Role-based Access Control (RBAC)

Roles can be defined for local Wiz users as well as for federated SAML-based sessions in order to control the information they see and the actions they can perform.

Wiz recommends that you assign users the least permissive role possible.

Role descriptions

Every Wiz user must be assigned one of the following roles:

Wiz Role	Description	Recommended Users
Project Graph Reader	Read-only access to Inventory and Security Graph for Projects, and can manage queries and export query results. However, Project Graph Reader cannot change Project settings, or read/create/update Issues, Actions, compliance reports, etc.	Infrastructure engineers relevant to the Project who shouldn't have access to security info
Project Reader	Read-only access to all the user's projects data, and can export data and reports. However, Project Reader cannot make any changes to the Project settings or configurations.	Dev and/or DevOps personnel relevant to the Project
Project Member	The user sees information related only to their Projects and can perform limited actions on Project-specific settings, such as updating Issues.	Dev and/or DevOps personnel relevant to the Project

Wiz Role	Description	Recommended Users
Project Admin	The user sees information related only to their Projects and can manage most Project-specific settings.	Dev and/or DevOps personnel relevant to the Project
Global Graph Reader	Read-only access to the Inventory and Security Graph, and can manage queries and export query results. However, Global Graph Reader cannot change settings or read/create/update Issues, Actions, compliance reports, etc.	Senior infrastructure engineers who shouldn't have access to security info
Global Reader	The user has read-only access to all portal pages and their content, and can export data and reports. However, they cannot make any changes to Wiz settings or configurations.	Developers, compliance officers, executives, or anyone else who only needs to view data in Wiz
Global Responder	The user has all of Global Reader’s permissions, and can also manage (read and write) saved searches, Reports and Issues (e.g. ignore Issue), run scans, and upload scan results to Wiz.	SOC personnel, security analysts, DevOps, or anyone else with the authority to perform remediation actions in your cloud environment
Global Limited Responder	The user has all of Global Reader’s permissions, but can also run existing Actions and Automation Rules.	SOC personnel, security analysts, DevOps, or anyone else with the authority to perform remediation actions in your cloud environment
Global Incident Response Analyst	The user has all of Global Limited Responder's permissions, and can also run forensics and response flows (e.g. evidence collection).	SOC personnel, Incident Response team members or forensics examiners
Global Policy Manager	The user has all of Global Reader’s permissions, but can also run existing Actions and Automation Rules as well as manage custom compliance frameworks.	Compliance managers who should not be able to access Deployments or other settings
Global Contributor	The user has full read and write permissions to all portal pages and	Security architects, Wiz champions or cloud

Wiz Role	Description	Recommended Users
	their content, including Controls and Deployments. However, they cannot change Wiz settings for managing users, projects, and access. Finally, all Global Contributors may open support tickets by default.	admins
Global Admin	The user has full read and write permissions to all portal pages and their content. Furthermore, a Global Admin can change all Wiz settings, such as managing users, projects, and access. Finally, all Global Admins may open support tickets by default.	Senior security personnel
Settings Admin	The user has access to Wiz settings only.	Security or support personnel (who do not actually use Wiz)
Connector Reader	The user has read-only access to Deployment settings.	Technical support personnel (who do not actually use Wiz)
Connector Admin	The user has access to and control over Deployment settings only.	Senior technical support personnel (who do not actually use Wiz)
Documentation Reader	The user has access only to the documentation.	Security or support personnel (who do not actually use Wiz)

> By default, only users assigned the Global Admin or Global Contributor may open support tickets.

Role permissions

Click Project-scoped roles, Global roles, or Miscellaneous roles below to see each role's permissions per portal page or feature:

- A = Admin
- C = Create
- D = Delete

- R = Read
- U = Update
- W = Create, Delete, and Update
- - = No access

Project-scoped roles

Page/Feature	Project Graph Reader	Project Reader	Project Member	Project Admin
Action Templates	-	-	-	R/W
Admission Controllers	-	-	-	-
Application Services	-	-	-	-
Automation Actions	-	R	R	R/W
Automation Rules	-	R	R	R/W
Benchmarks	-	R	R	R
Cloud Accounts (Subscriptions)[6]	R	R	R	R
Cloud Configuration	-	R	R	R/W
Cloud Event Rules[3]	-	R	R	R/U
Cloud Events	R	R	R	R
Controls	-	R	R	R/W
Cost and Usage	-	-	-	-
Dashboards	R/W	R/W	R/W	R/W
Global Users Only Dashboardss	-	-	-	-
Org Dashboards	-	-	-	-
Project Dashboards	-	-	-	A
Dashboard Settings	-	-	-	-
Data Classifier Rules	-	-	-	R
Data Findings	R	R	R	R
Detections	-	-	-	-

