/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/networkInterfaces/sample797_z1'.:Authorization failed for template resource 'Sample-nsg' of type 'Microsoft.Network/networkSecurityGroups'. The client 'BillieJean@yakubshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/networkSecurityGroups/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/networkSecurityGroups/Sample-nsg'.:Authorization failed for template resource 'Sample' of type 'Microsoft.Network/virtualNetworks'. The client 'BillieJean@yakubshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/virtualNetworks/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/virtualNetworks/Sample'.:Authorization failed for template resource 'Sample-ip' of type 'Microsoft.Network/publicIpAddresses'. The client 'BillieJean@yakubshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/publicIpAddresses/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/publicIpAddresses/Sample-ip'.:Authorization failed for template resource 'Sample' of type 'Microsoft.Compute/virtualMachines'. The client 'BillieJean@yakubshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Compute/virtualMachines/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Compute/virtualMachines/Sample'.

(Code: InvalidTemplateDeployment)

Explain with Copilot

Troubleshooting Options

Check Usage + Quota ↗ New Support Request ↗

Give feedback

Tell us about your experience with the ARM Errors page ↗

As expected

Microsoft Azure

Home > Resource groups >

Resource groups

Sample Resource group

Search: Sample

+ Create Manage view ...

Filter for any field...

Name ↑

NetworkWatcherRG ...

Sample

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

+ Create Manage view ...

Search: Sample

+ Create Manage view ...

Search resources, services, and docs (G+)

Copilot

Subscription (move) : Azure for Students

Subscription ID : 3a612e70-8e22-4425-b3ea-29f6ac932428

Tags (edit) : Add tags

Deployments : No deployments

Location : East US

Essentials

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Showing 0 to 0 of 0 records. Show hidden types

Name ↑ Type ↑

No grouping List view

No resources match your filters

Try changing or clearing your filters.

Create resources Clear filters

Learn more

Page 1 of 1

Give feedback

Logged in as an Admin

Microsoft Azure

Home > Resource groups > Sample

Resource groups

Sample Resource group

Search: Sample

+ Create Manage view ...

Filter for any field...

Name ↑

NetworkWatcherRG ...

Sample

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

+ Create Manage view ...

Search resources, services, and docs (G+)

Copilot

assignments - Sample

Current role assignments Eligible assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2)

Role	Description	Scope	Group assignment	Condition
Contributor	Grants full access to manage all resources in this resource.	This resource	Admins	None
Reader	View all resources, but does not change them.	Subscription (Inherited)	Admins	None

Deny assignments (0)

Classic administrators (0)

Check access Role assignments Roles Deny assignments Classic administrators

My access View my level of access to this resource.

View my access

Check access Review the level of access a user, group, service principal, or managed identity has to this resource.

Check access

Grant access to this resource Grant access to resources by assigning a role.

Add role assignment

View access to this resource View the role assignments that grant access to this and other resources.

View

New! Permissions Management Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management.

Get started

Page 1 of 1

Practical Task 4: Securing Sensitive Information with Azure Key Vault

Set up Azure Key Vault to securely store and manage sensitive information such as keys, secrets, and certificates.

1. Create a new Azure Key Vault in your subscription.

The screenshot shows the Microsoft Azure Key Vault service page. At the top, there's a navigation bar with 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user profile. Below the navigation is a breadcrumb trail: 'Home > Create a resource > Marketplace >'. The main title is 'Key Vault' with a 'Microsoft Azure Service' badge and a '4.1 (689 ratings)' star rating. A 'Create' button is visible. The page content includes sections for 'Enhance data protection and compliance', 'All of the control, none of the work', and 'Boost performance and achieve global scale'. It also features a 'Media' section with a thumbnail image of the Azure portal interface. The URL 'https://portal.azure.com/#' is visible at the bottom of the browser window.

Home > Create a resource > Marketplace > Key Vault >

Create a key vault ...

[Basics](#) [Access configuration](#) [Networking](#) [Tags](#) [Review + create](#)

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, Key Vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure for Students
Resource group *	Sample
	Create new

Instance details

Key vault name *	YakubshynKeyVault
Region *	East US
Pricing tier *	Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft delete	Enabled
Days to retain deleted vaults *	90
Protection	<input checked="" type="radio"/> Disable purge protection (allow key vault and objects to be purged during retention period) <input type="radio"/> Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

[Previous](#) [Next](#) [Review + create](#)

Search resources, services, and docs (G+)

goldyakub@kp.ua
YAKUBSHYN.ORG

Home >

YakubshynKeyVault | Overview



Search resources, services, and docs (G+)



Deployment

Search



Delete



Cancel



Redeploy



Download



Refresh

Overview

Inputs

Outputs

Template



Deployment



Deployment

Deployment is in progress

Deployment name : YakubshynKeyVault

Subscription : Azure for Students

Resource group : Sample

Start time : 1/1/2025, 2:48:32 PM

Correlation ID : 55454180-5cd0-4ce2-87c1-05bc0eb163ee

Deployment details

Resource	Type	Status	Operation details
YakubshynKeyVault	Key vault	OK	Operation details

Give feedback

[Tell us about your experience with deployment](#)

Microsoft Defender for Cloud

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials

[Start learning today >](#)

