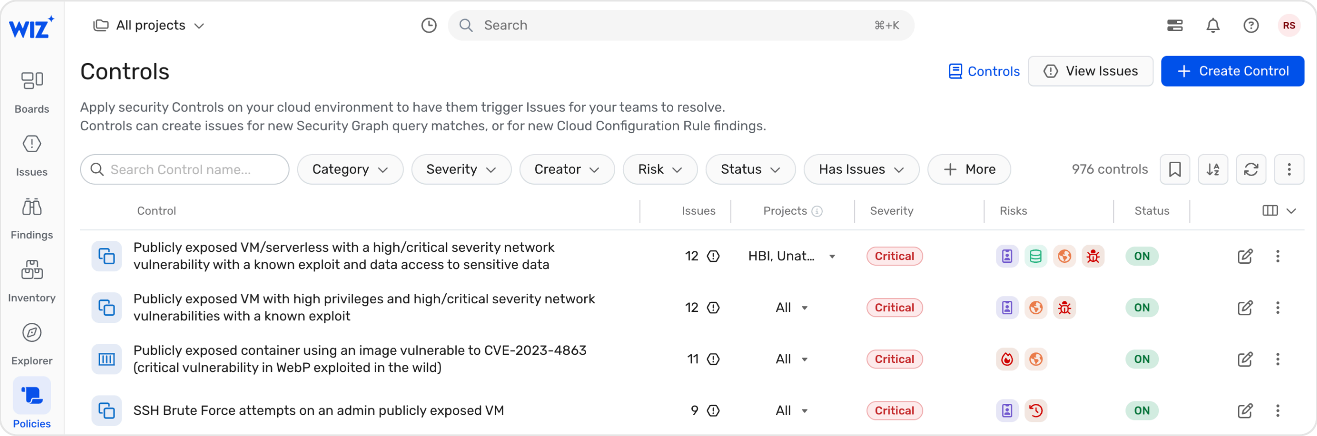
Controls

A Control consists of a pre-defined Security Graph query and a Severity level—if a Control's query returns any results, an Issue is generated for every result. See Controls & Issues for further details.

Each Control is assigned to a category in one or more compliance frameworks.



Controls

Apply security Controls on your cloud environment to have them trigger Issues for your teams to resolve.
Controls can create issues for new Security Graph query matches, or for new Cloud Configuration Rule findings.

Control	Issues	Projects	Severity	Risks	Status
Publicly exposed VM/serverless with a high/critical severity network vulnerability with a known exploit and data access to sensitive data	12	HBI, Unat...	Critical		ON
Publicly exposed VM with high privileges and high/critical severity network vulnerabilities with a known exploit	12	All	Critical		ON
Publicly exposed container using an image vulnerable to CVE-2023-4863 (critical vulnerability in WebP exploited in the wild)	11	All	Critical		ON
SSH Brute Force attempts on an admin publicly exposed VM	9	All	Critical		ON

From the Policies > Controls page, you can:

- Filter, sort, reorder, or hide Controls
- Create a custom Control
- Change the Project scope of a Control
- Disassociate a ticket from a Control
- Edit a custom Control
- Edit a built-in Control
- Reset an edited built-in Control
- Disable or enable a Control
- Delete a custom Control
- Create an Automation Rule from a Control
- View Run History
- Assign Controls to framework categories
- Add Control widgets to boards

Filter, sort, reorder, or hide Controls

By default, the Controls tab lists all Controls, including those that have not generated any Issues in your environment, ordered by severity.

To search for, filter, sort, or reorder Controls:

- At the top left, click Search to search for Controls by name
- Filter by Category, Severity, Created By, Risk, and more
- Click + More for more filters
- Click Order Options and select a different ordering

Create a custom Control

> ℹ It takes up to 48 hours for your environment to be assessed by a newly-created Control and for information to be shown on the Security Graph.