Page/Feature	Project Graph Reader	Project Reader	Project Member	Project Admin
Endpoint Attack Surfaces	-	R	R	R
External Data Ingestion	-	-	-	C
Host Configuration	-	R	R	R
Ignore Rules	R	R	R	R/W
Image Integrity Validators Settings	-	-	-	R/W
Inventory	R	R	R	R/U
Issue Comments[7]	-	-	R/W	R/W
Issue due at	-	-	W	W
Issues[2]	-	R	R/U	R/U
Kubernetes Clusters	R	R	R	R
Monitored Metrics	R	R/C	R/C/D	R/W
Network Exposure (Report)	R	R	R	R
Outposts	-	-	-	-
Portal Settings	-	-	-	-
Portal Views	-	-	-	-
Private Portal Views	A	A	A	A
Projects	R	R	R	R
Registry Global Settings	-	-	-	-
Registries	R	R	R	R/U
Remediation And Response Deployments	-	-	-	-
Reports	-	R/C	R/C/D	R/W
CI/CD Reports[4]	-	R	R	R/W
Report Cancel Run	-	-	-	U
Repositories	-	R	R	R/U

Page/Feature	Project Graph Reader	Project Reader	Project Member	Project Admin
Resource Scan Result	-	-	-	-
Response Actions	-	-	-	-
Run Action	-	C	C	C
Run Control	-	-	C	C
Run Integration Action	-	C	C	C
Run Outpost Cluster Update	-	-	-	-
Run Response Action	-	C	C	A/C
Runtime Response Policies	-	C	C	-
Saved Cloud Event Filters	R	R	R/W	R/W
Saved Queries	R/W	R	R/W	R/W
Sbom Artifacts	-	R	R	R
Security Frameworks	-	R	R	R
Sensors	-	-	R	R
Service Tickets	-	-	W	W
Support Settings	-	-	-	-
Threat Center	R	R	R	R
User Accounts	-	R	R	R
Validators	-	-	-	R/W
Vulnerabilities	-	R	R	R
⚙ Ask AI	-	R	R	R
⚙ Audit Log	-	-	-	-
⚙ Cloud Event Settings	-	R	R	R
⚙ Custom File Detection	-	-	-	-
⚙ Deployments[5]	-	-	-	-

Page/Feature	Project Graph Reader	Project Reader	Project Member	Project Admin
⚙ Digital Trust	-	-	-	-
⚙ Identity Providers	-	-	-	-
⚙ Integrations	-	-	-	R/W
⚙ Issues and Reports	-	R	R	R
⚙ Legal Consent Settings	-	-	-	-
⚙ License	-	-	-	R
⚙ Preview Hub	R	R	R	R
⚙ Scan Policies (CI/CD)	-	R	R	R
⚙ Scanner Settings	-	R	R	R
⚙ Security Scans	-	R	R	R
⚙ Service Accounts	-	R	R	R/C/D
⚙ SSO & Login Security	-	-	-	-
⚙ System Activity Log	R	R	R	R
⚙ System Health	-	-	-	-
⚙ User Management	-	-	-	-

Projects Admins can't create Deployments

Project Admins cannot perform this action because Project-scoped roles are meant to be able to only control their own part of the estate, without the option to view other subscriptions or add workloads to Wiz tenants.

A couple of alternatives are:

- Assign the Project Admin and a Connector Admin role to the user, via SAML Group Mapping in SSO so that the user can switch between the roles.
- Create a Wiz Service Account with only the `create:connectors` permission, then provide the authentication credentials to Project Admins to create Deployments programmatically. The addition of the Deployments can be either an ad hoc operation or an orchestrated onboarding via a change management pipeline.

Global roles

Page/Feature	Global Graph Reader	Global Reader	Global Limited Responder	Global Incident Response Analyst	Glo Resp
Action Templates	-	R	R	R	
Admission Controllers	-	R	R	R	
Application Services	-	R	R	R	
Automation Actions	-	R	R	R	
Automation Rules	-	R	R	R	
Benchmarks	-	R	R	R	
Cloud Accounts (Subscriptions)[6]	-	R	R	R	
Cloud Configuration	-	R	R	R	
Cloud Event Rules[3]	-	R	R	R	
Cloud Events	-	R	R	R	
Controls	-	R	R	R	
Cost and Usage	-	R	R	R	
Dashboards	R/W	W	W	W	\
Global Users Only Dashboards	-	-	-	-	
Org Dashboards	-	-	-	-	
Project Dashboards	-	-	-	-	
Dashboard Settings	-	R	R	R	
Data Classifier Rules	-	R	R	R	
Data Findings	-	R	R	R	