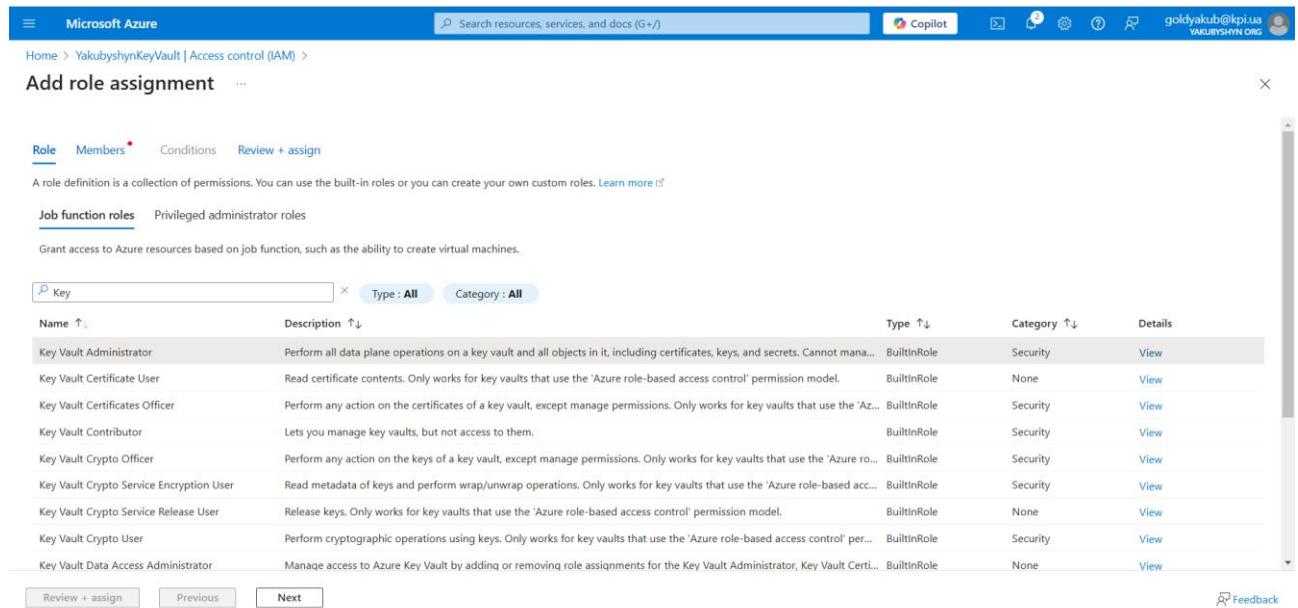
Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

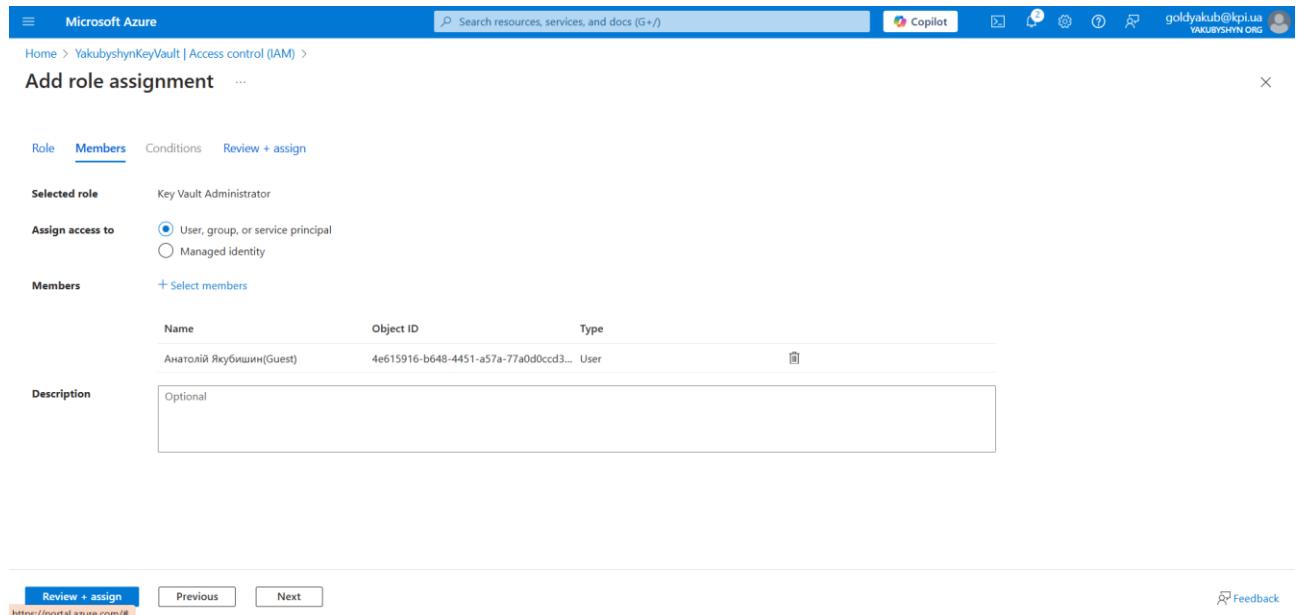
[Find an Azure expert >](#)

2. Add a secret to the Key Vault (e.g., a database connection string).

Before doing this, it is needed to assign myself as the "Key Vault Administrator" role (<https://learn.microsoft.com/en-us/answers/questions/1370440/azure-keyvault-the-operation-is-not-allowed-by-rba>)



The screenshot shows the 'Add role assignment' page for the 'Key' role in Microsoft Azure. The 'Members' tab is selected. The table lists various Azure roles under the 'Job function roles' category, all of which are 'Privileged administrator roles'. The 'Key Vault Administrator' role is highlighted. The table columns are: Name, Description, Type, Category, and Details. The 'Details' column for the Key Vault Administrator shows 'Security' and 'View'. At the bottom of the page are 'Review + assign', 'Previous', and 'Next' buttons.



