



Understanding Roles & Permissions in Microsoft Sentinel

Microsoft Sentinel RBAC
ensures least-privilege access
and clear separation of duties.

Role Overview (Microsoft Docs Table)

- Sentinel includes 5 built-in roles for least-privilege access.
- roles table: Reader, Responder, Contributor, Playbook Operator, Automation Contributor.

Role	SIEM support	Data lake support
Microsoft Sentinel Reader	View data, incidents, workbooks, and other resources	Access advanced analytics and run interactive queries on workspaces only.
Microsoft Sentinel Responder	All Reader permissions, plus manage incidents	N/A
Microsoft Sentinel Contributor	All Responder permissions, plus install/update solutions, create/edit resources	Access advanced analytics and run interactive queries on workspaces only.
Microsoft Sentinel Playbook Operator	List, view, and manually run playbooks	N/A
Microsoft Sentinel Automation Contributor	Allows Microsoft Sentinel to add playbooks to automation rules. Not used for user accounts.	N/A

IAM Overview

- Roles are managed via Access Control (IAM) in the resource group.
- RG-Sentinel Access Control IAM.

The screenshot displays the 'RG-Sentinel | Access control (IAM)' interface. The left sidebar contains a navigation menu with options: Overview, Activity log, Access control (IAM) (selected), Tags, Resource visualizer, Events, Settings, Cost Management, Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations, Monitoring, Automation, and Help. The main content area shows the 'Check access' view for the user 'Perparim Abdullahu'. It includes a summary section with counts for Active (2), Eligible (0), and Deny (0) assignments. Below this is a table of assignments. The table has columns for Role Name, Scope, and Membership. It shows two 'Active permanent assignments' where the user is the 'Owner' with the role 'Subscription (Inherited)'. Other sections for 'Active time-bound assignments', 'Eligible permanent assignments', 'Eligible time-bound assignments', and 'Deny assignments' all show zero counts.

RG-Sentinel | Access control (IAM) ☆ ...

Search

Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Automation
Help

Check access | Role assignments | Roles | Deny assignments | Classic administrators

Looking for the previous check access view? [Click here.](#)

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

[Check access](#)

Perparim Abdullahu Assignments

Active ⓘ	Eligible ⓘ	Deny ⓘ
2	0	0

Search by role name or membership

Role Name ↑↓	Scope ↑↓	Membership ↑↓
Active permanent assignments (2)		
Owner	Subscription (Inherited)	Perparim Abdullahu
Owner	Subscription (Inherited)	Perparim Abdullahu
Active time-bound assignments (0)		
Eligible permanent assignments (0)		
Eligible time-bound assignments (0)		
Deny assignments (0)		

PerparimLabs

Current Assignments

- Azure RBAC
Owner/Contributor may override Sentinel roles.
- role assignments list with Owner + Contributor.

+ Add ▾ Download role assignments Edit columns Refresh Delete Feedback

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription ⓘ 4 4000





Privileged ⓘ 2

[View assignments](#)