Page/Feature	Global Graph Reader	Global Reader	Global Limited Responder	Global Incident Response Analyst	Glo Resp
Detections	-	R	R	R	
Endpoint Attack Surfaces	-	-	-	-	
External Data Ingestion	-	-	-	-	
Host Configuration	-	R	R	R	
Ignore Rules	R	R	-	-	
Image Integrity Validators Settings	-	-	-	-	
Integrity Validators	-	-	-	-	
Inventory	R	R	R	R	
Issue Comments[7]	-	-	-	-	R,
Issue due at	-	-	-	-	\
Issues[2]	-	R	R	R	R,
Kubernetes Clusters	-	R	R	R	
Monitored Metrics	R	C	C	C	\
Network Exposure (Report)	R	R	R	R	
Outposts	-	-	-	-	
Portal Settings	-	-	-	-	
Portal Views	-	-	-	-	
Private Portal Views	A	A	A	A	A
Projects	R	R	R	R	
Registry Global Settings	-	R	R	R	
Registries	R	R	R	R	
Remediation And Response	-	-	-	-	

Page/Feature	Global Graph Reader	Global Reader	Global Limited Responder	Global Incident Response Analyst	Glo Resp
Deployments					
Reports	R/C/D	R/C	C	C	R/(
CI/CD Reports[4]	-	R	R	R	
Report Cancel Run	-	-	-	-	
Repositories	-	R	R	R	
Resources[1]	R	R	R	R	R
Resource Scan Result	-	R	R	R	
Response Actions	-	-	-	-	
Run Action	-	-	C	C	(
Run Control	-	-	-	-	(
Run Integration Action	-	-	C	C	(
Run Outpost Cluster Update	-	-	-	C	
Run Response Action	-	-	C	C	(
Runtime Response Policies	R/W	R	R	R	
Saved Cloud Event Filters	R/W	R	R	R	R/
Saved Queries	R/W	R	R	R/W	R/
Sbom Artifacts	-	-	-	-	
Security Frameworks	-	R	R	R	
Sensors	-	-	-	-	
Service Tickets	-	-	-	-	\
Support Settings	-	-	-	-	
Threat Center	R	R	R	R	

Page/Feature	Global Graph Reader	Global Reader	Global Limited Responder	Global Incident Response Analyst	Glo Resp
User Accounts	-	R	R	R	
Vulnerabilities	-	R	R	R	
⚙ Ask AI	-	R	R	R	
⚙ Audit Log	-	-	-	-	
⚙ Cloud Event Settings	-	-	-	-	
⚙ Custom File Detection	-	R	R	R	
⚙ Deployments[S]	-	R	R	R	
⚙ Digital Trust Settings	-	R	R	R	
⚙ Forensics	-	-	-	R	
Copy Resource Forensics	-	-	-	A	
Forensics Package Download	-	-	-	A	
⚙ Identity Providers	-	-	-	-	
⚙ Integrations	-	R	R	R	
⚙ Issues and Reports	-	R	R	R	
⚙ Legal Consent Settings	-	-	-	-	
⚙ Licenses	-	R	R	R	
⚙ Preview Hub	R	R	R	R	
⚙ Scan Policies (CI/CD)	-	R	R	R	
⚙ Scanner Settings	-	R	R	R	
⚙ Security Scans	-	R	R	R	

Page/Feature	Global Graph Reader	Global Reader	Global Limited Responder	Global Incident Response Analyst	Glo Resp
⚙ Service Accounts	-	R	R	R	
⚙ SSO & Login Security	-	R	R	R	
⚙ System Activity Log	R	R	R	R	
⚙ System Health	-	R	R	R	
⚙ User Management	-	R	R	R	

Miscellaneous roles

Page/Feature	Settings Admin	Connector Reader	Connector Admin	Documentatio Reader
Action Templates	-	-	-	-
Admission Controllers	-	-	-	-
Application Services	-	-	-	-
Automation Actions	R/W	-	-	-
Automation Rules	R/W	-	-	-
Benchmarks	-	-	-	-
Cloud Accounts (Subscriptions)[6]	R	R	R	-
Cloud Configuration	-	-	-	-
Cloud Event Rules[3]	-	-	-	-
Cloud Events	-	-	-	-
Controls	-	-	-	-
Cost and Usage	-	-	-	-
Dashboards	-	-	-	-

