

InCommon®



# InCommon Certificate Manager

Integration of Identity Provider for Single Sign-On

InCommon  
c/o Internet2  
1000 Oakbrook Drive, Suite 300  
Ann Arbor MI, 48104

## Integration of Identity Provider for Single Sign-On

InCommon Certificate Manager (InCommon CM) allows administrators of different privilege levels to login to the console using their Identity Provider (IdP) account login credentials, relieving the MRAO administrators from the burden of creating distinct usernames and passwords for each newly enrolled administrator.

To set it up, your IdP needs to participate in the InCommon Federation and release the appropriate information (detailed [here](#)). Once associated, you will be able to enroll new users who can login to InCommon CM using credentials at your IdP. You can send invitation mails to enrolled staff to login to InCommon CM with their IdP credentials.

### Login to InCommon CM using IdP

InCommon will generate an IdP login URL which needs to be communicated to your IdP users. Users can visit the URL to open the IdP login page, select their IdP, and enter their credentials to login to InCommon CM.

**Multi-factor Authentication** – If required, multi-factor authentication (MFA) can be implemented for your account. MFA means, in addition to their IdP username and password, users will need to provide a second form of authentication to login into InCommon CM. For example, a one-time passcode sent to the user's phone.

**Note:** At this time, MFA will be applied only for MRAO and RAO administrators and not for DRAO administrators.

### Create IdP User accounts

You can create accounts for users to login using IdP credentials and/or enable existing administrators to login using IdP credentials. There are three alternative methods you can use to accomplish this:

- Create new admin account with IdP login – You can enroll a new user, assign them roles and privileges, and enable them for IdP login by specifying their IdP login ID (ePPN). See [Create New Admin account with IdP Login](#).
- Create IdP users and invite them – You can enroll a new user, assign roles and privileges and send an invitation to the user. See [Create IdP User account and send invitation](#) for more details
- Enable existing administrators for IdP Login – You can invite pre-enrolled administrators to login through their IdP Login Credentials. See [Enable Existing Admins for IdP Login](#).

### Create New Admin Account with IdP Login

- MRAOs (and RAOs with admin creation privileges) can add new users, assign roles and define privileges as required.
- The identity provider and the login credentials for the new user can be specified during creation. Once enrolled, the new administrator can login to InCommon CM using their IdP credentials.


**Note:** RAOs can only add new RAO administrators if 'Allow creation of peer admin users' is enabled for them.

### To add a new administrator:

- Click the 'Admins' tab at the top of the InCommon CM interface.
- Click the 'Add' button to open the 'Add New Client Admin' form.

Dashboard Certificates Discovery Code Signing on Demand Reports

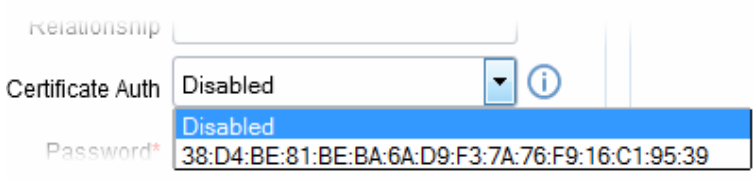
Filter

 **+ Add** Add IdP User

| NAME         | EMAIL                  | LOGIN   | TYPE     |
|--------------|------------------------|---------|----------|
| Forrest Gump | forrest@dithercons.com | forrest | Standard |