Search by name or email

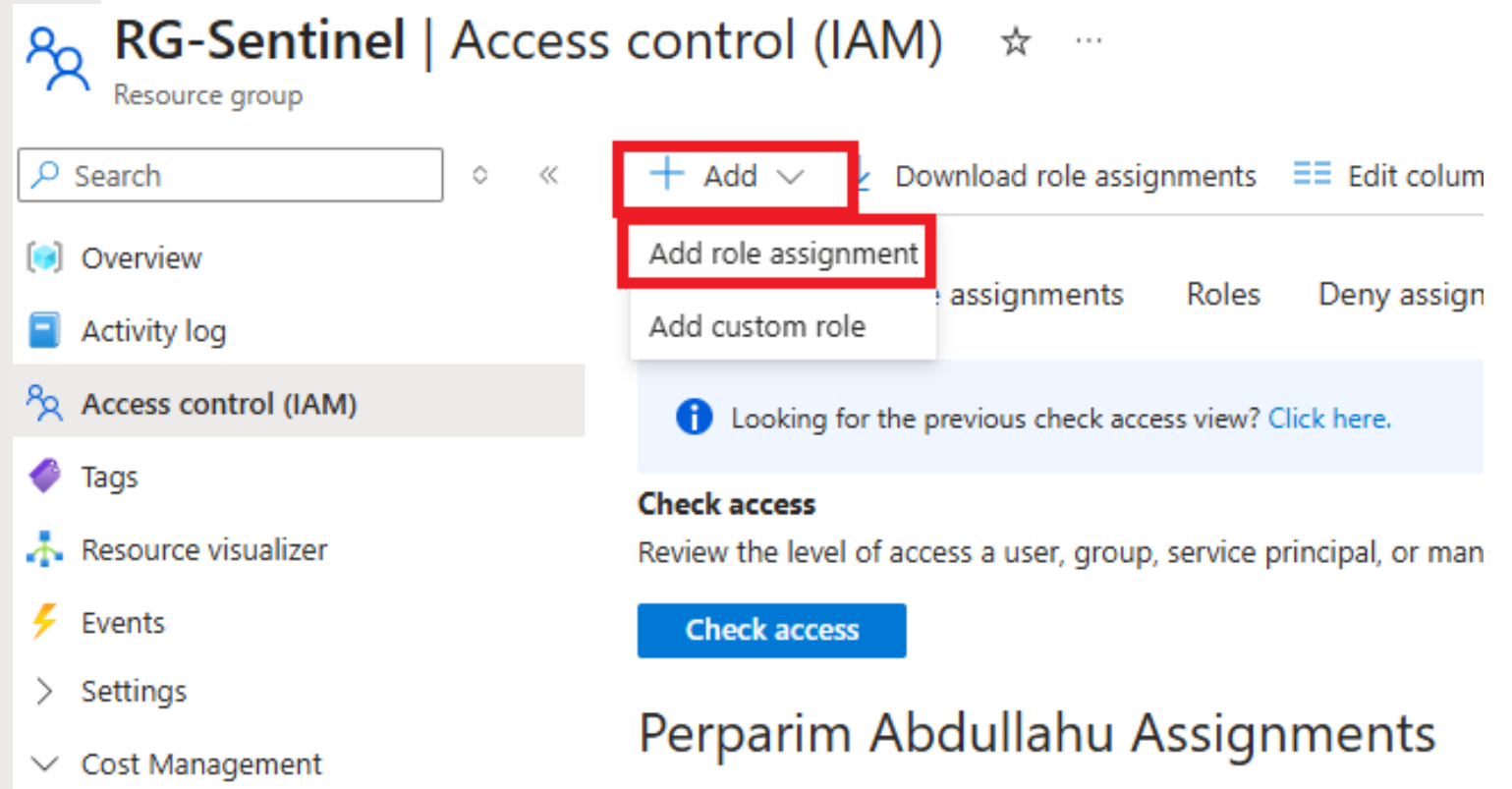
Type: All Role: All Scope: All scopes State: All End time: All Group by: Role

All (4) Job function roles (2) Privileged administrator roles (2)

<input type="checkbox"/>	Name ↑↓	Type ↑↓	Role ↑↓	Scope ↑↓	State ↑↓	End time ↑↓	Condition ↑↓
▼	Owner (2)						
<input type="checkbox"/>	 Perparim Abdullahi padmin@cloudmatearchite...	User	Owner	 Subscription (Inherited)	Active Permanent	Permanent	None
<input type="checkbox"/>	 Perparim Abdullahi padmin@cloudmatearchite...	User	Owner	 Subscription (Inherited)	Active Permanent	Permanent	None
▼	Microsoft Sentinel Contributor (2)						

Add Role Assignment

- Assign Sentinel roles through IAM.
- Add → Role assignment.



The screenshot shows the Azure portal interface for a resource group named 'RG-Sentinel'. The page title is 'Access control (IAM)'. On the left sidebar, the 'Access control (IAM)' option is selected. In the main content area, the '+ Add' button is highlighted with a red box, and its dropdown menu is open, showing 'Add role assignment' and 'Add custom role', with 'Add role assignment' also highlighted by a red box. Other visible elements include a search bar, navigation links for Overview, Activity log, Tags, Resource visualizer, Events, Settings, and Cost Management, and a 'Check access' button.

RG-Sentinel | Access control (IAM) ☆ ...