Page/Feature	Settings Admin	Connector Reader	Connector Admin	Documentatio Reader
Global Users Only Dashboards	-	-	-	-
Org Dashboards	-	-	-	-
Project Dashboards	-	-	-	-
Dashboard Settings	-	-	-	-
Data Classifier Rules	-	-	-	-
Data Findings	-	-	-	-
Detections	-	-	-	-
Endpoint Attack Surfaces	-	-	-	-
External Data Ingestion	-	-	-	-
Host Configuration	-	-	-	-
Ignore Rules	-	-	-	-
Image Integrity Validators Settings	R/W	-	-	-
Integrity Validators	R/W	-	-	-
Inventory	-	-	-	-
Issue Comments[7]	-	-	-	-
Issues[2]	-	-	-	-
Kubernetes Clusters	R	R	R	-
Monitored Metrics	-	-	-	-
Network Exposure (Report)	-	-	-	-
Outposts	R/W	R	R/W	-
Portal Settings	-	-	-	-

Page/Feature	Settings Admin	Connector Reader	Connector Admin	Documentatio Reader
Portal Views	-	-	-	-
Private Portal Views	-	-	-	-
Projects	A/R	-	-	-
Registry Global Settings	-	-	-	-
Registries	-	-	-	-
Remediation And Response Deployments	R/W	R	R/W	-
Reports	-	-	-	-
CI/CD Reports[4]	-	-	-	-
Report Cancel Run	U	-	-	-
Repositories	R/U	R	R	R
Resource Scan Result	-	-	-	-
Response Actions	-	-	-	-
Run Action	-	-	-	-
Run Control	-	-	-	-
Run Integration Action	-	-	-	-
Run Outpost Cluster Update	-	-	-	-
Run Response Action	-	-	-	-
Runtime Response Policies	-	-	-	-
Saved Cloud Event Filters	-	-	-	-
Saved Queries	-	-	-	-
Sbom Artifacts	-	-	-	-

Page/Feature	Settings Admin	Connector Reader	Connector Admin	Documentatio Reader
Security Frameworks	R/C/D	-	-	-
Service Tickets	-	-	-	-
Sensors	-	-	-	-
Support Settings	A	-	-	-
Threat Center	R	R	R	-
User Accounts	-	-	-	-
Vulnerabilities	-	-	-	-
⚙ Ask AI	A/R	-	-	-
⚙ Audit Log	-	-	-	-
⚙ Cloud Event Settings	A/R	-	-	-
⚙ Custom File Detection	-	-	-	-
⚙ Deployments[S]	R/W	R	R/W	-
⚙ Digital Trust Settings	-	-	-	-
⚙ Identity Providers	A	-	-	-
⚙ Integrations	-	-	-	-
⚙ Issues and Reports	R/U	-	-	-
⚙ Legal Consent Settings		-	-	A
⚙ Licenses	-	-	-	-
⚙ Preview Hub	R	R	R	-
⚙ Scan Policies (CI/CD)	-	-	-	-
⚙ Scanner Settings	R/U	-	-	-
⚙ Security Scans	-	-	C	-

Page/Feature	Settings Admin	Connector Reader	Connector Admin	Documentatio Reader
⚙ Service Accounts	-	-	-	-
⚙ SSO & Login Security	A/R	-	-	-
⚙ System Activity Log	-	-	-	-
⚙ System Health	R/W	R	R/W	-
⚙ User Management	A/R	-	-	-

1️⃣ Refers to Wiz Boards and Security Graph.

2️⃣ In order to rescan an Issue, users must have the `create:run_control` permission.

3️⃣ Wiz recently renamed 'Cloud Event Rules' to 'Threat Detection Rules'. However, the corresponding RBAC permission has not been updated yet. If any roles require permissions for 'Threat Detection Rules', please continue using the existing permission name `Cloud Event Rules` for now.

4️⃣ In order to view CI/CD reports on the Reports > CI/CD Reports page, users must have the `read:security_scans` permission.

5️⃣ All roles can manually initiate rescans of an object (VM, Subscription, or Connector) if their role allows them to view it.

6️⃣ Information about Subscriptions (aka accounts in AWS, projects in GCP, and compartments in OCI) is pulled from your cloud environment via Cloud Connectors. You cannot add or edit Subscriptions in Wiz, only in your cloud provider portal.

7️⃣ Users with the `update:issues` permission are also able to write comments on Issues. In order to write a comment on an Issue, a user must have either the `write:issues_comments` permission or the `update:issues` permission.