### Add New Client Admin

| CREDENTIALS   | PRIVILEGES  | ROLE   |
|---|---|--|
| <p><b>*-required fields</b></p> <p>Login* <input type="text"/></p> <p>Email* <input type="text"/></p> <p>Forename* <input type="text"/></p> <p>Surname* <input type="text"/></p> <p>Title <input type="text"/></p> <p>Telephone Number <input type="text"/></p> <p>Street <input type="text"/></p> <p>Locality <input type="text"/></p> <p>State/Province <input type="text"/></p> <p>Postal Code <input type="text"/></p> <p>Country <input type="text"/></p> <p>Relationship <input type="text"/></p> <p>Certificate Auth Disabled <input type="text"/> ⓘ</p> <p>Identity provider Disabled <input type="text"/></p> <p>IdP Person Id* <input type="text"/></p> <p>Password* <input type="password"/></p> <p>Confirm Password* <input type="password"/></p> | <p><input type="checkbox"/> Allow creation of peer admin users</p> <p><input type="checkbox"/> Allow editing of peer admin users</p> <p><input type="checkbox"/> Allow deleting of peer admin users</p> <p><input type="checkbox"/> Allow SSL details changing</p> <p><input type="checkbox"/> Allow SSL auto approve</p> <p><input type="checkbox"/> WS API use only ⓘ</p> <p><input type="checkbox"/> MS AD Discovery</p> | <p><a href="#">Expand All</a></p> <p><input type="checkbox"/> MRAO Admin</p> <p><input type="checkbox"/> RAO Admin - SSL</p> <p><input type="checkbox"/> RAO Admin - S/MIME</p> <p><input type="checkbox"/> RAO Admin - Code Signing</p> <p><input type="checkbox"/> RAO Admin - Device Certificate</p> <p><input type="checkbox"/> DRAO Admin - SSL</p> <p><input type="checkbox"/> DRAO Admin - S/MIME</p> <p><input type="checkbox"/> DRAO Admin - Code Signing</p> <p><input type="checkbox"/> DRAO Admin - Device Certificate</p> |

| Form Element       | Type       | Description   |
|--------------------|------------|---|
| <b>Credentials</b> |            |   |
| Login*             | Text Field | Enter the login username for the new administrator.   |
| Email*             | Text Field | Enter full email address of the new administrator.  |
| Forename*          | Text Field | Enter first name of the new administrator.  |
| Surname*           | Text Field | Enter surname of the new administrator.   |
| Title              | Text Field | Enter the title for the new administrator.  |
| Telephone Number   | Text Field | Enter the contact phone number for the new administrator.   |
| Street             | Text Field | Enter the address details of the new administrator.   |
| Locality           | Text Field |   |
| State/Province     | Text Field |   |
| Postal Code        | Text Field |   |
| Country            | Drop-down  |   |
| Relationship       | Text Field | The role of the new administrator, for example, 'RAO Admin – SSL'   |
| Certificate Auth   | Drop-down  | <p>Specify whether the new administrator must authenticate themselves to Certificate Manager with their client certificate over a https: connection prior to being granted login rights. The drop-down is auto-populated with the client certificate(s) issued by InCommon CM for the new administrator, based on their email address in the 'Email' field.</p>  <p>If authentication is needed, the administrator can select the certificate from the drop-down. The new administrator can login to InCommon CM, only if the specified certificate is installed on the computer from which he/she attempts to login.</p> |

| Form Element                                  | Type       | Description   |
|---|------------|---|
|   |            | If authentication is not needed, the administrator can select 'Disabled' from the drop-down.  |
| Identity provider                             | Drop-down  | Specify which Identity provider (IdP) InCommon CM should use to authenticate the user's login session. If disabled, InCommon CM will not make use of a federated login and instead rely on itself for user credentials.<br><br><u>Available Options:</u> <ul style="list-style-type: none"> <li>InCommon Federated Login</li> <li>Disabled; (<i>default</i>)</li> </ul>   |
| IdP Person Id                                 | Text Field | Enter the unique identifier of the administrator, as asserted by the IdP. For the InCommon CM, this is the user's eduPersonPrincipalName (ePPN) attribute.  |
| Privileges                                    |            |   |
|   |            | <ul style="list-style-type: none"> <li>By default, new admins will be able to create/edit/delete admins of a lower rank in their role type. For example, an RAO SSL will be able to create a DRAO SSL, but not a DRAO code-signing.</li> <li>If enabled, the 'peer' privileges add the ability to create/edit/delete admins of equivalent rank in their role type. So, for example, an RAO SSL would be able to create another RAO SSL.</li> <li>Some privileges are not relevant to certain roles. For example, 'Allow SSL details changing' will have no impact on a RAO S/MIME.</li> </ul> |
| Allow creation of peer admin users            | Checkbox   | The admin will be able to create new admins with the same role as themselves  |
| Allow editing of peer admin users             | Checkbox   | The admin will be able to modify the details of other admins with the same role as themselves.  |
| Allow deleting of peer admin users            | Checkbox   | The admin will be able to remove admins with the same role as themselves.   |
| Allow domain validation without Dual Approval | Checkbox   | The new administrator will be privileged so that the domain creation/delegation approved by the administrator will be activated immediately, without the requirement of approval by a second MRAO. The checkbox will be active only for Administrators with MRAO role.  |
| Allow DCV                                     | Checkbox   | Enables the new administrator to initiate Domain Control Validation (DCV) process for newly created domains. The privilege is available only for MRAO and RAO/DRAO SSL Administrators.  |
| Allow SSL Details changing                    | Checkbox   | Enables the new MRAO or RAO/DRAO SSL administrator to change  |