The screenshot shows the 'Add role assignment' page with the 'Members' tab selected. A 'Selected role' section shows 'Key Vault Administrator'. An 'Assign access to' section has 'User, group, or service principal' selected. A 'Members' section shows 'Анатолий Якубшин(Guest)' selected. A 'Description' section contains the text 'Optional'. At the bottom are 'Review + assign', 'Previous', and 'Next' buttons.

The screenshot shows the Microsoft Azure Key Vault Secrets page. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects, Keys, Certificates, Settings, Monitoring, Automation, and Help. The 'Secrets' option is selected. The main area has a table with columns: Name, Type, Status, and Expiration date. A message says 'There are no secrets available.' At the top, there are buttons for Generate/Import, Refresh, Restore Backup, View sample code, and Manage deleted secrets.

Then click Generate/Import

The screenshot shows the 'Create a secret' dialog box. It has fields for Name (set to 'my-secret'), Secret value (set to '*****'), Content type (optional), Set activation date (unchecked), Set expiration date (unchecked), Enabled (set to Yes), and Tags (0 tags). At the bottom, there are 'Create' and 'Cancel' buttons.

Then click Create

The screenshot shows the Microsoft Azure Key Vault interface. The left sidebar is collapsed, and the main area displays the 'Secrets' section. A message at the top states: 'The secret 'my-secret' has been successfully created.' Below this, a table lists the secret 'my-secret' with columns for Name, Type, Status, and Expiration date. The status is marked as 'Enabled'. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects, Keys, Secrets (which is selected), Certificates, Settings, Monitoring, Automation, and Help.

3. Set access policies to grant the Application Developer role (assigned to the Developers group) permission to retrieve secrets from the Key Vault.

Settings->Access configuration-> vault Access policy

The screenshot shows the Microsoft Azure Key Vault 'Access configuration' page. The left sidebar is collapsed, and the main area shows the 'Permission model' section. It indicates that data plane access is granted using a 'Vault access policy'. A warning message states: 'WARNING: You are changing the permission model. This may immediately change users and services that are allowed to access this key vault. You may proceed if this key vault is new, not used in production workloads, or if you are undoing a previous change. Otherwise it's strongly recommended that you perform this action in the beginning of your own planned maintenance event, during which you can test the new configuration and undo if necessary.' A blue button labeled 'Go to access policies' is visible.

Update for main user

Microsoft Azure

Home > YakubshynKeyVault | Access policies >

Create an access policy ...

YakubshynKeyVault

Permissions Principal Application (optional) Review + create

Configure from a template

Select a template

Key permissions	Secret permissions	Certificate permissions
<input checked="" type="checkbox"/> Select all	<input checked="" type="checkbox"/> Select all	<input checked="" type="checkbox"/> Select all
<input checked="" type="checkbox"/> Get	<input checked="" type="checkbox"/> Get	<input checked="" type="checkbox"/> Get
<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> List
<input checked="" type="checkbox"/> Update	<input checked="" type="checkbox"/> Set	<input checked="" type="checkbox"/> Update
<input checked="" type="checkbox"/> Create	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Create
<input checked="" type="checkbox"/> Import	<input checked="" type="checkbox"/> Recover	<input checked="" type="checkbox"/> Import
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Backup	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> Recover	<input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Recover
<input checked="" type="checkbox"/> Backup		<input checked="" type="checkbox"/> Backup
<input checked="" type="checkbox"/> Restore		<input checked="" type="checkbox"/> Restore

Previous Next

Microsoft Azure

Home > YakubshynKeyVault | Access policies >

Create an access policy ...

YakubshynKeyVault

Permissions Principal Application (optional)

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous

Search

Select a directory member by entering object ID, name or email address

78 results found

All Users Groups Enterprise applications

Name	Type	Details
Анатолий Якубшин	User	goldyakub@kpi.ua
AAD Request Verification Service - PROD c728155f-7b2a-4502-a08b-b8af9b269319	Enterprise application	f0ae4899-d877-4d3c-ae25-679e38eea492
AADReporting 1b912ec3-a9dd-4c4d-a53e-76aa7adb28d7	Enterprise application	c728155f-7b2a-4502-a08b-b8af9b269319
Admins	Group	
Billie Jean	User	BillieJean@yakubshyn.onmicrosoft.com
Developers	Group	

Selected item

No item selected

Selected (1)

Анатолий Якубшин
goldyakub@kpi.ua

Previous Next Select

Then next, next review and create

Microsoft Azure

Home > YakubshynKeyVault | Access policies >

Create an access policy

YakubshynKeyVault

Permissions **Principal** **Application (optional)** **Review + create**

Configure from a template

Select a template

Key permissions	Secret permissions	Certificate permissions
Key Management Operations <input type="checkbox"/> Select all <input type="checkbox"/> Get <input type="checkbox"/> List <input type="checkbox"/> Update <input type="checkbox"/> Create <input type="checkbox"/> Import <input type="checkbox"/> Delete <input type="checkbox"/> Recover <input type="checkbox"/> Backup <input type="checkbox"/> Restore	Secret Management Operations <input type="checkbox"/> Select all <input checked="" type="checkbox"/> Get <input checked="" type="checkbox"/> List <input type="checkbox"/> Set <input type="checkbox"/> Delete <input type="checkbox"/> Recover <input type="checkbox"/> Backup <input type="checkbox"/> Restore	Certificate Management Operations <input type="checkbox"/> Select all <input type="checkbox"/> Get <input type="checkbox"/> List <input type="checkbox"/> Update <input type="checkbox"/> Create <input type="checkbox"/> Import <input type="checkbox"/> Delete <input type="checkbox"/> Recover <input type="checkbox"/> Backup <input type="checkbox"/> Restore <input type="checkbox"/> Manage Contacts <input type="checkbox"/> Manage Certificate Authorities <input type="checkbox"/> Get Certificate Authorities
Cryptographic Operations <input type="checkbox"/> Select all <input type="checkbox"/> Decrypt	Privileged Secret Operations <input type="checkbox"/> Select all <input type="checkbox"/> Purge	

