COMODO
Creating Trust Online®

Comodo Certificate Manager

Integration of Identity Provider for Single Sign-On

Comodo CA Limited
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Integration of Identity Provider for Single Sign-On

Comodo Certificate Manager (CCM) 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.

CCM requires your IdP account to be integrated with the CCM server and associated with your CCM account. Once associated, you will be able to enroll new users who can login to CCM using with IdP credentials. You can send invitation mails to enrolled staff to login to CCM with their IdP credentials.

New users can login in two ways:

- Place the IdP login link on your CCM account login page. Users can click the link to open the IdP login page and enter their SSO credentials to access CCM.
- Comodo will generate an IdP login URL. Communicate this URL to new users. Users can visit the URL and login to CCM using their IdP credentials.

This document gives a walk through on how to setup IdP for your CCM account and enroll new administrators who will be enabled to login using their IdP credentials.

Process in short:

- Step 1 - Establish communication between CCM server and your IdP service provider server
- Step 2 - Add the IdP service provider to CCM and assign it to your CCM account
- Step 3 - Create IdP User accounts
  - Create new admin account with IdP Login
  - Create IdP User account template
  - Create IdP users and invite them
  - Enable Existing Admins for IdP Login

Step 1 - Establish communication between CCM server and your IdP service provider server

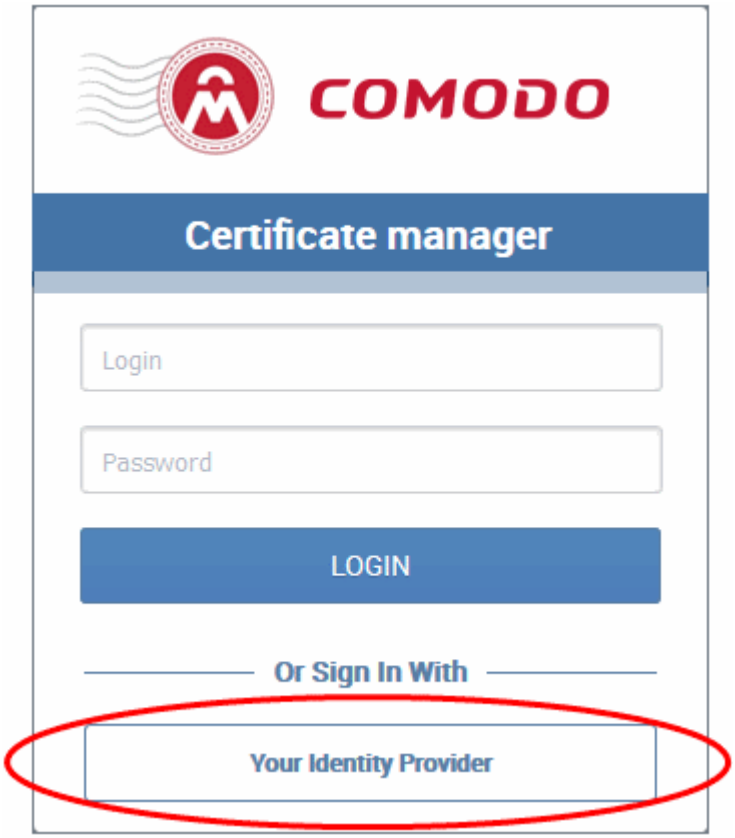
In order for CCM to securely connect to your IdP server, a communication channel needs to be established between the two via an exchange of meta data between the servers. This involves two steps:

- You need to obtain the IdP meta data from your IdP service provider and forward the same as a .xml file to your Comodo Account Manager. The meta data will be stored in the cloud based CCM storage provider (SP) server.
- Your Comodo Account Manager will provide the service provider meta data to you. You should forward the same to your IdP, for storage on your IdP cloud server, communicable by CCM.

Step 2 - Add the IdP service provider to CCM and assign it to your account

Once the communication channel is established, your IdP will be added to CCM and associated with your account by the administrators at Comodo. You can choose from the following options:

- IdP login link on CCM login page - Your CCM account login page will contain an IdP login link. An example is shown below:



If you do not want the links to be displayed, a unique IdP login URL will be generated by the Account Manager and given to you. You can communicate the URL facilitating your users to login to CCM by visiting that URL

- Multi-factor Authentication - If required, multi-factor authentication (MFA) can be set for your account. In addition to IdP username and password, the users need to authenticate themselves with second factor authentication like One Time Password (OTP) sent to their phone, codes generated by authentication apps on their phones and more. If chosen for MFA, you need to specify the mode of second factor authentication.
- New users that directly login to CCM through IdP credentials without being enrolled, will be automatically added as Administrators with privileges as defined in IdP template of your CCM account.