1. At the top right of the Controls tab, click Create Control. The Create new Control page loads.
2. Manually enter a Graph Query or choose one from the Query catalog. Learn about building custom queries.
3. Select a Project Scope for the new Control to scan. Learn about Project scoping.
4. Select an Issue Severity Impact that will be assigned to any Issues generated by the Control.
5. (Optional) If the Control will be assigned to a Compliance framework, consider clicking Advanced > Use a custom scope. Learn about using custom scopes.

Using custom scopes

Applying a custom scope to a Control limits which resources (VMs, containers, etc.) are assessed by the Control when the Control is assigned to a Compliance framework. A custom scope has no effect whatsoever on a Control that is not assigned to a Compliance framework.

Let's look for example at a Control named EC2 instances running Windows must have Microsoft Defender for Endpoints, that detects two such VMs in your environment. When this Control is assigned to a compliance framework, the framework performs a general check and:

- Fails VMs running Windows without Microsoft Defender (two VMs in our example)
- Passes all VMs that DO NOT match the Control's query (that could be a lot of VMs)

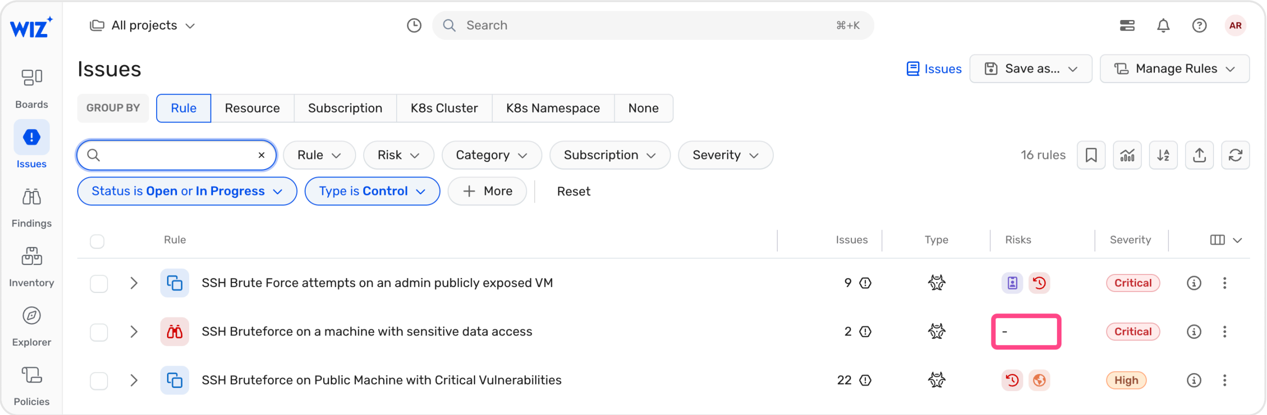
But in this case that's not a valid assumption because there could be dozens or hundreds of VMs running operating systems other than Windows. The correct assessment would compare the number of EC2 instances running Windows with Microsoft Defender for Endpoints to the number of EC2 instances running Windows without.

This is exactly what adding a custom scope to the Control achieves. Limiting the Control's scope to EC2 instances running Windows provides the true assessment of the percentage of Windows VMs that don't have Microsoft Defender for Endpoints.

6. Enter a short but meaningful Control Name. This name will be displayed throughout the portal.
7. (Optional) Enter a longer Description. This information will be displayed when the Control is hovered over.
8. (Optional) Assign the new Control to a framework:
   - Select one or more sub-categories from a compliance framework, e.g. GDPR, CIS, or ISO/IEC 27001.
   - Select one or more built-in Wiz sub-categories to map the new Control to the corresponding risk categories, e.g. Vulnerability Assessment > Vulnerability or Data Security > Unprotected Data (see below).

Mapping custom Controls to risks

If you do not associate a custom Control with any Wiz sub-categories, the Issues it generates will not be mapped to any risks.