Previous **Next**

Microsoft Azure

Home > YakubshynKeyVault | Access policies >

Create an access policy

YakubshynKeyVault

Permissions **Principal** **Application (optional)** **Review + create**

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

- AAD Request Verification Service - PROD
c728155f-7b2a-4502-a0b8-b8af9b269319
- AADReporting
fb912ec3-a9dd-4c4d-a53e-76aa7adb28d7
- acapi
c5b17a4f-cc6f-4649-9480-884280a2af3a

Selected item

Developers

https://portal.azure.com/#

Microsoft Azure

Home > YakubshynKeyVault

YakubshynKeyVault | Access policies

Key vault

Search **Create** Refresh Delete Edit

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

Showing 1 to 2 of 2 records.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
Developers		Get, List		
Андрій Якубшин	goldyakub_kpi.ua#EXT#@yakubshy...	Get, List, Update, Create, ...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create, Import, Del...

Microsoft Azure

Home > YakubivhKeyVault | Access control (IAM) >

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more ↗

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name	Description	Type	Category	Details
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vault resources or manage...	BuiltinRole	Security	View
Key Vault Certificate User	Read certificate contents. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	None	View
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Key Vault Contributor	Lets you manage key vaults, but not access to them.	BuiltinRole	Security	View
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	None	View
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administrator, Key Vault Certificates Officer, Key Vault Crypto ...	BuiltinRole	None	View
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material. Only works for key v...	BuiltinRole	Security	View
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	Security	View
Operator Nexus Key Vault Writer Service Role (Preview)	(Preview) Provides Azure Operator Nexus services the ability to write to a Key Vault. This role is in preview and subject to change.	BuiltinRole	None	View

Showing 1 - 13 of 13 results.

Review + assign Previous Next Feedback

Microsoft Azure

Home > YakubivhKeyVault | Access control (IAM) >

Add role assignment

Role Members Conditions Review + assign

Selected role Key Vault Reader

Assign access to User, group, or service principal Managed identity

Members + Select members

Name	Object ID	Type
Developers	b23e4820-3a75-449f-89ad-0bae70161d...	Group

Description Optional

Review + assign Previous Next Feedback

https://central.azure.com/#/

4. Verify that only members of the Developers group can access the stored secret.

The screenshot shows the Microsoft Azure portal interface for a Key Vault. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user profile for 'BillieJean@yakubshyn...'. Below the navigation is a breadcrumb trail: 'Home > YakubshynKeyVault | Secrets > my-secret >'. The main content area displays a secret named '38f3dcbdc60a411a8cceaffb47e29fa2'. The 'Properties' section shows the secret was created and updated on 1/1/2025 at 3:08:03 PM. It has a 'Secret identifier' of <https://yakubshynkeyvault.vault.azure.net/secrets/my-secret/38f3dcbdc60a411a8cceaffb47e29fa2>. Under 'Settings', there are options for 'Set activation date' and 'Set expiration date', both currently set to 'No'. The 'Enabled' switch is turned 'Yes'. There are 0 tags. The 'Secret' section contains a text input field with 'secret' typed into it. A 'Hide Secret Value' button is visible. At the bottom are 'Apply', 'Discard changes', and 'Close' buttons, along with a 'Give feedback' link.

Developer (Billie Jean) can see secret content

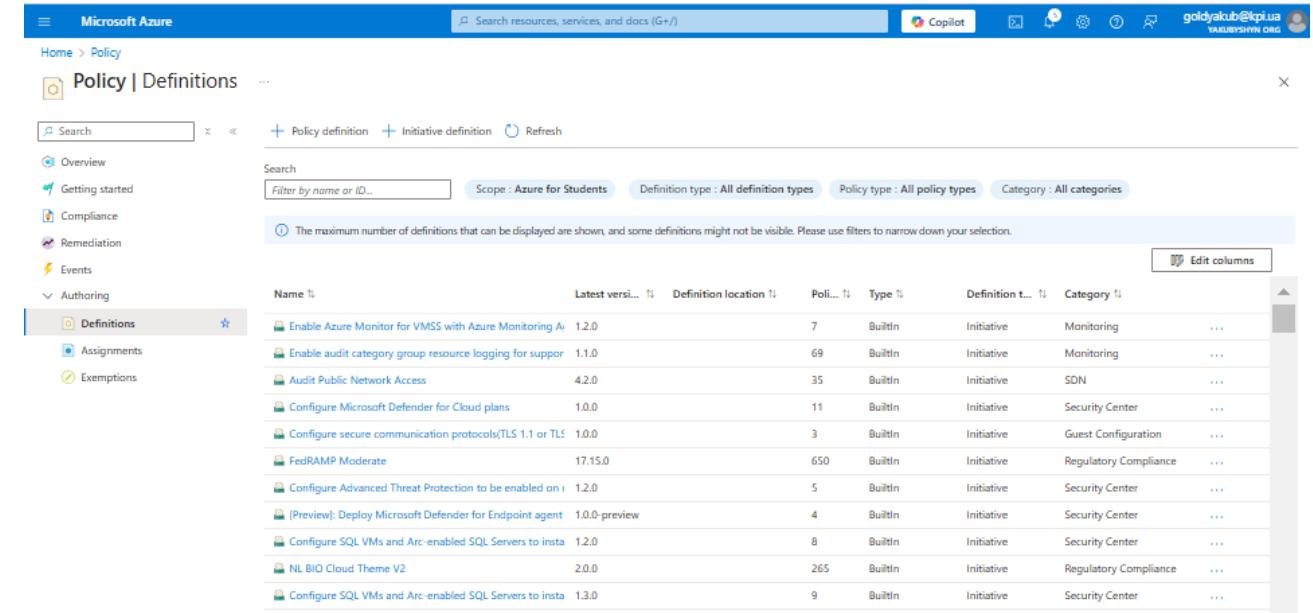
The screenshot shows the Microsoft Azure portal interface for a Key Vault. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user profile for 'JoeDoe@yakubshyn...'. Below the navigation is a breadcrumb trail: 'Home > YakubshynKeyVault | Secrets > ...'. The left sidebar menu is open, showing options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Access policies', 'Events', 'Objects', 'Keys', 'Certificates', 'Settings', 'Monitoring', 'Automation', and 'Help'. The 'Certificates' item is currently selected. The main content area shows a table for managing secrets. The table has columns for 'Name', 'Type', 'Status', and 'Expiration date'. A message at the top of the table area states: '⚠️ The operation "List" is not enabled in this key vault's access policy.' and 'You are unauthorized to view these contents.' At the bottom right is a 'Give feedback' link.