| Form Element  | Type       | Description   |
|---|------------|---|
|   |            | the details of SSL certificates from the Certificates > SSL Certificates interface.   |
| Allow SSL auto approve  | Checkbox   | The SSL certificates requested by the MRAO administrator is automatically approved and those by RAO/DRAO SSL administrators are automatically approved by the administrator of same level and await approval from higher level administrator.   |
| WS API use only   | Checkbox   | The administrator account can only be used for API integration. InCommon CM GUI access will not be allowed for this account.  |
| MS AD Discovery   | Checkbox   | Enables the new administrator to access the Settings > MS Agents interface, integrate an AD server to InCommon CM by downloading and installing the MS agent and view the certificates/web servers discovered by the MS agents by scanning respective AD servers.                           |
| Role  |            |   |
| <ul style="list-style-type: none"> <li>MRAO admins are master administrators with access to all organizations, departments and certificate types. (i.e. InCommon staff)</li> <li>RAO admins are responsible for the certificates and users of specific organizations. They also have control over any departments of their organization.</li> <li>DRAO admins are responsible for the certificates and users of specific departments.</li> <li>The RAO and DRAO roles are further divided by certificate type. An administrator of one type of certificate will not be able to manage a different type of certificate. For example, an 'RAO Admin – SSL' will not be able to manage code-signing certificates.</li> <li>You can, however, assign multiple roles to a single administrator. For example, you can assign 'RAO Admin – SSL' and 'RAO Admin – S/MIME' roles to a single admin, allowing them to manage both certificate types.</li> </ul> |            |   |
| <ul style="list-style-type: none"> <li>MRAO Admin</li> <li>RAO Admin – SSL</li> <li>RAO Admin – S/MIME</li> <li>RAO Admin – Code Signing</li> <li>DRAO Admin – SSL</li> <li>DRAO Admin – S/MIME</li> <li>DRAO Admin – Code Signing</li> </ul>   | Checkboxes | <ul style="list-style-type: none"> <li>New RAO and DRAO administrators can be assigned to a particular organization/department by selecting from the list that appears after choosing a role.</li> <li>Click the '+' button beside an organization name to view its departments.</li> </ul> |

- Complete the form and click 'OK' to add the new administrator.
- If you have chosen to display IdP links on your InCommon CM login page then the new admin can follow the link to enter their IdP credentials.
- Otherwise, you can communicate the URL of your IdP login page to new admins as required.

## Create IdP users and invite them

MRAO administrators or RAO administrators with admin creation privileges can add new IdP users assign roles and define privileges for them. The newly created IdP Users need to be approved by another MRAO administrator and then can be sent an invitation mail containing a link to login.