Rule	Issues	Type	Risks	Severity
SSH Brute Force attempts on an admin publicly exposed VM	9			Critical
SSH Bruteforce on a machine with sensitive data access	2		-	Critical
SSH Bruteforce on Public Machine with Critical Vulnerabilities	22			High

Assigning a custom Control to one or more of the following Wiz for Risk Assessment categories associates Issues generated by the Control to the corresponding risk:

Category	Risk
Exposure Management	External Exposure
Identity Management	Unprotected Principal
Vulnerability Assessment	Vulnerability
Data Security	Unprotected Data

Category	Risk
High Profile Threats	High Profile Threat
Key & Secret Management	Insecure Use of Secrets
Container & Kubernetes Security	Insecure Kubernetes Cluster
Software & Application Management	Insecure Application
Operationalization	Reliability Impact
AI Security	Unprotected AI Model
SDLC Security	Insecure CI/CD
High Profile Threats	High Profile Threat

Learn about the Wiz for Risk Assessment framework.

9. (Optional) Enter a Recommendation that explains how to mitigate Issues generated from this Control. You may use markdown language to format this text.
10. (Optional) Add up to 10 Tags to the Control.
11. Click Create Control.

⚠ Controls are subject to limits. Learn more.

Change the Project scope of a Control

Apply a Control according to the Project's business impact. This Control will still be visible but will trigger Issues only in Projects that meet the specified business impact.

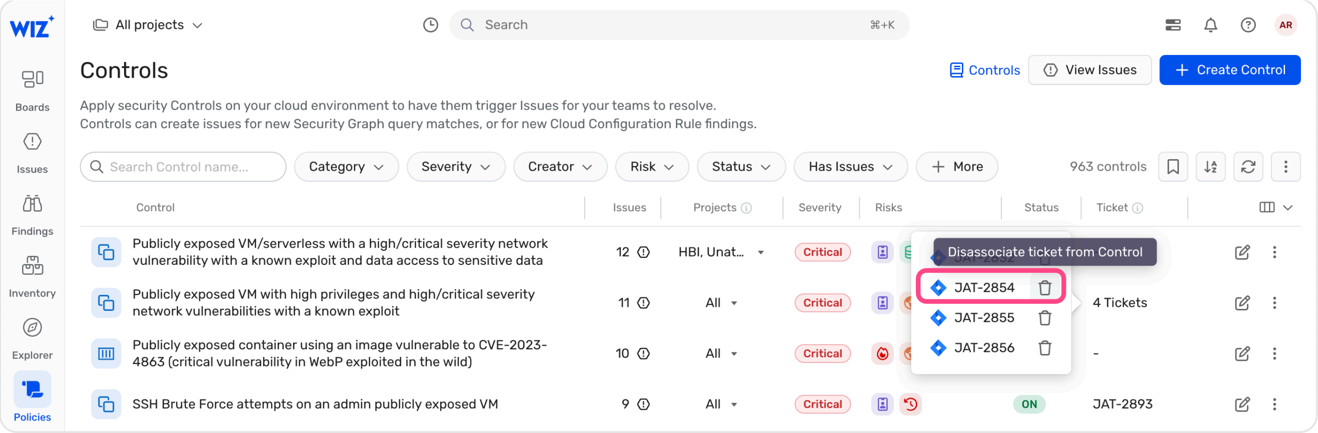
To change the Project scope of a built-in Control:

1. In the Projects column, click All.
2. Toggle which Projects (according to business impact) the Control should apply to.

Disassociate a ticket from a Control

If a ticket is associated with a Control, either manually or due to an Automation Rule, you can disassociate the ticket from the Control:

1. On the Policies > Controls page, the Ticket columns lists any ticket associated with this Control. If you do not see the Ticket column, add it by clicking Show/Hide table columns and add Ticket.
2. Hover over a ticket, then click Disassociate ticket from Control.



Controls

Apply security Controls on your cloud environment to have them trigger Issues for your teams to resolve.
Controls can create issues for new Security Graph query matches, or for new Cloud Configuration Rule findings.

