

How to setup security groups

Objectives

- What is a security group?
- Create a security group
- Add rules to security groups

What is a security group?



A security group is a collection of security rules acting as a firewall for your virtual instances. Security rules are setup to allow traffic to and from specific ports.

You can assign security groups to each of your virtual instances independently.

Create a security group



To create a security group, you need to log into the Cloud dashboard. Then click on the **Compute** dropdown menu on the left hand side of the screen, then select the **Access & Security** item.


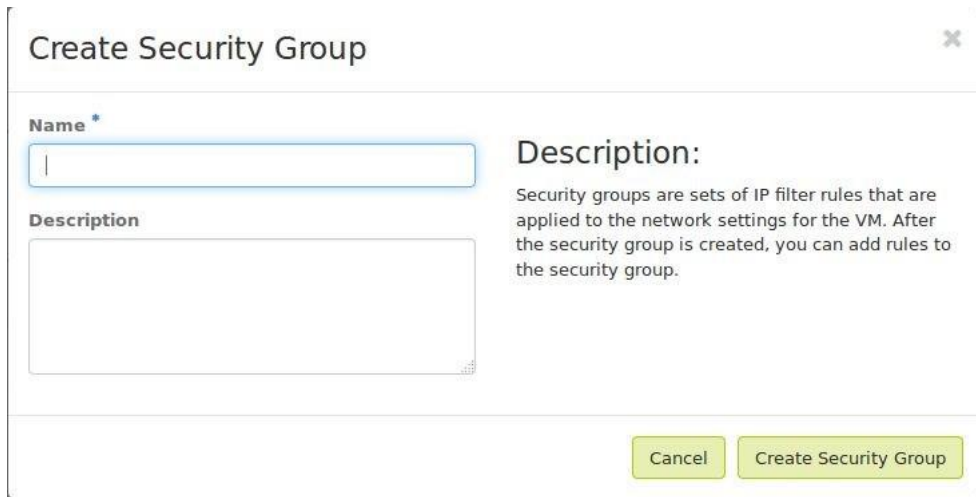
Select the **Security Groups** tab to view your security groups.

The screenshot displays the 'Access & Security' dashboard. On the left, a navigation sidebar shows 'Project' and 'Compute' expanded, with 'Access & Security' highlighted. The main content area is titled 'Access & Security' and contains tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active, showing a table with two items: 'ICMP Ingress all ports' and 'default'. The table has columns for 'Name', 'Description', and 'Actions'. The 'Actions' column contains 'Manage Rules' buttons for each group. At the top right of the table area, there is a search filter, a '+ Create Security Group' button, and a 'Delete Security Groups' button. Below the table, it says 'Displaying 2 items'.

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	ICMP Ingress all ports	Allow Ping to all ports	Manage Rules
<input type="checkbox"/>	default	Default security group	Manage Rules

Create a security group

Click the **Create Security Group** button in the top right-hand side of the screen. This will display a popup screen where you create your new security group.



Enter a descriptive **Name** for the Security Group and complete the **Description** in the fields provided, then click the **Create Security Group** button.

Then **Cancel** button will close the popup screen.

Create a security group



After your new security group was created, you will see the new group displayed in the list on the dashboard.

The screenshot displays the 'Access & Security' dashboard. On the left is a navigation sidebar with categories: Project, Compute, Access & Security (highlighted), Network, Orchestration, and Identity. The main content area is titled 'Access & Security' and contains sub-tabs for Security Groups, Key Pairs, Floating IPs, and API Access. The 'Security Groups' tab is active, showing a table with columns for Name, Description, and Actions. The table lists two security groups: 'ICMP Ingress all ports' and 'default'. Above the table are controls for filtering, creating, and deleting security groups. Below the table, it indicates 'Displaying 2 items'.

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	ICMP Ingress all ports	Allow Ping to all ports	Manage Rules
<input type="checkbox"/>	default	Default security group	Manage Rules

Add rules to a security group



To add new security rules to the security group, click the **Manage Rules** option from the dropdown menu under the **Actions** column.

A screenshot of the AWS IAM console interface. On the left is a navigation sidebar with categories: Project, Compute, Access & Security (highlighted), Network, Orchestration, and Identity. The main content area shows the path "Access & Security / Manage Security Group Rules: ICMP Ingress all ports (be477dab-942c-4beb-b663-a73845cdbde8)". Below the path are two buttons: "+ Add Rule" and "Delete Rules". A table lists three security rules with columns for checkboxes, Direction, Ether Type, IP Protocol, Port Range, Remote IP Prefix, Remote Security Group, and Actions. Each rule has a "Delete Rule" button in the Actions column. Below the table, it says "Displaying 3 items".

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	Delete Rule
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule

Add rules to a security group



Click the **Add Rule** button in the top right-hand side of the screen. This will display a popup screen where you create your new security rules.

A screenshot of a web-based 'Add Rule' popup window. The window has a title bar with 'Add Rule' and a close button. It contains three input fields: a dropdown menu for 'Rule' with 'HTTP' selected, a dropdown menu for 'Remote' with 'CIDR' selected, and a text input field for 'CIDR' containing '0.0.0.0/0'. To the right of these fields is a 'Description' section with three paragraphs of text explaining rule templates, port ranges, and remote sources. At the bottom right of the popup are two buttons: 'Cancel' and 'Add'.

Select a **Rule** from the dropdown list. We will use **HTTP** for this demonstration, but all rules are available. Leave the fields provided as is then click the **Add** button.

Then **Cancel** button will close the popup screen.



Add rules to a security group



That is it. You have added your first rule to a security group.
Notice your new rule is displayed in the list.

Project ^

Compute ^

Overview

Instances

Volumes

Images

Access & Security

Network v

Orchestration v

Identity v

Access & Security / Manage Security Group Rules: ICMP Ingress all ports (be477dab-942c-4beb-b663-a73845cddbde8)

+ Add Rule Delete Rules

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	Delete Rule
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	Delete Rule

Displaying 4 items



To Delete a rule,
click the **Delete Rule** button under
the **Actions**
column.

We suggest
creating a group for
each rule you wish
to apply to make it
easier to assign
these rules.

Thank you

For Support log a call at:
support@wingu.co.za