Once assigned, your Comodo Account Manager will be providing the IdP Login URL for your account. Your staff members can just visit the URL and access the CCM console by logging-in with their IdP credentials.

Step 3 - Create IdP User accounts

The next step is to create user accounts for users to login through IdP credentials and/or enable existing standard administrators to login through their IdP login credentials. There are four 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 Identity Provider and IdP login ID. See **Create New Admin account with IdP Login**.
- IdP User account template - You can create a template with defined roles and privileges. Any new users that are not pre-enrolled but invited directly to login to CCM, will be assigned with roles and privileges as defined in the template. See **Create IdP User account template** for more details.
- 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**.

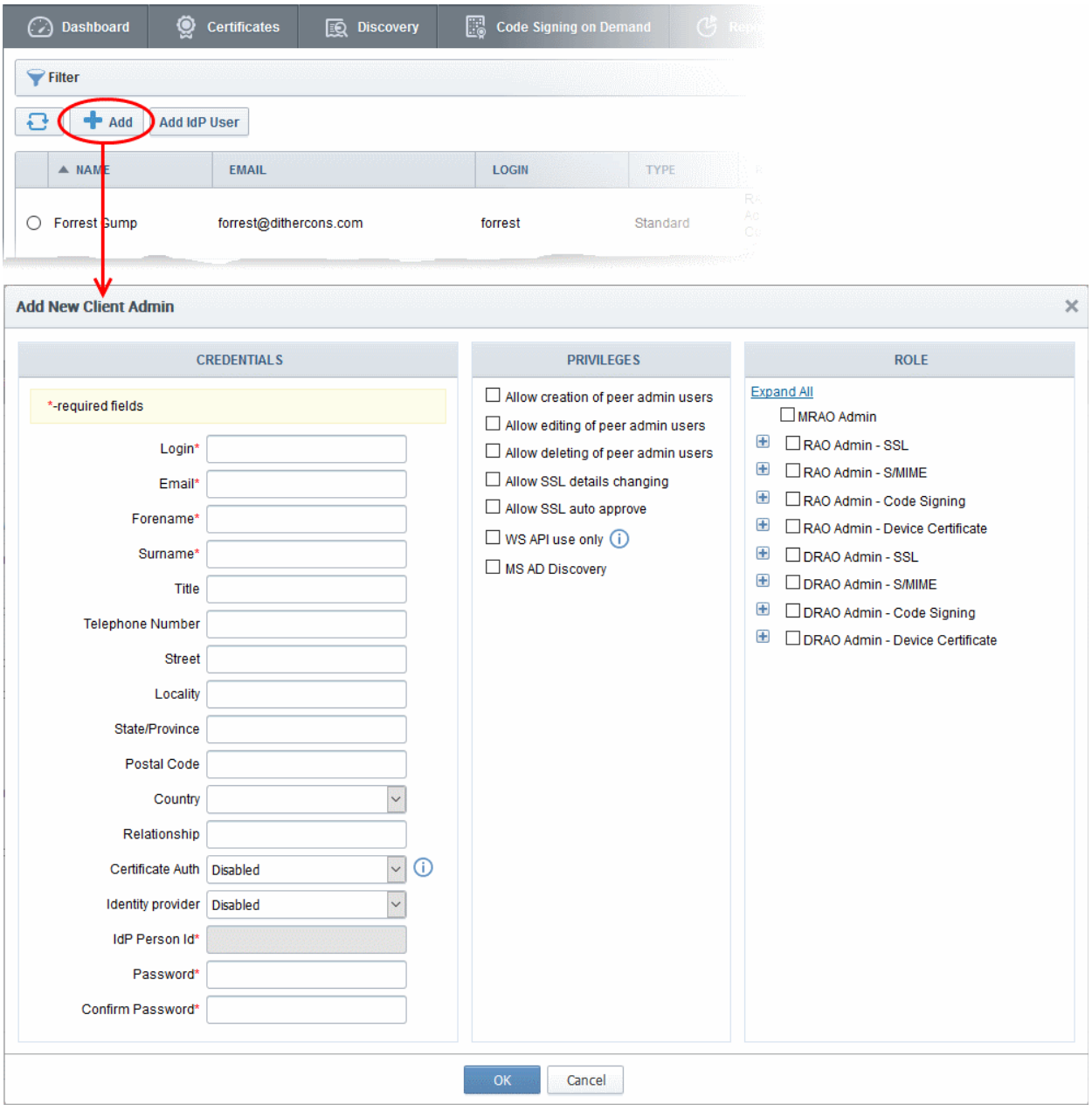
Create New Admin Account with IdP Login

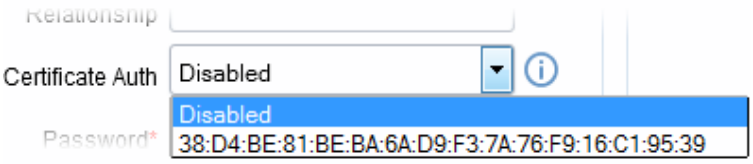
- MRAOs (and RAOs with admin creation privileges) can add new users, assign roles and define privileges as required.
- The identity provider and the login credentials for the new user can be specified during creation. Once enrolled, the new administrator can login to CCM using their IdP credentials.

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

To add a new user

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



Form Element	Type	Description
Credentials		
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 Locality State/Province Postal Code Country	Text Field Text Field Text Field Text Field Drop-down	Enter the address details of the new administrator.
Relationship	Text Field	The role of the new administrator, for example, RAO SSL Administrator.
Certificate Auth	Drop-down	Specify whether the new administrator must authenticate themselves to Certificate Manager with his/her 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 CCM for the new administrator, based on his/her email address in the 'Email' field.  If authentication is needed, the administrator can select the certificate from the drop-down. The new administrator can login to CCM, only if the specified certificate is installed on the computer from which he/she attempts to login. If authentication is not needed, the administrator can select 'Disabled' from the drop-down.
Identity Provider	Drop-down	Choose the Identity Provider account to be used by the administrator to login to CCM Tip: You can enable IdP login for the admin at any time in the future by sending an IdP invitation or by editing the admin account. See Enable Existing Admins for IdP Login for more help with this.