**Note:** RAO administrators can only add IdP templates if 'Allow creation of peer admin users' is enabled for them.

## To add an IdP user account

- Click the 'Admins' tab from the top of the Certificate Manager interface
- Click the 'Add IdP User' button to open the 'Add New Client Admin' form

Add IdP User
✕

| CREDENTIALS   | PRIVILEGES  | ROLE   |
|---|---|--|
| <div style="background-color: #ffffcc; padding: 5px; margin-bottom: 10px;">*-required fields</div> <p>Email* <input type="text"/></p> <p style="text-align: center;"><a href="#">Click here to hide additional fields</a></p> <p>Forename <input type="text"/></p> <p>Surname <input type="text"/></p> <p>Title <input type="text"/></p> <p>Telephone Number <input type="text"/></p> <p>Street <input type="text"/></p> <p>Locality <input type="text"/></p> <p>State/Province <input type="text"/></p> <p>Postal Code <input type="text"/></p> <p>Country <input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100px;" type="text"/> ▾</p> <p>Relationship <input type="text"/></p> | <p><input type="checkbox"/> Allow creation of peer admin users</p> <p><input type="checkbox"/> Allow editing of peer admin users</p> <p><input type="checkbox"/> Allow deleting of peer admin users</p> <p><input type="checkbox"/> Allow SSL details changing</p> <p><input type="checkbox"/> Allow SSL auto approve</p> <p><input type="checkbox"/> MS AD Discovery</p> | <p><a href="#">Expand All</a></p> <p><input type="checkbox"/> MRAO Admin</p> <p><input checked="" type="checkbox"/> RAO Admin - SSL</p> <p><input checked="" type="checkbox"/> RAO Admin - S/MIME</p> <p><input checked="" type="checkbox"/> RAO Admin - Code Signing</p> <p><input checked="" type="checkbox"/> RAO Admin - Device Certificate</p> <p><input checked="" type="checkbox"/> DRAO Admin - SSL</p> <p><input checked="" type="checkbox"/> DRAO Admin - S/MIME</p> <p><input checked="" type="checkbox"/> DRAO Admin - Code Signing</p> <p><input checked="" type="checkbox"/> DRAO Admin - Device Certificate</p> |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/>   |   |  |

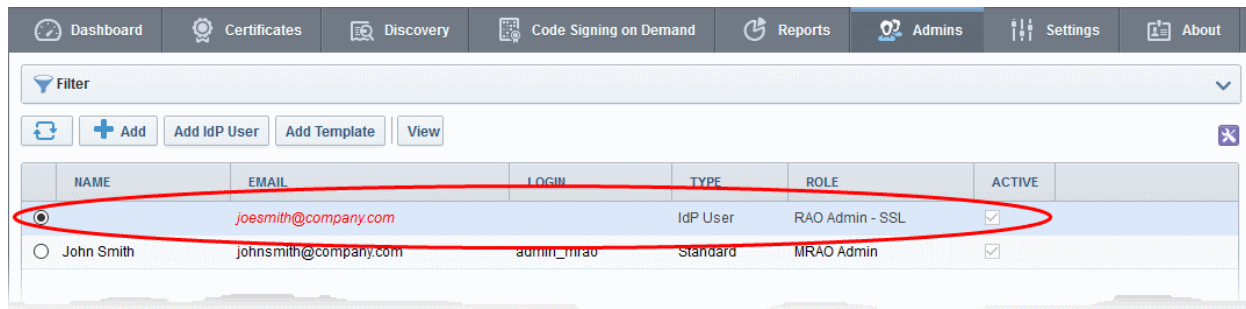
## Add New Client Admin Form - Table of Parameters:

| Form Element   | Type       | Description  |
|--|------------|--|
| <b>Credentials</b>   |            |  |
| Email*   | Text Field | Enter full email address of the new administrator.                     |
| <ul style="list-style-type: none"> <li>Click '<a href="#">Click here to show more fields</a>' to open the additional fields to enter the details of the new administrator. (Optional)</li> </ul> |            |  |
| Forename   | Text Field | Enter first name of the new administrator.                             |
| Surname  | Text Field | Enter surname of the new administrator.                                |
| Title  | Text Field | Enter the title for the new administrator.                             |
| Telephone Number   | Text Field | Enter the contact phone number for the new administrator.              |
| Street   | Text Field | Enter the address details of the new administrator.                    |
| Locality   | Text Field |  |
| State/Province   | Text Field |  |
| Postal Code  | Text Field |  |
| Country  | Drop-down  |  |
| Relationship   | Text Field | The role of the new administrator, for example, RAO SSL Administrator. |

