Roles and Permissions

Roles are a way to organize access to Applications for your users. A Role can represent a person's role in the organization, for example, "Accounting" or "Customer", or it can be more technical, such as "Zendesk Administrator". A user can have any number of Roles.

A Role consists of Members and Permissions. The members are the users that have been assigned the role, and the Permissions are the access to Applications that the users are granted when assigned the role.

There are two types of Permissions that can be assigned to roles: Single Sign-on and Assertiv API. In the near future, there will also be "Account" permissions that create an account for a user in an Application.

Single Sign-on Permissions

When an administrator creates an Application, if that application supports Single Sign-on, a Permission becomes available to allow users to access the application from the Assertiv web application or mobile application. When a user has a Role that has this Permission, the user will see the application's icon on the "Apps" page. When the user clicks on this icon, they will be taken to the application without having to enter a password. Not only is this a convenience for the user, but it is also a security benefit for your organization, as the user does not have to know or remember their password in the target application. Therefore, you avoid the common security problem of users either writing down their passwords or using the same password for every application that they use. By enabling the Multi-Factor Authentication features of Assertiv the users are required to also have in their possession their mobile device when logging in to Assertiv. This drastically reduces the chances that hackers can get unauthorized access to the Applications that your users use.

Assertiv API Permission

These Permissions allow the administrator to delegate administration of Assertiv to others and can provide users access to the public API of Assertiv for your organization. This latter type of access would normally only be required by software developers to extend the capabilities of the Assertiv platform to meet the specific requirements of your organization.

When certain Assertiv API Permissions are granted to a user, they will see new functionality appear in Assertiv the next time they log on. The Assertiv API Permissions are a fine-grained security control to the individual functions of the Assertiv Identity Platform. Some of the management tasks require more than one Permission to perform. For example, the "List Roles" permission is required to enable the "Roles" icon on the Dashboard, but to view the details of a Role, the user would also require "Get Role Details", "Get Role Memberships" and "Get Role Permissions".

To make it easier for an administrator to delegate the administration tasks of Assertiv, we have created a list of administrator roles that are available out of the box.