IdP Person Id	Text Field	Enter the unique identifier for the administrator in the IdP realm. The identifier can be obtained from the meta data provided by the IdP service provider. Tip: Usually the 'IdP Person Id' value for a user can be obtained from the value of the 'Person Principal Name' (PPn) field in the meta data. This may vary for different IdP service providers. Contact your IdP

Form Element	Type	Description
		service provider for help on this.
Password* Confirm Password*	Text Fields	Enter the password for the new administrator to access the CCM interface and reenter the same for confirmation. The new administrator will need to change the password upon his/her first login.
Privileges		
Administrator can assign admin management privileges to the new administrator. The new administrator will be able to add, edit or remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected here.		
Allow creation of peer admin users	Checkbox	Enables the new administrator to add new administrators from their management interface.
Allow editing of peer admin users	Checkbox	Enables the new administrator to edit roles of existing administrators from their management interface.
Allow deleting of peer admin users	Checkbox	Enables the new administrator to remove existing administrators from their management interface.
Note: The new administrator can create, edit or delete the other administrators of their own tier and administrators of the lower tier.		
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 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. CCM 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 CCM by downloading and installing the MS agent and view the certificates/web servers discovered by the MS agents by scanning respective AD servers.
Note: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.		
Role		
Administrator can assign the role to the new administrator.		
• MRAO Admin	Checkboxes	The new Administrator can be assigned to a particular

Form Element	Type	Description
• RAO Admin SSL • RAO Admin S/MIME • RAO Admin Code Signing • RAO Device Cert • DRAO Admin SSL • DRAO Admin S/MIME • DRAO Admin Code Signing • DRAO Device Cert		Organization/Department by selecting the appropriate Organization/Department from the list that appears after selecting a role. All Organizations are listed by default. Clicking the '+' button beside the Organization name expands the tree structure to display the Departments associated with the Organization. • Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. • Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization.

- Complete the form and click 'OK' to add the new administrator.
- If you have chosen to display IdP links on your CCM 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.