- Privileges – [Click here](#) to view an explanation of the privilege system
- Role – [Click here](#) to view an explanation of roles
- Complete the 'Add New Client Admin' form and click 'OK'.

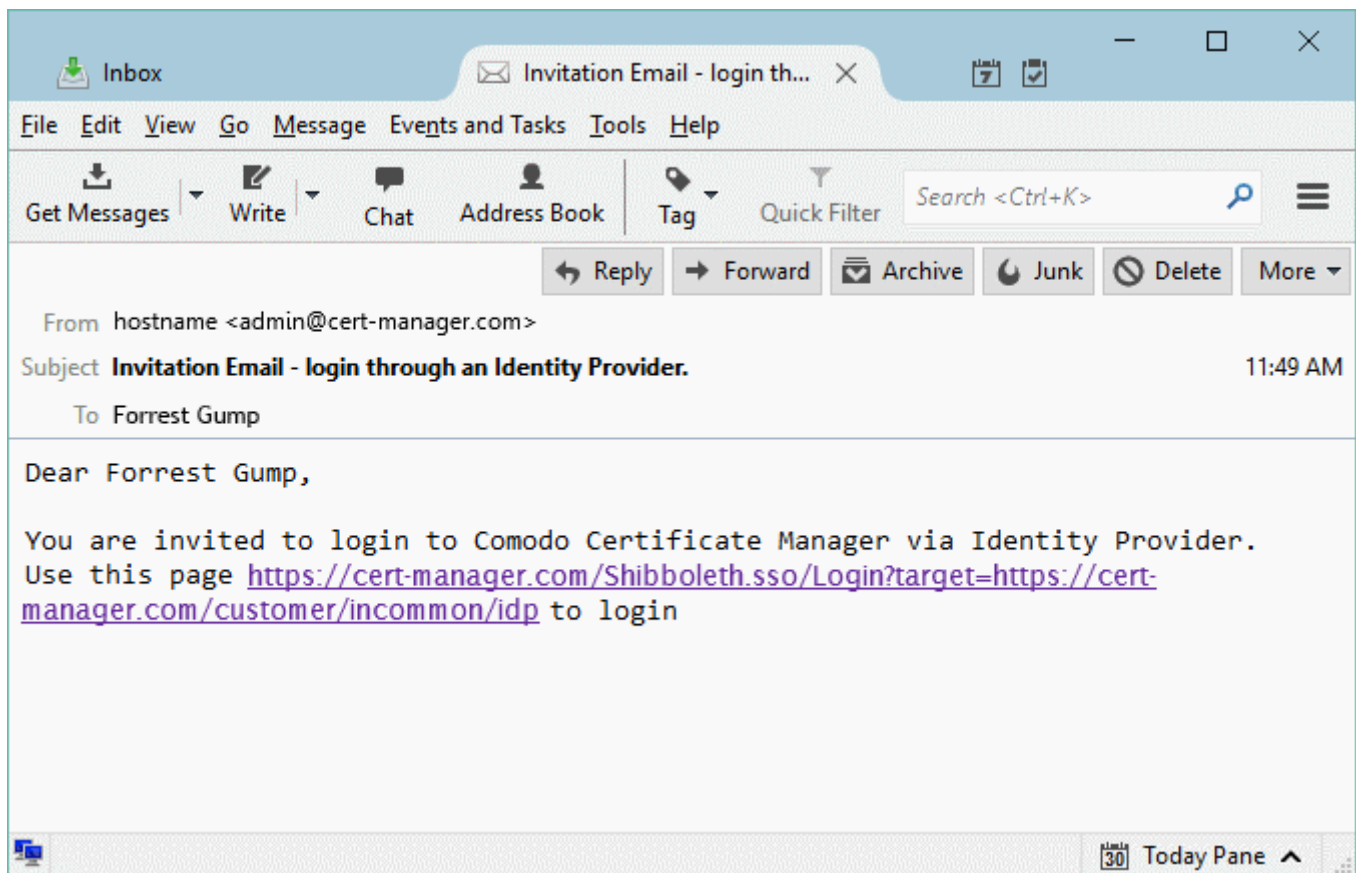
The new user will be added as a new administrator.