Control	Issues	Projects	Severity	Risks	Status	Ticket
Publicly exposed VM/serverless with a high/critical severity network vulnerability with a known exploit and data access to sensitive data	12	HBI, Unat...	Critical			
Publicly exposed VM with high privileges and high/critical severity network vulnerabilities with a known exploit	11	All	Critical			4 Tickets
Publicly exposed container using an image vulnerable to CVE-2023-4863 (critical vulnerability in WebP exploited in the wild)	10	All	Critical			-
SSH Brute Force attempts on an admin publicly exposed VM	9	All	Critical		ON	JAT-2893

3. Click Confirm.

Edit a custom Control

You may edit only the custom Controls created in your environment.

1. Display only custom Controls by filtering on Creator > User (direct link).
2. Select the Control and click Edit.
3. On the Edit control page, modify the custom Control's graph query, scope, severity, and/or general info.
4. Click Save.

Edit a built-in Control

You can edit a built-in Control's metadata, including the Severity, Control Name, Description, and Recommendation. If you want to edit the Control further, you can create your own Control based on the built-in Control, edit whatever you want, and then disable the built-in Control.

Edit a built-in Control

1. For the Control you want to edit, click Edit.
2. Edit the relevant information.
3. Click Save.

> When Wiz updates a Control, e.g., a Control's Severity, your edits won't be overwritten.

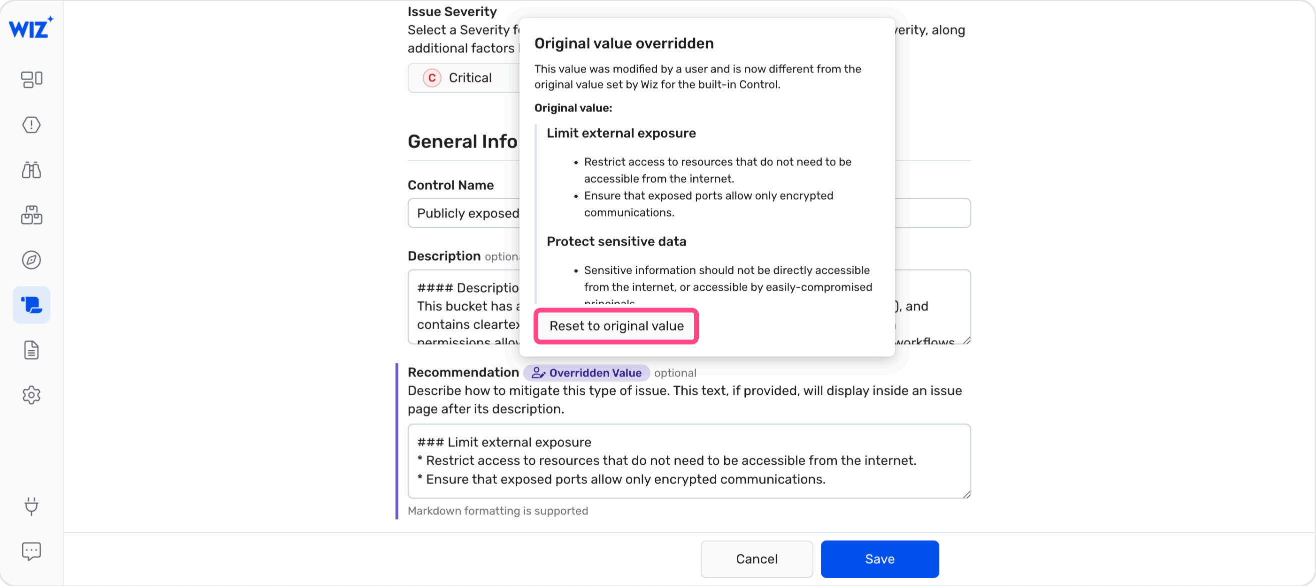
Create Control based on a built-in Control

1. For the Control you want to edit, click More options > View on graph.

2. Review the existing query and add/remove filters to adjust the query to the new Control.
3. At the top right, click Save as > Control. The Create a new control page opens with the query pre-populated.
4. On the Create a new control page, fill in or change the details. See [above](#).
5. Click Create Control.