Admins even can't list secrets

Practical Task 5: Creating and Assigning Basic Azure Policies

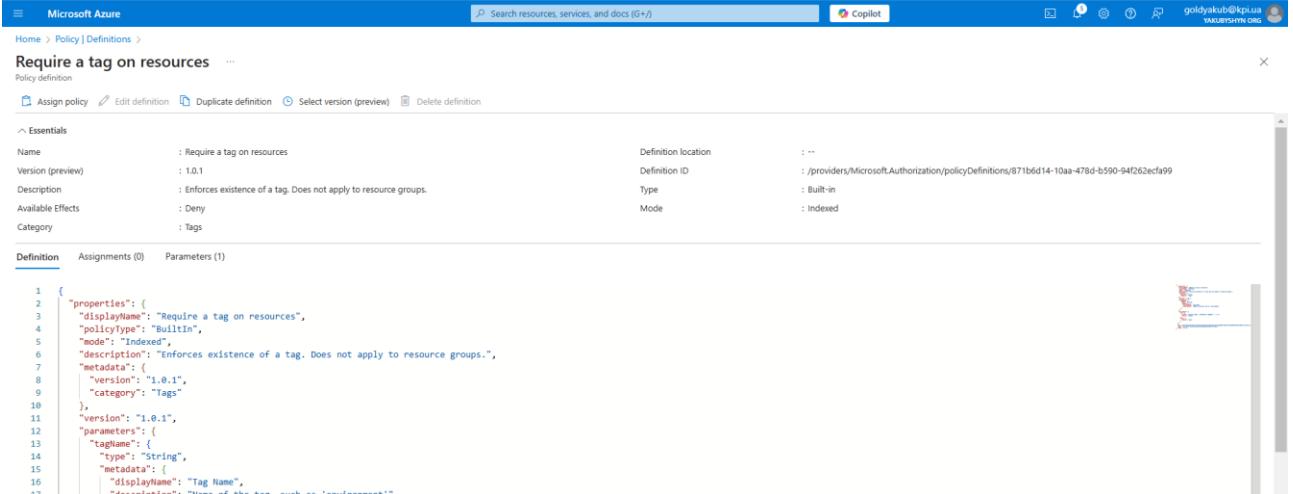
Define and assign Azure Policies to enforce compliance with organizational standards for resource management.

1. Create an Azure Policy to enforce tagging for all newly created resources with a specific tag (e.g., Environment: Development).



The screenshot shows the Microsoft Azure Policy Definitions page. The left sidebar has sections for Overview, Getting started, Compliance, Remediation, Events, and Authoring. Under Authoring, 'Definitions' is selected. The main area displays a table of policy definitions:

Name	Latest version	Definition location	Type	Definition type	Category
Enable Azure Monitor for VMS with Azure Monitoring	1.2.0	Builtin	Initiative	Monitoring	Monitoring
Enable audit category group resource logging for supper	1.1.0	Builtin	Initiative	Monitoring	Monitoring
Audit Public Network Access	4.2.0	Builtin	Initiative	SDN	SDN
Configure Microsoft Defender for Cloud plans	1.0.0	Builtin	Initiative	Security Center	Security Center
Configure secure communication protocols(TLS 1.1 or TLS 1.2)	1.0.0	Builtin	Initiative	Guest Configuration	Guest Configuration
FedRAMP Moderate	17.15.0	Builtin	Initiative	Regulatory Compliance	Regulatory Compliance
Configure Advanced Threat Protection to be enabled on i	1.2.0	Builtin	Initiative	Security Center	Security Center
[Preview]: Deploy Microsoft Defender for Endpoint agent	1.0.0-preview	Builtin	Initiative	Security Center	Security Center
Configure SQL VMs and Arc-enabled SQL Servers to insta	1.2.0	Builtin	Initiative	Security Center	Security Center
NL BIO Cloud Theme V2	2.0.0	Builtin	Initiative	Regulatory Compliance	Regulatory Compliance
Configure SQL VMs and Arc-enabled SQL Servers to insta	1.3.0	Builtin	Initiative	Security Center	Security Center



The screenshot shows the 'Require a tag on resources' policy definition creation page. The 'Essentials' section contains the following details:

Name	: Require a tag on resources	Definition location	: --
Version (preview)	: 1.0.1	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/871b6d14-10aa-478d-b590-94f262ecfa99
Description	: Enforces existence of a tag. Does not apply to resource groups.	Type	: Built-in
Available Effects	: Deny	Mode	: Indexed
Category	: Tags		