| NAME                             | EMAIL                | LOGIN                 | TYPE       | ROLE            | ACTIVE                              |                                     |
|----------------------------------|----------------------|-----------------------|------------|-----------------|-------------------------------------|-------------------------------------|
| <input checked="" type="radio"/> | joesmith@company.com |                       | IdP User   | RAO Admin - SSL | <input checked="" type="checkbox"/> |                                     |
| <input type="radio"/>            | John Smith           | johnsmith@company.com | admin_mrao | Standard        | MRAO Admin                          | <input checked="" type="checkbox"/> |

An invitation mail will be sent to the new IdP user with a link to access the login page.



After clicking the link, the user account will be activated and the user will be taken to the IdP login page.

## Enable Existing Admins for IdP Login

Existing MRAO, RAO and DRAO admins that login through the InCommon login page can be enabled for IdP login in two ways:

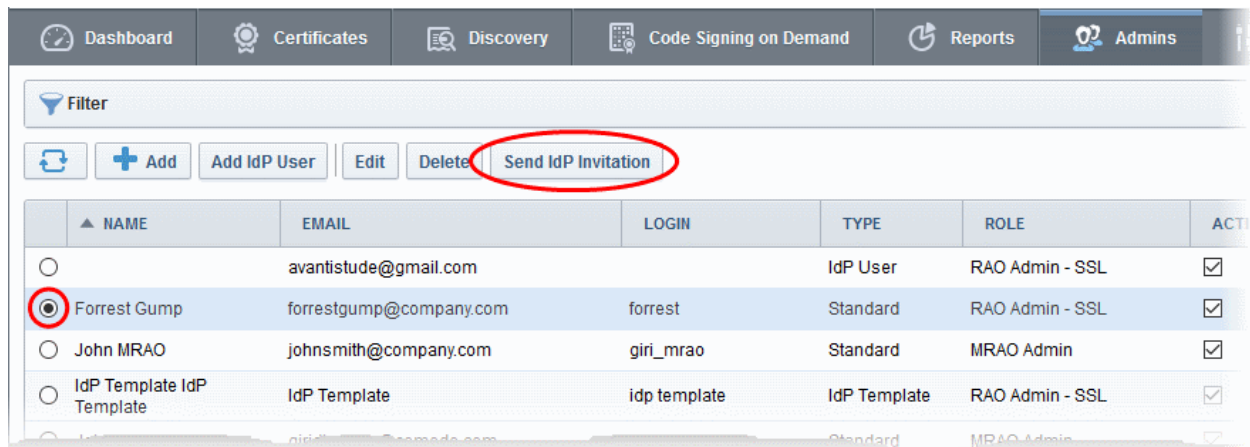
- [Send an IdP Invitation](#)
- [Edit the administrator](#)

### Send an IdP Invitation

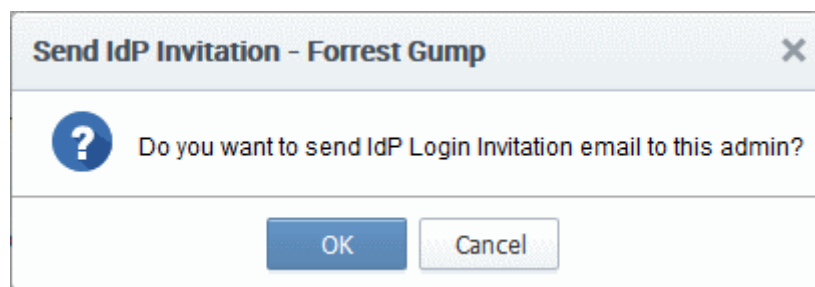
MRAOs (and RAOs with admin creation privileges) can facilitate IdP logins by sending an invitation from the InCommon CM interface. The invitation mail will contain a link for the administrator to login to InCommon CM through the IdP login page.