Reset an edited built-in Control

1. Go to the Policies > Controls page.
2. Click More Filters > Overridden built-in Control > True ([direct link](#)).
3. On the Control to reset, click Edit.
4. On the edited section, hover over Overridden value, then click Reset to original value.



Issue Severity

Select a Severity f... verity, along additional factors ...

C Critical

General Info

Control Name

Publicly exposed ...

Description optional

Descriptio...
This bucket has a ...
contains cleartex...), and
permissions allow... workflows

Original value overridden

This value was modified by a user and is now different from the original value set by Wiz for the built-in Control.

Original value:

Limit external exposure

- Restrict access to resources that do not need to be accessible from the internet.
- Ensure that exposed ports allow only encrypted communications.

Protect sensitive data

- Sensitive information should not be directly accessible from the internet, or accessible by easily-compromised principals

Recommendation Overridden Value optional

Describe how to mitigate this type of issue. This text, if provided, will display inside an issue page after its description.

```
### Limit external exposure
* Restrict access to resources that do not need to be accessible from the internet.
* Ensure that exposed ports allow only encrypted communications.
```

Markdown formatting is supported

5. Click Save.

Disable or enable a Control

> It takes up to 48 hours for your environment to be assessed by a recently-enabled Control and for information to be shown on the Security Graph.

You can disable both built-in and custom Controls.

> ⚠ Disabling a Control causes its open Issues to be first resolved, which could trigger Automation Rules, and then deleted.

To disable a Control, click More options > Disable.

> ⚠ Enabling a Control causes its query to be re-evaluated against the current state of your Security Graph, which could generate new Issues that, in turn, could trigger Automation Rules.

To enable a Control, click More options > Enable.

Delete a custom Control

To delete a custom Control:

1. Display only custom Controls by filtering on Creator > User (direct link).
2. Click More options > Delete Control. Any un-resolved Issues generated by the Control are automatically transitioned to resolved.

> ℹ Built-in Controls cannot be deleted, only disabled.

Create an Automation Rule from a Control

If you've defined an Integration with a third-party tool like Jira or Slack (see the guide on response and automation), you can create an Automation Rule to trigger an Action when a Control generates an Issue.

To create an Automation Rule from a Control:

1. Click More Options > Create automation. The New Automation Rule page opens with the graph query pre-populated.
2. Fill in the details for the new Automation rule. See the Integration-specific guide for the selected third-party tool.

View run history

View the recent run history of a Control in the System Activity Log.

> ℹ View run history is only supported for Controls based on Security Graph queries.

1. For the relevant Control, click More options > View Run History.
2. (Optional) On the Settings > System Activity Log page that opens, apply extra filters to further refine the results.