The 'Definition' tab shows the JSON code for the policy:

```
1 {
2   "properties": {
3     "displayName": "Require a tag on resources",
4     "policyType": "Builtin",
5     "mode": "Indexed",
6     "description": "Enforces existence of a tag. Does not apply to resource groups.",
7     "metadata": {
8       "version": "1.0.1",
9       "category": "Tags"
10    },
11    "version": "1.0.1",
12    "parameters": {
13      "tagName": {
14        "type": "String",
15        "metadata": {
16          "displayName": "Tag Name",
17          "description": "Name of the tag, such as \"environment\""
18        }
19      }
20    }
21 }
```

2. Assign the policy to a resource group.

The screenshot shows the 'Assign policy' page in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user account. The main title is 'Assign policy'. Below it, the 'Basics' tab is selected, showing fields for 'Scope' (set to 'Azure for Students/Sample'), 'Exclusions' (empty), 'Policy definition' (set to 'Require a tag on resources'), 'Version (preview)' (set to '1.0.*'), 'Overrides' (empty), 'Assignment name' (empty), 'Description' (empty), and 'Policy enforcement' (set to 'Enabled'). At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Review + create' button.

The screenshot shows the 'Assign policy' page in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user account. The main title is 'Assign policy'. Below it, the 'Parameters' tab is selected, showing a search bar for 'Search by parameter name' and a checkbox for 'Only show parameters that need input or review'. A field for 'Tag Name' is set to 'Environment'. At the bottom, there are 'Previous' and 'Next' buttons, and a blue 'Review + save' button.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

golodiyakub@kpi.ua
YAKUBISHIN Oleg

Home > Policy | Assignments > Require a tag on resources >

Assign policy ...

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope	Azure for Students/Sample
Exclusions	--
Policy definition	Require a tag on resources
Assignment name	Require a tag on resources
Version (preview)	1.0.*
Description	--
Policy enforcement	Enabled
Assigned by	Анатолий Якубышин

Advanced

Resource selectors	No selectors associated with this assignment.
Overrides	No overrides associated with this assignment.

Parameters

Tag Name	Environment
----------	-------------

Remediation

Create a Managed Identity	No managed identity associated with this assignment.
---------------------------	--

Non-compliance messages

Non-compliance messages	No non-compliance messages associated with this assignment.
-------------------------	---

Previous Next Save Give feed!

Creating policy assignment succeeded



Creating policy assignment 'Require a tag on resources' in 'Azure for Students/Sample' was successful. Please note that the assignment takes around 5-15 minutes to take effect.

a few seconds ago

3. Verify that any new resource created in the resource group without the required tag is marked as non-compliant.

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. On the left, the 'Create a virtual machine' wizard is open, with the 'Review + create' step selected. A validation error message at the top states: 'Validation failed. Click here to view details... →'. Below this, three buttons are visible: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. The 'Tags' tab is highlighted. On the right, an 'Errors' panel is displayed, showing a single error: 'Resource 'sample830_z3' was disallowed by policy. (Code: RequestDisallowedException)'. It also includes a link to 'Policy: Require a tag on resources'. Other sections in the errors panel include 'Summary', 'Raw Error', 'ERROR DETAILS', 'WAS THIS HELPFUL?', 'Explain with Copilot', 'Troubleshooting Options', and 'Give feedback'.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
Environment	Dev	13 selected
		13 selected

< Previous Next : Review + create > Review + create

https://portal.azure.com/#

Give feedback

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Validation passed

Price

1 X Standard D2s v3 by Microsoft Subscription credits apply 0.0960 USD/hr Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name: Анатолий Якубович
Preferred e-mail address: goldyakub@kpi.ua
Preferred phone number:

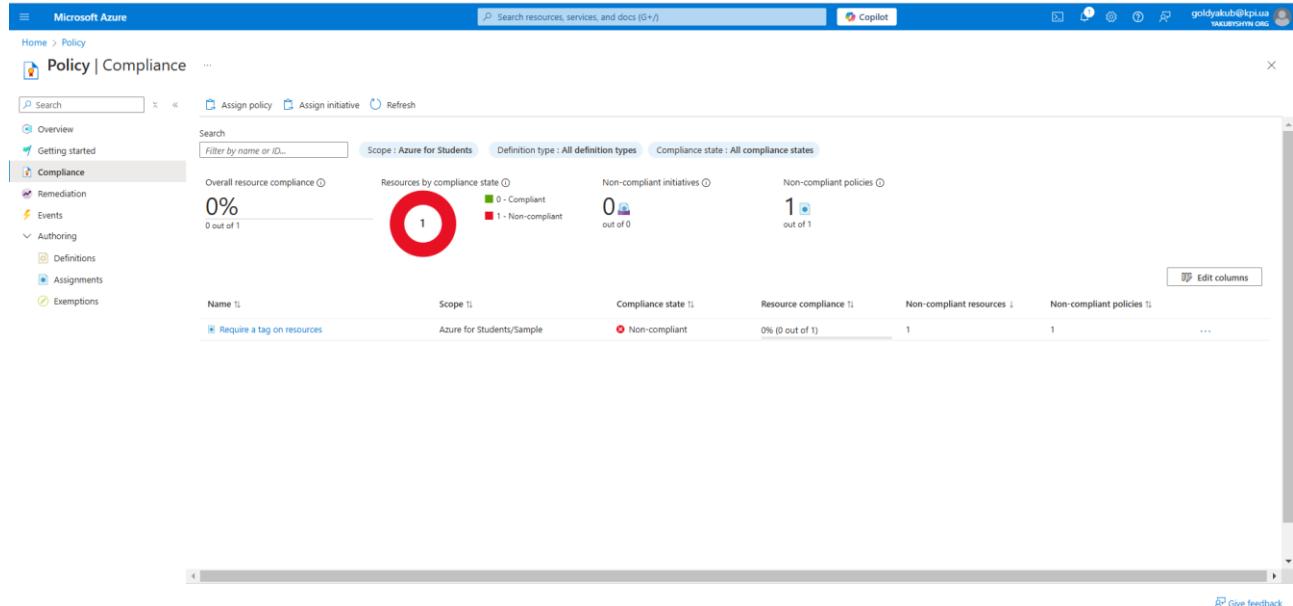
You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