**To send an invitation to an administrator**

- Click the 'Admins' tab at the top of the CM interface
- Select the administrator you want to enable for IdP login
- Click the 'Send IdP Invitation' button

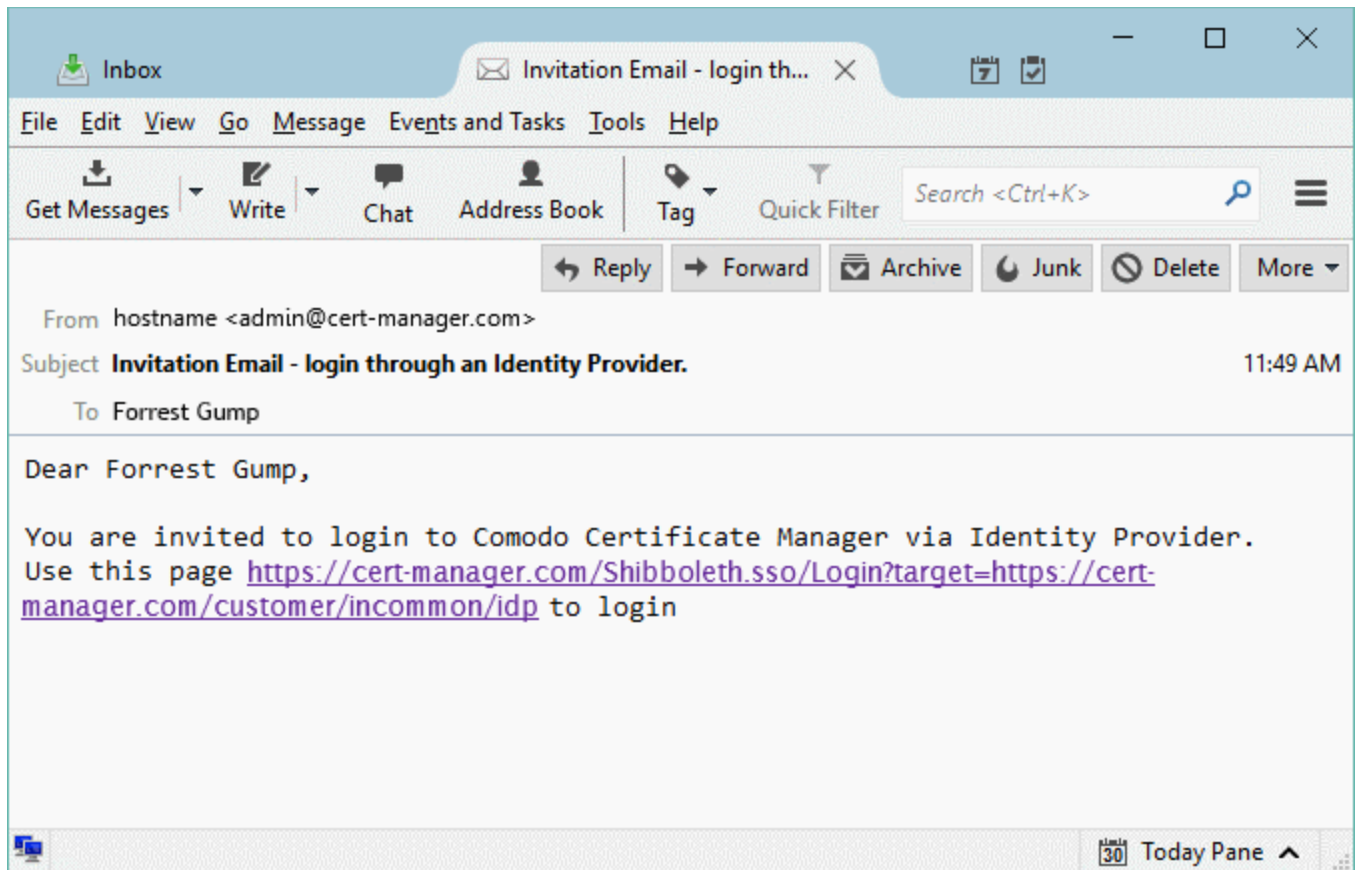


A confirmation dialog will appear:



- Click 'OK' to send the invitation.

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



The admin account will be activated after clicking the link. The admin will be taken to the IdP login page to login to InCommon CM using their IdP credentials.

### Edit the Administrator

An existing administrator can be enabled for IdP login by specifying the IdP to be used and the unique identifier of the administrator.

#### To edit an administrator to enable IdP

- Click the 'Admins' tab at the top of the Certificate Manager interface
- Select the administrator you want to enable for IdP login and click the 'Edit' button.

The 'Edit Client Admin' form will appear:

Edit Client Admin ✕

| CREDENTIALS  | PRIVILEGES   | ROLE  |
|--|--|---|
| <div style="background-color: #ffffcc; padding: 2px; margin-bottom: 5px;">*-required fields</div> <p>Login* <input type="text" value="forrest"/></p> <p>Email* <input type="text" value="forrest@university.edu"/></p> <p>Forename* <input type="text" value="Forrest"/></p> <p>Surname* <input type="text" value="Gump"/></p> <p>Title <input type="text"/></p> <p>Telephone Number <input type="text"/></p> <p>Street <input type="text"/></p> <p>Locality <input type="text"/></p> <p>State/Province <input type="text"/></p> <p>Postal Code <input type="text"/></p> <p>Country <input type="text" value=""/></p> <p>Relationship <input