Assign Controls to framework categories

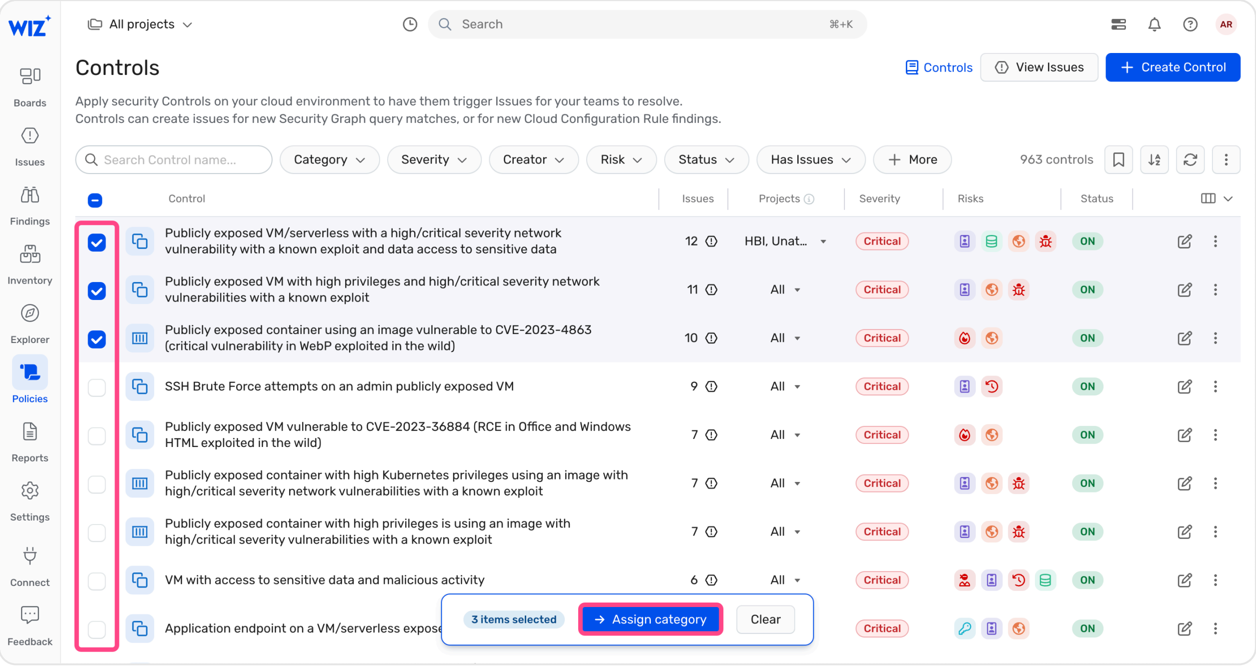
If the built-in mappings of Controls to framework categories do not perfectly align with your organizational needs, you can disable the relevant built-in Controls and/or assign custom Controls to more appropriate framework categories.

In addition, some Wiz categories map Issues to the risk domain boards on the Board page. Thus, you can ensure that Issues generated by a custom Control appear on the relevant risk-specific board. For example, assigning a custom Control to the Exposure Management category would result in its Issues appearing on the External Exposure board.

> Built-in Controls cannot be assigned to built-in compliance frameworks, only custom compliance frameworks. Learn more.

To assign Controls to framework categories:

1. Click More Options > Assign to Category.



Controls

Apply security Controls on your cloud environment to have them trigger Issues for your teams to resolve.
Controls can create issues for new Security Graph query matches, or for new Cloud Configuration Rule findings.

963 controls

	Control	Issues	Projects	Severity	Risks	Status
☑	Publicly exposed VM/serverless with a high/critical severity network vulnerability with a known exploit and data access to sensitive data	12	HBI, Unat...	Critical		ON
☑	Publicly exposed VM with high privileges and high/critical severity network vulnerabilities with a known exploit	11	All	Critical		ON
☑	Publicly exposed container using an image vulnerable to CVE-2023-4863 (critical vulnerability in WebP exploited in the wild)	10	All	Critical		ON
☐	SSH Brute Force attempts on an admin publicly exposed VM	9	All	Critical		ON
☐	Publicly exposed VM vulnerable to CVE-2023-36884 (RCE in Office and Windows HTML exploited in the wild)	7	All	Critical		ON
☐	Publicly exposed container with high Kubernetes privileges using an image with high/critical severity network vulnerabilities with a known exploit	7	All	Critical		ON
☐	Publicly exposed container with high privileges is using an image with high/critical severity vulnerabilities with a known exploit	7	All	Critical		ON
☐	VM with access to sensitive data and malicious activity	6	All	Critical		ON
☐	Application endpoint on a VM/serverless expose			Critical		ON

2. (Optional) On the left, select additional Controls to assign.
3. At the bottom, click Assign Category.
4. In the Assign categories dialog:
   1. Click Add to or Remove from.
   2. Select one or more framework categories from the drop-down.
   3. Click Assign categories.

Add Control widgets to boards

You can further monitor Controls and their associated Issues by adding widgets to your custom boards.

1. Click a Control name to open its details drawer.
2. Select a widget and click Add to board.
3. In the Add widget to board window, select a board and click Add to board.

You can also access a Control's details drawer from the Compliance and Issues pages by clicking its name.

Updated 6 days ago

← Policies

Vulnerability Catalog →