Permissions Management

Permissions let you specify who has access to Smartenit resources, and what actions they can perform on those resources. All permissions are identity-based, you can grant permissions to a single user or to a role. In addition to application scopes, which define access to resources for a role, permissions let you configure access to specific users over specific resources. In conjunction, both security checks guarantee that the current user or app trying to access a resource are allowed.

Permissions can be granted to specific users or roles on a resource level. For example:

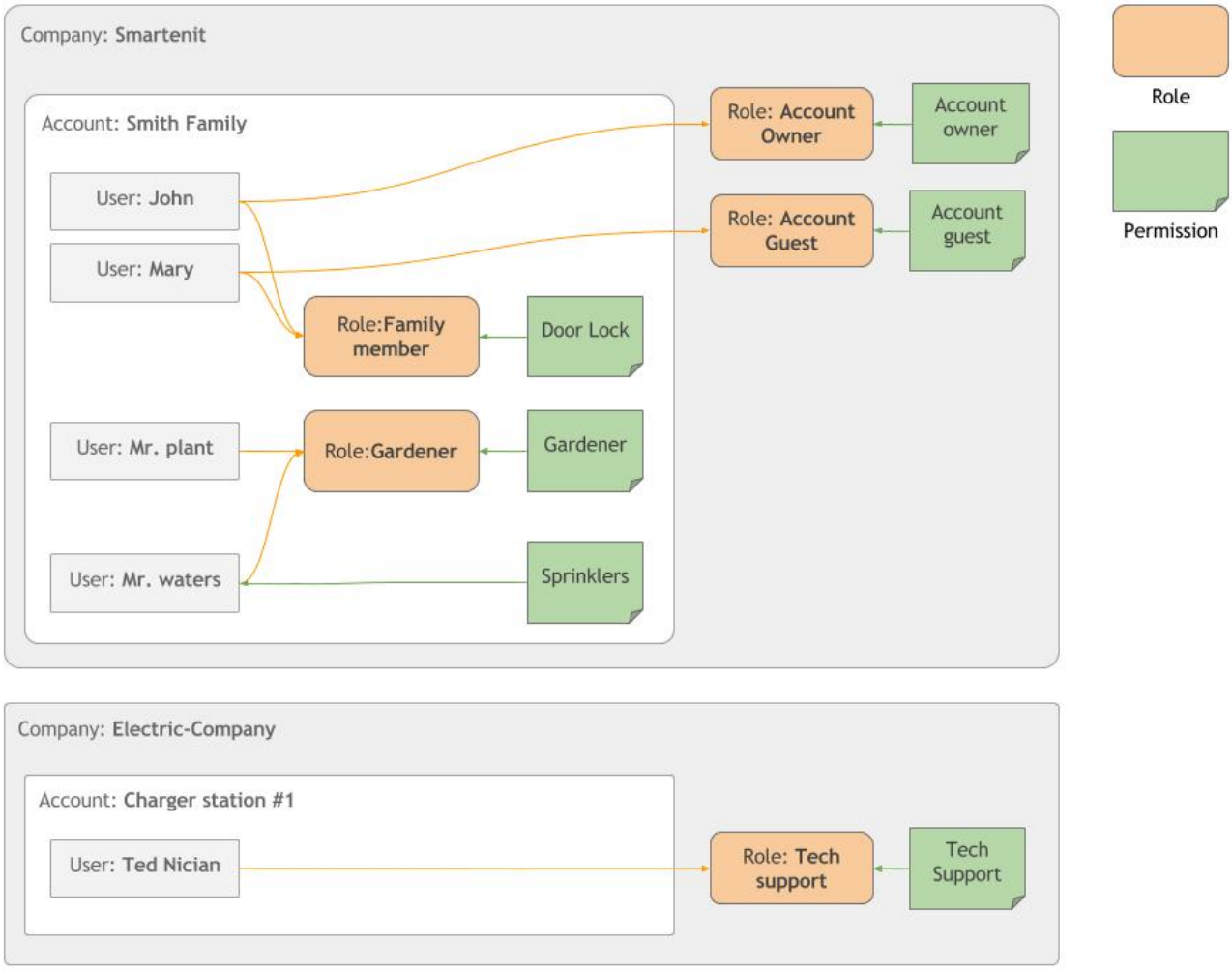
- John can turn on or off the garage light.
- Family members can open the door.
- Tech support guy can reset my gateway for 2 hours.

Permissions are evaluated using the request context of the current user and application, in conjunction with OAuth2 server, permissions can use authentication information stored in the access token to decide whether to allow or deny access to a resource action.

Smartenit has a collection of default roles to allow users to securely share control over their devices or to allow company administrator to manage their accounts:

- Company Administrator: Can manage their own company accounts.
- Account Owner: Can manage their devices and guest users that belong to its account including other resources.
- Account Guest: Can control and manage devices allowed by the account owner.

In the following example, there are 2 companies, Smartenit, and Electric-Company. Smartenit has one account, The Smith family, this account has 4 users 2 of them are family members that have access to the door lock and the other 2 are gardeners. Additionally to gardener permissions, Mr. waters can control the sprinklers. For Electric-Company, there is one account for an electric charger and there is one Tech support user that is currently assigned to that charger station.



Next Steps

- Explore OAuth 2 examples

- API Overview