Resource group

Search

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

+ Add ▾

Download role assignments

Edit column

Add role assignment

Add custom role

Looking for the previous check access view? [Click here.](#)

Check access

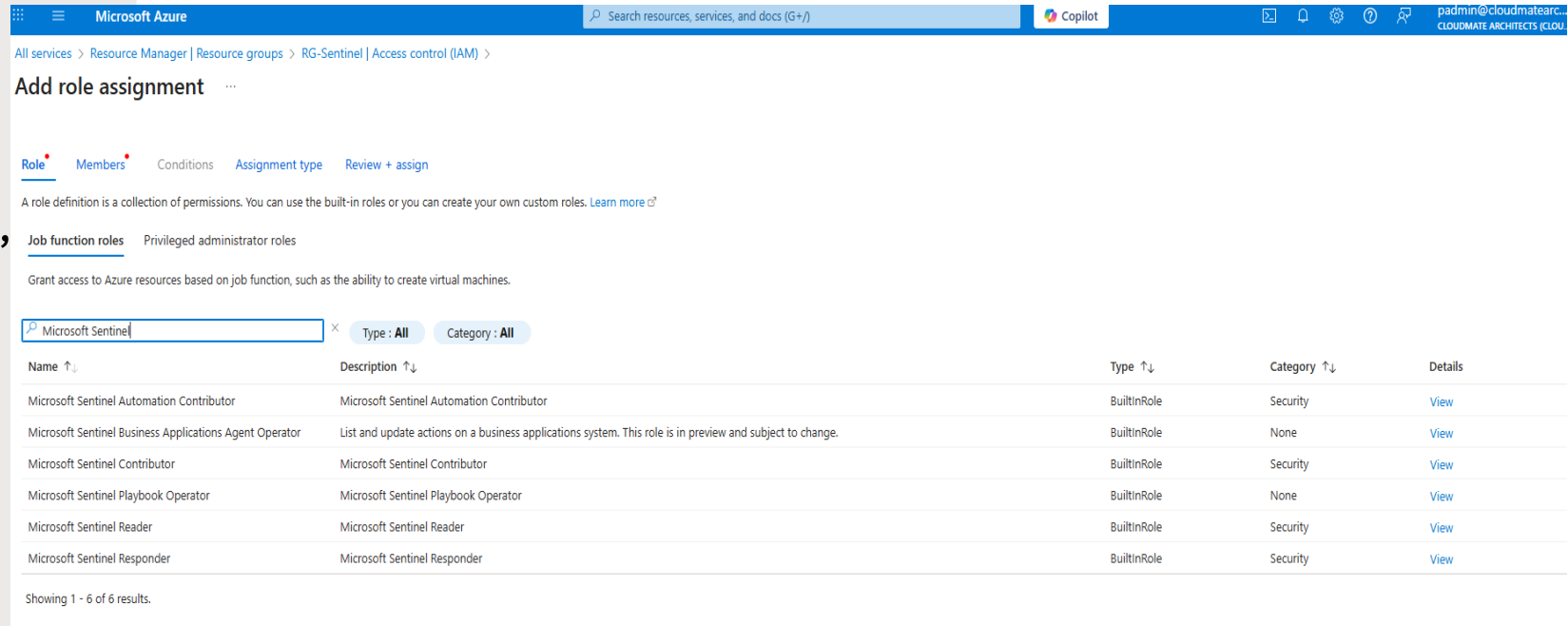
Review the level of access a user, group, service principal, or man

Check access

Perparim Abdullahu Assignments

Filtering Sentinel Roles

- Filter to view all Sentinel roles available.
- search 'Microsoft Sentinel', roles appear.



The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal. The breadcrumb navigation indicates the path: All services > Resource Manager > Resource groups > RG-Sentinel > Access control (IAM). The page title is 'Add role assignment'. Below the title, there are tabs for 'Role', 'Members', 'Conditions', 'Assignment type', and 'Review + assign'. The 'Role' tab is selected. A description states: '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](#)'. Under the 'Job function roles' section, it says 'Privileged administrator roles' and 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' A search bar contains the text 'Microsoft Sentinel'. To the right of the search bar are filters: 'Type : All' and 'Category : All'. Below the search bar is a table with the following columns: Name, Description, Type, Category, and Details. The table lists six roles, all of which are 'BuiltInRole' and categorized under 'Security'.

