


## Security Groups

### Introduction

Security Groups are setup to delegate administrative rights to administrators in AC Nio. Administrators assigned to a Security Group inherit all the permissions set for the group. Security Groups can be configured to grant or restrict administrative access to hardware or programming of AC Nio. When a new Administrator takes over, their account will be added to the proper Security Group.

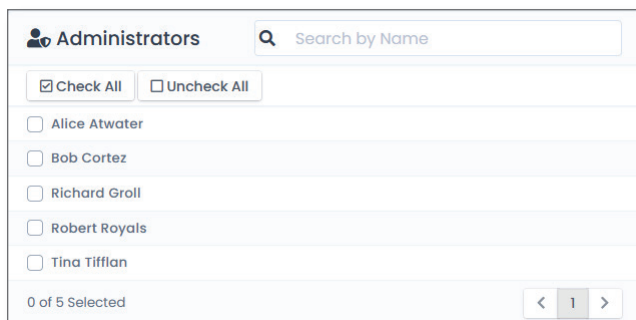
### Creating a Security Group

Click **+Add** to create a new Security Group. Give the Security Group a **Name** and optional **Description**.



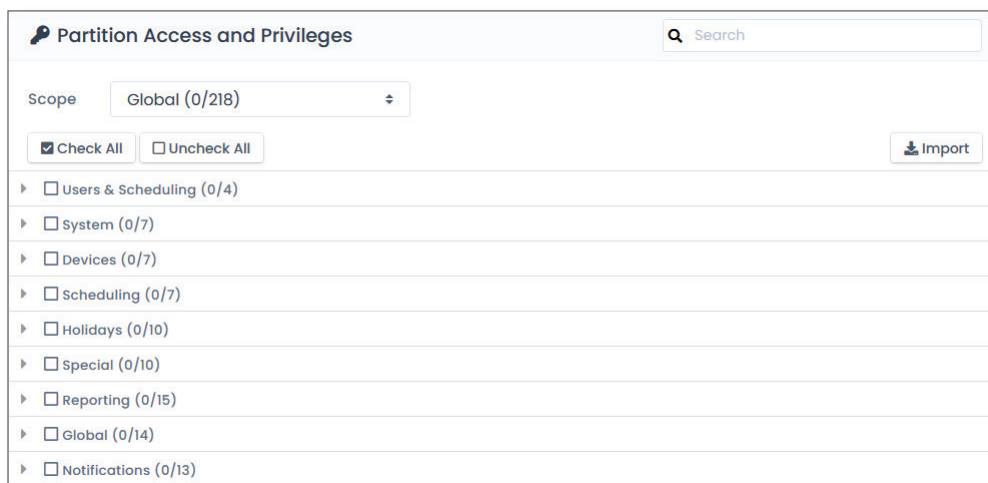
The form is titled "Security Group" with a gear icon. It contains two input fields: "Name" with a "Required" label and "Description" with an "Optional Description" label. The "Description" field has a small icon in the bottom right corner.

Check any **Administrators** to be added to the Security Group.



The form is titled "Administrators" with a search bar "Search by Name". It has two buttons: "Check All" and "Uncheck All". Below is a list of administrators with checkboxes: Alice Atwater, Bob Cortez, Richard Groll, Robert Royals, and Tina Tiffan. At the bottom, it says "0 of 5 Selected" and has navigation buttons "< 1 >".

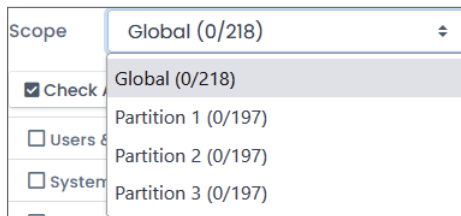
Assign permissions to the Security Group in **Partition Access and Privileges**. More detail on permissions are listed on the second page of this document.



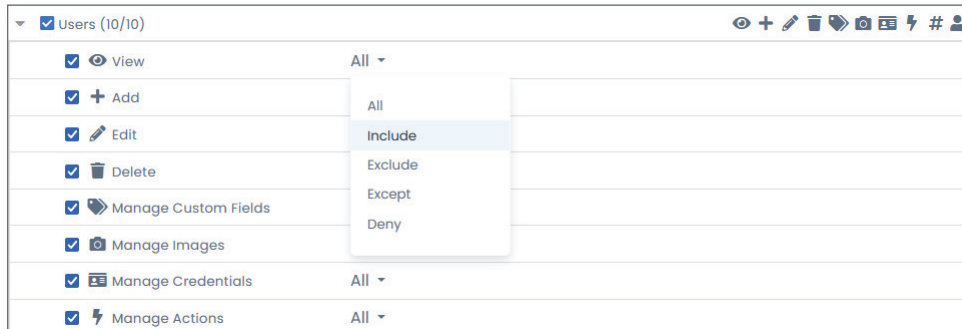
The form is titled "Partition Access and Privileges" with a search bar "Search". It has a "Scope" dropdown menu set to "Global (0/218)". There are two buttons: "Check All" and "Uncheck All", and an "Import" button. Below is a list of permissions with checkboxes and expand/collapse arrows: Users & Scheduling (0/4), System (0/7), Devices (0/7), Scheduling (0/7), Holidays (0/10), Special (0/10), Reporting (0/15), Global (0/14), and Notifications (0/13).

## Partition Access and Privileges

For the **Scope**, select the partition the Security Group will attribute permissions to. If setting up a Security Group for integrators, Global settings can be used.



Permissions can be as granular as needed. Inclusions or exclusions can be added to the View, Edit or Delete permissions so the Security Group does not grant access to specified Users, Devices, Partitions, Sites, Action Plans or Action Triggers.



## Users and Scheduling

Users and Scheduling permissions grant or revoke access to Access Privilege Groups, Users, Card Templates and Card Template Images

### System

System permissions grant or revoke access to Partitions, Sites, Maps, Action Triggers and Plans, and Dashboards.

### Devices

Permissions for Doors, Elevators, Panels, Cameras and Camera Integrations, Alarm Panels and Alarm Partitions.

### Scheduling

Permissions for Door Schedules, Floor Schedules, One Time Runs, User Schedules and I/O Schedules.

### Holidays

Permissions to View, +Add, Edit or Delete Holiday, Holiday Schedules and Holiday Groups.

### Special

Permissions for Hardware Overrides, Disengage Alarm, and Updating Panels.

### Reporting

Permissions for reporting User Activity, User Time Tracking, Floor Activity, Elevator Activity, Monitoring, Configuration, I/O, Anti-Passback, Alert History, Notifications, Administrative Logs, and Alarm Activity.

### Global

Permissions to View, Add, Edit or Delete Administrators and Custom Fields. Manage Crisis Levels, Licensing, Migrate Data, LDAP, View, and Edit Health Settings.

### Notifications

Permissions for creating notification Rules, Managing Cameras, Acknowledging Alerts, and Push Notifications.