

siterra | Knowledge Base Article

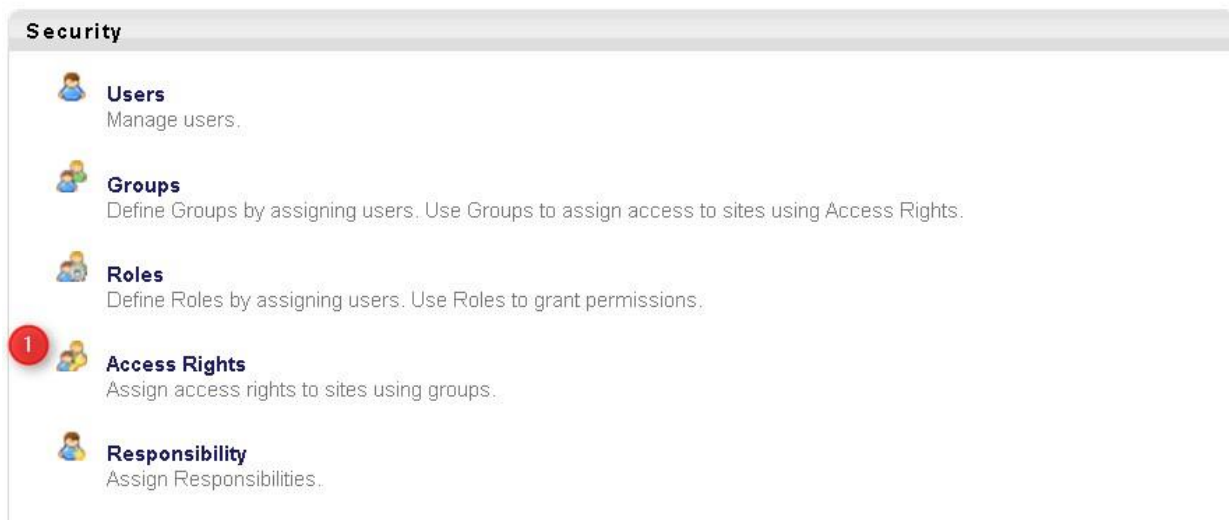
Users & Security – Permissions Overview

User access in Siterra is determined by the combination of three factors: Groups, Roles and Admin. By using these three separate factors to determine access, clients can create a very specific level of access for each particular user, determining what objects they can see and what they can do with those objects. At a high level, the three factors can be summarized like this:

Groups

Groups determine what parts of the portfolio your user has access to. For example, one group might grant access to the Org Unit for New York State, while another might grant access to Australia and Malaysia.

To change what objects a group has access to, use the “Access Rights” (1) link on the Admin page.



Below, we can see a screen shot from the Access Rights tool, which sets which group has access to which objects. The object type in this case is “Property” (1), from the “Denver” (2) Org unit. Note that “Include child objects” (4) has been checked and that “000RegTest” (5) is set as the group. After clicking “Search” (3), we can see the results populate below, showing us that 000RegTest has “Group Access” (6) to the sites returned by the search.

Access Rights

Add Access Rights
 Remove Access Rights
 Remove All Access Rights
 Add Inheritance
 Remove

Note: Every user in each group will assume the permissions for each of the roles to which they are associated.

1 Display Property from Denver
 3 Search
 4 ☒ Include child objects in

5 Indicate where this group has access 000RegTest

☐ Attribute Search

Search for test in Name
 Search
 ☐ Match whole column only
 ☐ Match case

☐	Type	Name ▲	6 Group Access	Number
☐	Site	10 Year Test Site	✓	943543544443556
☐	Site	JBA Site Test	✓	943543544443580
☐	Site	JMW Test	✓	943543544443588
☐	Site	Ownership Test	✓	92513
☐	Site	Test@ Siterra Site	✓	55555

Roles

Roles determine how your user can affect objects. One role might give users permission to view sites that their group has access to, while another might allow them to edit leases.

First, browse to Admin, then select “Roles” (1), as pictured below.

Security

Users
Manage users.

Groups
Define Groups by assigning users. Use Groups to assign access to sites using Access Rights.

Roles
Define Roles by assigning users. Use Roles to grant permissions.

Access Rights
Assign access rights to sites using groups.

Responsibility
Assign Responsibilities.

In this screen, you can click on the “Blue and white menu button” (1) to the left of the role you would like to modify. Next, click “Set Global Permissions” (2).

Roles

Add

Search for in ☐ M:

	Name ▲	Description
1	Archive Test Role	
	Edit Set Global Permissions 2 Delete Log	Used for testing various access levels
	PRM_TEST	
	PT Test	
	ST Test Role	
	TPH Test role	

On this screen, there is a tab for each different object type within Siterra. Pictured below, “Search Ring” (1) permissions have been listed. Note that each action that a user can take with an object has its own tick box, and “Create” (2) specifically has been noted. Using these tick boxes, you can control what users with particular roles are able to do when they interact with a particular object.



Search Ring 1		☐ Select All		
☒	Create 2			
☐	Update			
☒	View			
☐	Mark Deleted			
☐	Archive/ Activate			

Administrator Access

Primarily, Admin access allows a user to use the Admin page, which contains tools to edit and create users, Extended Attributes, Schedule Templates and Org Units. The vast majority of users will not be Administrators, so we'll focus on Groups and Roles instead.

It's best to think of Groups as *where you can go* and Roles as *what you can do* when you get there. A user can have as many Groups and Roles as they need, and it is the combination of all assigned Groups and Roles that determines their permissions. For example, if a user is assigned to the New York group described above as well as the Australia and Malaysia group, that user will be able to access both New York and Australia/Malaysia. A user's access is the sum of all of their groups. Similarly, by assigning a user the View Sites and Edit Leases roles, that user will be able to both view sites and edit leases.

Working with groups and roles can be quite confusing at times if you are unfamiliar with the groups and roles you're working with. This is why it is important to diligently map out what you want each group and role to do individually. If you are unsure how a particular set of Groups and Roles will affect a user's access, create a sample user to test with. This will allow you to verify that the combination of Groups and Roles that you are considering work the way that you expect it to.