



# Single Sign-On (SSO)

*OpCon's single sign-on (SSO) functionality gives your staff the ability to use one login ID for multiple applications, saving time and effort by removing the need to re-enter authentication credentials.*

## What You Can Do With SSO

### Use IDM with OpCon

With SSO, you can utilize a built-in Identity Management Application (IDM) in conjunction with OpCon. With the help of role assignments, OpCon users will be authenticated using a single sign-on. You can also map user groups to specific roles in OpCon.

### Support your choice of IDM

OpCon SSO includes but isn't limited to:

- Okta
- Azure AD
- Custom SSO servers

### Use the OpenID protocol

Leverage the OpenID protocol to communicate with IDM applications (OID vs. SAML).

## What SSO Functionality Offers

### Determine registration and authentication

Construct how the IDM will register and authenticate OpCon as a supported application.

### Define IDM and OpCon roles

Define the relationship between user groups in the IDM and OpCon roles.

### Use Solution Manager to grant permission

Grant user or group SSO permissions within a user-friendly web interface.

## SSO Benefits

- Included with OpCon Cloud subscription
- Customizable based on security and compliance requirements
- Simplifies user logon experience
- Group role changes are synchronized and updated dynamically
- Easy setup in user-friendly web client
- No additional installation required