SSO/MFA: Onboarding an Existing RAO/DRAO

Enable Existing Admins for SSO Login

Existing MRAO, RAO and DRAO administrators that login to CM through the InCommon CM Login page by entering their CM account login credentials can also be enabled for SSO login in two ways:

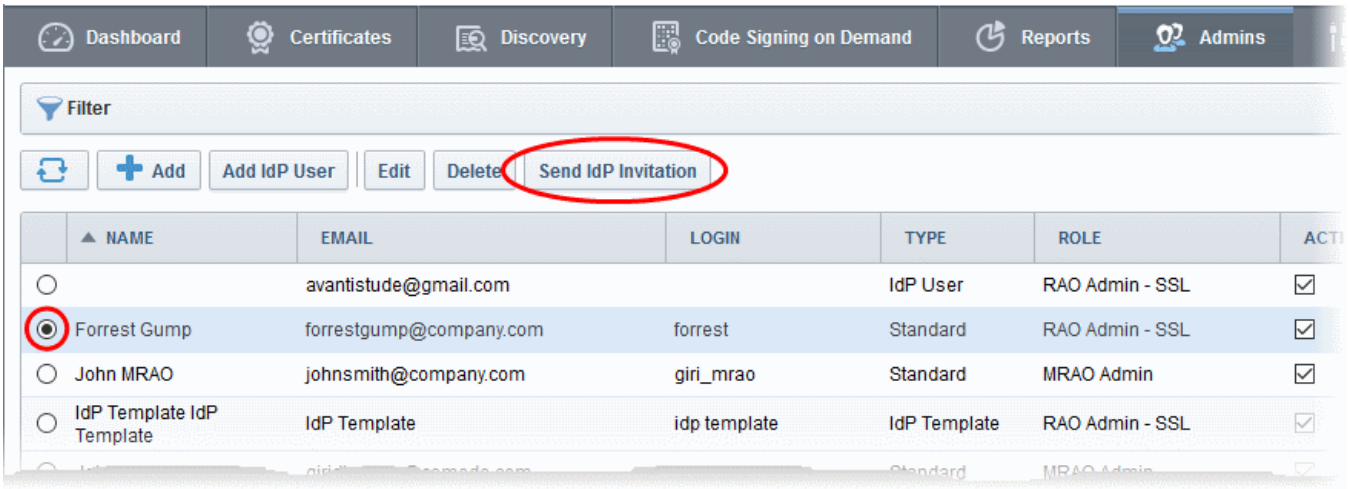
- Sending an SSO Invitation within CM
- Editing the administrator's existing account

1. Sending an SSO Invitation

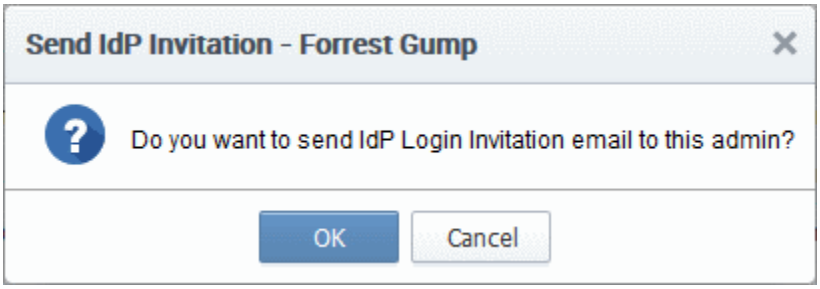
MRAO administrators and RAO/DRAO administrators with admin creation/editing privileges can enable SSO logins by sending an invitation from the CM interface. The invitation email will contain a link for the administrator to login to CM through the SSO login page.

To send an invitation to an administrator

- Click the 'Admins' tab from the top of the CM interface
- Select the administrator to be enabled for SSO login
- Click the 'Send IdP Invitation' button

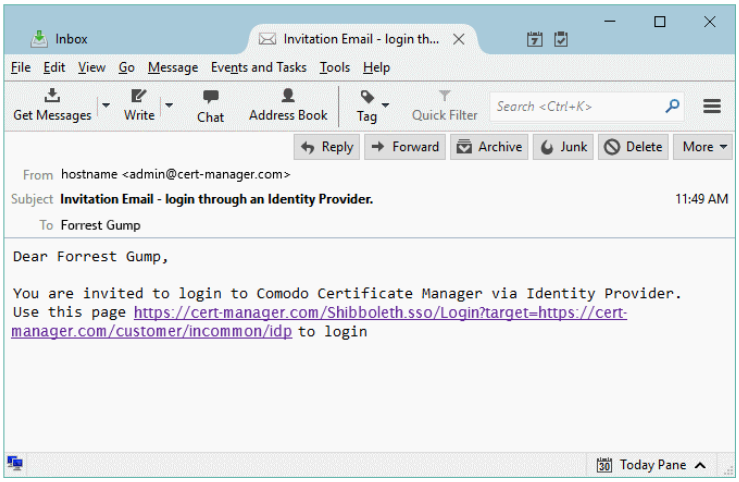


A confirmation dialog will appear:



- Click 'OK' to send the invitation.

An invitation email will be sent to the administrator with a link to access the login page.



The email will come from admin@cert-manager.com with the subject "Invitation Email - login through an Identity Provider."

Upon clicking the link, the admin account will be activated and the administrator will be taken to the SSO login page for logging-in to the CM using his/her SSO credentials.

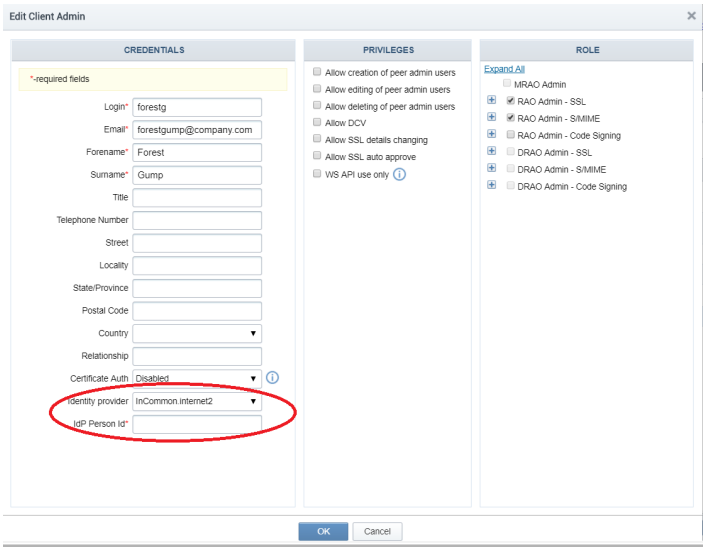
2. Editing the Administrator

An existing administrator can also be enabled for SSO login by specifying the user's identifier (ePPN) in their CCM admin settings.

To edit an administrator for enabling SSO

- Click the 'Admins' tab from the top of the Certificate Manager interface
- Select the administrator to be enabled for SSO login and click the 'Edit 'button.

The 'Edit Client Admin' form will appear:



- Edit the following field:
  - IdP Person Id - Enter the unique identifier (ePPN) for the administrator (as asserted by the IdP).
- Click 'OK' for your settings to take effect