Role assignment

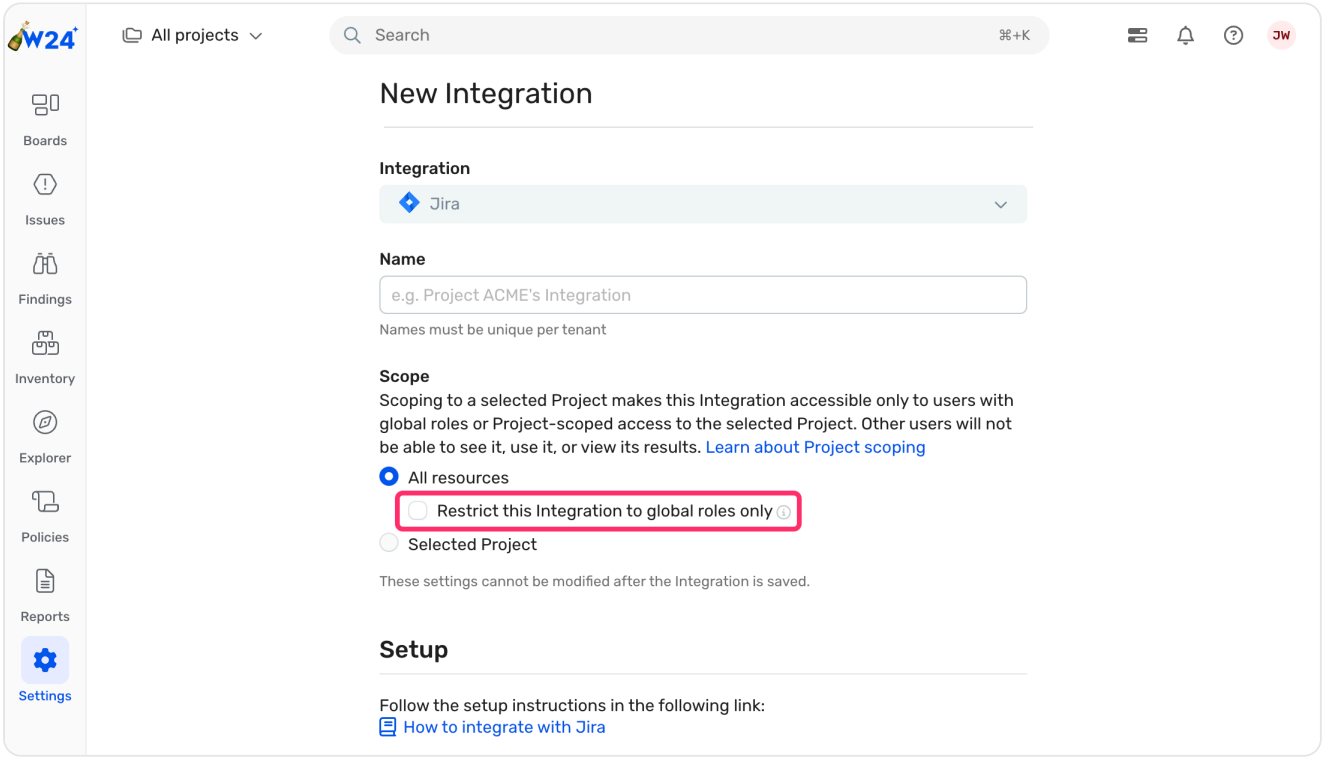
Roles can be assigned during user creation, assigned during bulk user invite, reassigned for an existing user, or passed via SAML.

Project-scoped components

The following are just some of the components in Wiz that can be scoped to a Project:

- Automation Rules
- Cloud Event filters
- Threat Detection Rules
- Ignore Rules
- Controls
- Integrations
- Reports
- Saved queries
- Service accounts
- Cloud Configuration Rules

When one of these components is scoped to a Project, only users with a global role or a matching Project-scoped role can see, use, run, and/or view results from the component. Moreover, the results of a Project-scoped component are limited to resources in that Project. For instance, a saved query for "VMs with critical severity vulnerabilities" that is scoped to a Project called "Acme AWS Prod" would return matching VMs only in that Project *even if it were run by user with a global role*.



Finally, Integrations and Automation Rules can be further restricted to only users with global roles, which prevents users with Project-scoped roles from viewing that Integration, manually running Actions that use it, and adding Automation Rules that use it.

FAQ

Questions? Take a look at the FAQ.

Updated 2 days ago

← Multi-tenant Login

Cloud Connectors →