< Previous Next > Create

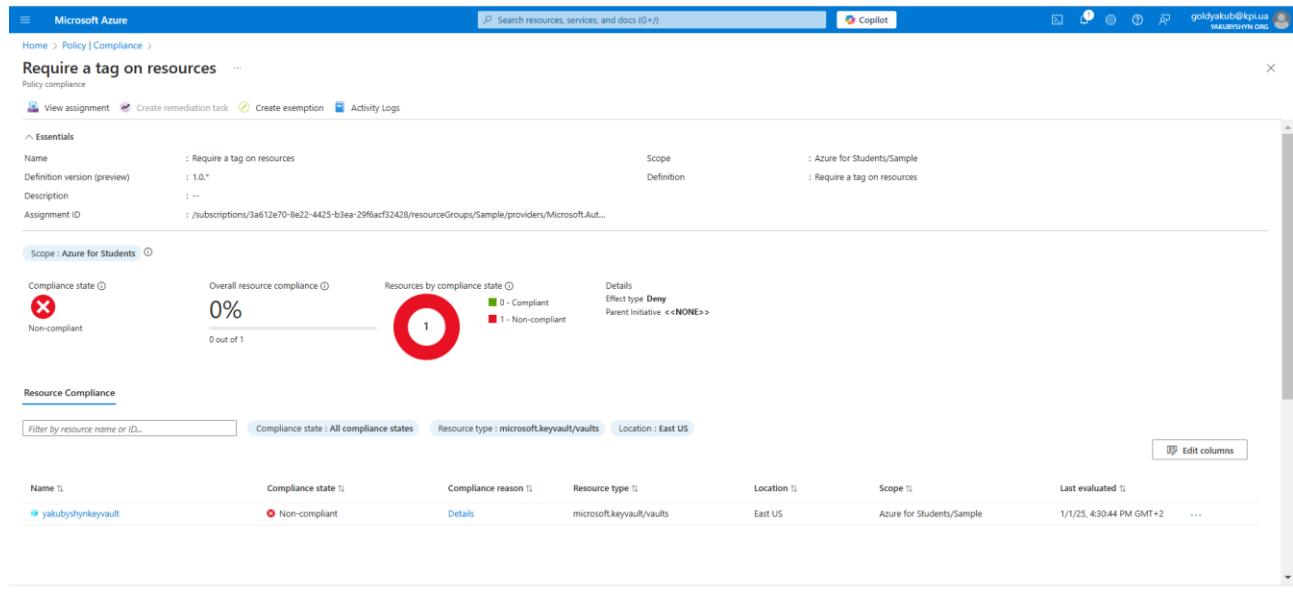
Download a template for automation Give feedback

4. Review and document the compliance status of the resource group.



The screenshot shows the Microsoft Azure Policy | Compliance dashboard. The main summary indicates 0% overall resource compliance for the scope "Azure for Students". It shows 1 resource, all of which are non-compliant. There are 0 non-compliant initiatives and 1 non-compliant policy. A table below provides detailed information about the single non-compliant resource.

Name	Scope	Compliance state	Resource compliance	Non-compliant resources	Non-compliant policies
Require a tag on resources	Azure for Students/Sample	Non-compliant	0% (0 out of 1)	1	1



The screenshot shows the details of the "Require a tag on resources" policy definition. The policy name is "Require a tag on resources", version 1.0.0, and it applies to the scope "Azure for Students/Sample". The policy is non-compliant. Below the policy details, there is a summary of the compliance status for the scope "Azure for Students", showing 0% overall compliance with 1 non-compliant resource. A table at the bottom lists the resource compliance for the vault "yakubsynkeyvault".

Name	Compliance state	Compliance reason	Resource type	Location	Scope	Last evaluated
yakubsynkeyvault	Non-compliant	Details	microsoft.keyvault/vaults	East US	Azure for Students/Sample	1/1/25, 4:30:44 PM GMT+2

As expected (because was created before this policy)

Practical Task 6: Using Policy Effects to Enforce Compliance

Configure Azure Policies with different policy effects to enforce compliance and manage resources according to organizational standards.

1. Create a policy with the Audit effect to monitor and log untagged resources within a resource group.

```
1 {  
2   "properties": {  
3     "displayName": "Audit Resources Without Tags",  
4     "policyType": "Custom",  
5     "mode": "Indexed",  
6     "description": "Audits resources that do not have any tags.",  
7     "metadata": {  
8       "version": "1.0.0",  
9       "category": "Tags"  
10    },  
11    "parameters": {},  
12    "policyRule": {  
13      "if": {  
14        "field": "tags",  
15        "exists": false  
16      },  
17      "then": {  
18        "effect": "Audit"  
19      }  
20    }  
21  }  
22 }  
23 }
```

The screenshot shows the Azure portal's 'Policy definition' creation page. The 'Policy Rule' section contains the JSON code provided above. The 'Category' dropdown is set to 'Azure for Students'. At the bottom, a success message says 'Creating policy definition succeeded'.