type="text"/></p> <p>Certificate Auth <input style="border: 1px solid #ccc;" type="text" value="Disabled"/> ⓘ</p> <p>Identity provider <input style="border: 1px solid #ccc;" type="text" value="Disabled"/></p> <p>IdP Person Id* <input style="background-color: #eee;" type="text"/></p> <p style="margin-top: 10px;"><a href="#">Reset Password</a></p> | <p><input type="checkbox"/> Allow creation of peer admin users</p> <p><input type="checkbox"/> Allow editing of peer admin users</p> <p><input type="checkbox"/> Allow deleting of peer admin users</p> <p><input checked="" type="checkbox"/> Allow DCV</p> <p><input type="checkbox"/> Allow SSL details changing</p> <p><input type="checkbox"/> Allow SSL auto approve</p> <p><input type="checkbox"/> WS API use only ⓘ</p> | <p><a href="#">Expand All</a></p> <p><input type="checkbox"/> MRAO Admin</p> <p><input checked="" type="checkbox"/> RAO Admin - SSL</p> <p><input type="checkbox"/> RAO Admin - S/MIME</p> <p><input checked="" type="checkbox"/> RAO Admin - Code Signing</p> <p><input type="checkbox"/> DRAO Admin - SSL</p> <p><input type="checkbox"/> DRAO Admin - S/MIME</p> <p><input type="checkbox"/> DRAO Admin - Code Signing</p> |

- Select **InCommon Federated Login** from the Identity provider drop-down selector box.

Identity provider

IdP Person Id\*

InCommon Federated Login

- Once the Identity provider has been selected, please edit the following fields:
  - **IdP Person Id** – Enter the unique identifier for the administrator that is asserted by the IdP. For the InCommon CM, this is the user's eduPersonPrincipalName (ePPN).

Identity provider

IdP Person Id\*

- Complete the form and click 'OK' to save your changes.