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Microsoft Sentinel Automation Contributor	Microsoft Sentinel Automation Contributor	BuiltInRole	Security	View
Microsoft Sentinel Business Applications Agent Operator	List and update actions on a business applications system. This role is in preview and subject to change.	BuiltInRole	None	View
Microsoft Sentinel Contributor	Microsoft Sentinel Contributor	BuiltInRole	Security	View
Microsoft Sentinel Playbook Operator	Microsoft Sentinel Playbook Operator	BuiltInRole	None	View
Microsoft Sentinel Reader	Microsoft Sentinel Reader	BuiltInRole	Security	View
Microsoft Sentinel Responder	Microsoft Sentinel Responder	BuiltInRole	Security	View

Showing 1 - 6 of 6 results.

Role Permissions Detail

- Each role grants specific actions. Example: Contributor can create rules and workbooks.
- *Sentinel Contributor permissions list.*

Microsoft Sentinel Contributor

BuiltInRole

[Permissions](#) [JSON](#) [Assignments](#)

Description: Microsoft Sentinel Contributor

Type : All

Permission Type

☒ Actions ☐ DataActions

Showing 500 of 1100 permissions [View all](#) (will take a moment to load)

Type	Permissions	Description
Microsoft.Authorization		
Read	Acquire policy token operation ⓘ	Acquire a policy token at the specified scope.
Read	Get administrator ⓘ	Reads the administrators for the subscription.
Read	Get administrator operation statuses ⓘ	Gets the administrator operation statuses of the subscription.
Read	Get deny assignment ⓘ	Get information about a deny assignment.
Read	Read the information about diagnostic settings categories ⓘ	Get the information about diagnostic settings categories
Read	Get information about diagnostics settings ⓘ	Read the information about diagnostics settings
Read	Get Role eligibility schedule instance ⓘ	Gets the role eligibility schedule instances at given scope.
Read	Get management locks ⓘ	Gets locks at the specified scope.
Read	Get operations ⓘ	Gets the list of operations
Read	List permissions ⓘ	Lists all the permissions the caller has at a given scope.
Read	Get policy assignment ⓘ	Get information about a policy assignment.
Read	Get Private Link Association ⓘ	Get information about private link association.
Read	Get Resource Management Private Link ⓘ	Get information about resource management private link.
Read	Get Private Endpoint Connection ⓘ	Get information about private endpoint connection.
Read	Get Private Endpoint Connection Proxy ⓘ	Get information about private endpoint connection proxy.

 PerparimLabs

Assigning to User

- Assign a role to a user or group with defined scope.
- Review + assign with member selected.

[All services](#) > [Resource Manager | Resource groups](#) > [RG-Sentinel | Access con](#)

Add role assignment ...

[Role](#) [Members](#) [Conditions](#) [Assignment type](#) [Review + assign](#)

Role Microsoft Sentinel Contributor

Scope

Members

Name

Austin Williams

Description

No description

Assignment type

Eligible

Assignment duration

Time bound

Start date and time

End date and time

 Users with eligible and/or time-bound assignments must have a valid license.

 PerparimLabs

Confirmation

- Assignment confirmed. User now has Sentinel Contributor role.
- IAM showing Owner + Contributor + new user.

Home > RG-Sentinel

RG-Sentinel | Access control (IAM) ☆ ...
Resource group

Search

Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Automation
Help

+ Add Download role assignments Edit columns Refresh Delete Feedback

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 4 4000 Privileged 2
View assignments

Search by name or email Type: All Role: All Scope: All scopes State: All End time: All Group by

All (5) Job function roles (3) Privileged administrator roles (2)

<input type="checkbox"/>	Name ↑↓	Type ↑↓	Role ↑↓	Scope ↑↓	State ↑↓
▼ Owner (2)					
<input type="checkbox"/>	Perparim Abdullahu padmin@cloudmatearchite...	User	Owner	Subscription (Inherited)	Active Permanent
<input type="checkbox"/>	Perparim Abdullahu padmin@cloudmatearchite...	User	Owner	Subscription (Inherited)	Active Permanent
▼ Microsoft Sentinel Contributor (3)					
<input type="checkbox"/>	Austin Williams austin.williams@cloudmate...	User	Microsoft Sentinel Contributor	This resource	Eligible time-bound

Key Takeaway

- ✓ Reader = view only
- ✓ Responder = manage incidents
- ✓ Contributor = build & manage
- ✓ Automation roles = playbooks & services”