Creating policy definition succeeded

Creating policy definition 'Audit Resources Without Tags' in 'Azure for Students' was successful.

a few seconds ago

Review+create -> create

Made a mistake in policy definition

```

1  {
2    "mode": "Indexed",
3    "policyRule": {
4      "if": {
5        "field": "tags",
6        "exists": "false"
7      },
8      "then": [
9        {
10          "effect": "audit"
11        }
12      ],
13      "parameters": {}
14    }
15  }

```

Corrected version

<https://techcommunity.microsoft.com/discussions/azuregovernance/azure-policy---find-ressources-without-tags/3289179>

changed exists “false” to exists “true” to see as non-compliant

```
"policyRule": {  
    "if": {  
        "field": "tags",  
        "exists": "true"  
    },  
    "then": {  
        "effect": "audit"  
    }  
},  
"versions": [  
    "1.0.0"  
]
```

},

But then changed back because compliant is expected status

IF parameter exists is ‘false’

The screenshot shows the Azure Policy Compliance blade. On the left, there's a navigation menu with 'Compliance' selected. The main area displays compliance statistics: Overall resource compliance at 0%, 0 out of 1 resource is non-compliant, and 1 non-compliant policy out of 2. Below this, a table lists two resources. The first resource, 'Require a tag on resources', has a scope of 'Azure for Students/Sample' and is marked as 'Non-compliant' with 0% compliance. The second resource, 'Audit Resources Without Tags', also has a scope of 'Azure for Students/Sample' and is marked as 'Compliant' with 100% compliance. A red circle highlights the 'Non-compliant' status of the first resource.

Name	Scope	Compliance state	Resource compliance	Non-compliant resources	Non-compliant policies
Require a tag on resources	Azure for Students/Sample	Non-compliant	0% (0 out of 1)	1	1
Audit Resources Without Tags	Azure for Students/Sample	Compliant	100% (1 out of 1)	0	0

As a result (false) as it should be

2. Create a policy with the DeployIfNotExists effect to automatically add a specific tag (Owner: IT) to any newly created resource.

```
{  
    "mode": "Indexed",  
    "policyRule": {  
        "if": {  
            "field": "tags.Owner",  
            "exists": "false"  
        },  
        "then": {  
            "effect": "DeployIfNotExists",  
            "details": {  
                "tags": {  
                    "Owner": "IT"  
                }  
            }  
        }  
    }  
}
```

```
 "then": {         "effect": "deployIfNotExists",         "details": {             "type": "Microsoft.Resources/tags",             "deployment": {                 "properties": {                     "mode": "Incremental",                     "template": {                         "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",                         "contentVersion": "1.0.0.0",                         "resources": [                             {                                 "type": "Microsoft.Resources/tags",                                 "apiVersion": "2019-10-01",                                 "properties": {                                     "tags": {                                         "Owner": "IT"                                     }                                 }                             }                         ]                     }                 }             }         }     },     "parameters": {} } |
```

Then I assigned policy:

The screenshot shows the Microsoft Azure Policy Assignments blade. The policy definition 'Deploy Owner Tag If Not Exists' is selected. The 'Assign policy' step is active. The 'Basics' tab is selected, showing the scope as 'Azure for Students/Sample' and the policy definition as 'Deploy Owner Tag If Not Exists'. The 'Copilot' feature is visible on the right side of the screen.

The screenshot shows the Azure Policy assignments interface. At the top, there are buttons for 'Assign policy', 'Assign initiative', and 'Refresh'. Below that is a search bar with 'Filter by name or ID...' and a scope dropdown set to 'Azure for Students'. The definition type is set to 'All definition types'. There are three sections: 'Total Assignments' (3), 'Initiative Assignments' (0), and 'Policy Assignments' (3). The table below lists the three policies assigned to 'Azure for Students/Sample'.

Assignment name	Scope	Type
Audit Resources Without Tags	Azure for Students/Sample	Policy
Require a tag on resources	Azure for Students/Sample	Policy
Deploy Owner Tag If Not Exists	Azure for Students/Sample	Policy

3. Assign these policies to a resource group and verify their behavior by:

Creating a resource without a tag and checking the compliance logs.

Creating a resource to validate the automatic tag deployment

(Created extra Azure Key Vaults)

It doesn't work

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
① 'deployIfNotExists' Policy action.	Failed	22 minutes ...	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
② Update Key Vault	Started	38 minutes ...	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
③ 'deployIfNotExists' Policy action.	Started	38 minutes ...	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
④ Update Key Vault	Accepted	38 minutes ...	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
⑤ Update Key Vault	Succeeded	28 minutes ...	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua

. The request to retrieve resources of type 'Microsoft.Resources/tags' failed with HTTP status code

I don't see 'Microsoft.Resources/tags'

In my student subscription

It is possible to do this task using *modify effect*

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/govern-tags>

```
{
  "mode": "Indexed",
  "policyRule": {
    "if": {
      "field": "tags.Owner",
      "equals": "goldiyakub"
    }
  }
}
```

```

    "exists": "false"
},
"then": {
  "effect": "modify",

  "details": {
    "roleDefinitionIds": [
      "/providers/microsoft.authorization/roleDefinitions/b24988ac-6180-42a0-
ab88-20f7382dd24c"
    ],
    "operations": [
      {
        "operation": "add",
        "field": "tags.Owner",
        "value": "IT"
      }
    ]
  }
},
"parameters": {}
}

```

Assigned this policy

Created vault with name ‘TestingVaultTolia’

I haven’t added Owner tag. But it was added automatically.

Tags

Name	Value
Environment	: QA
Owner	: IT

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Modify	Succeeded	4 minutes ago	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
Modify	Succeeded	4 minutes ago	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua
Create policy assignment	Succeeded	5 minutes ago	Wed Jan 01 ...	Azure for Students	goldiyakub@kpi.ua