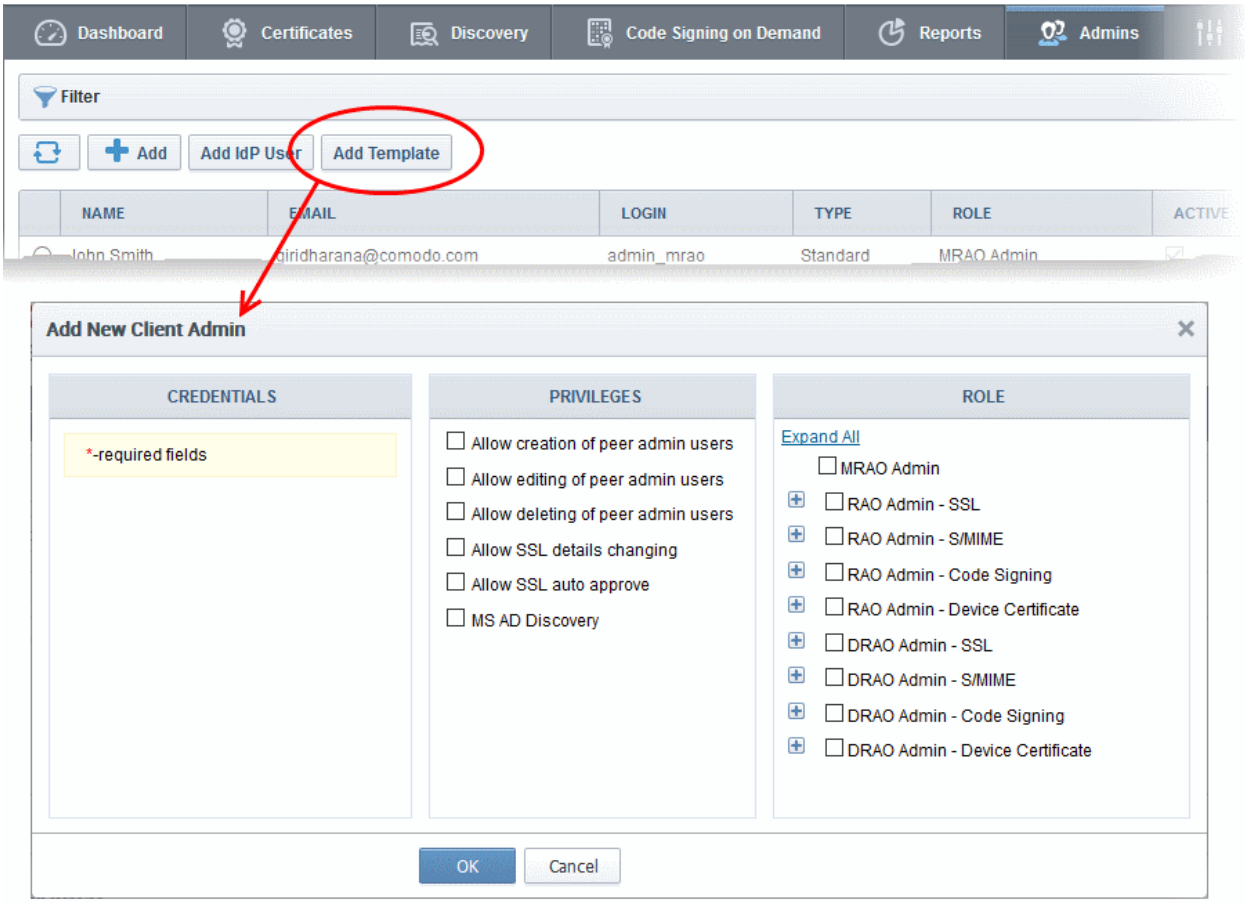
Create IdP User account template

MRAOs (and RAOs with admin creation privileges) can create an IdP template on their CCM account and assign roles and define privileges. Users that were not previously enrolled but invited directly to login to CCM using their IdP credentials will be assigned roles and privileges as defined in the template.

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

To add an IdP template

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



Add New Client Admin Form - Table of Parameters:

Form Element	Type	Description
Privileges		
Administrators can assign admin management privileges to the new administrator template. The new administrator added by logging-in to CCM through IdP Login credentials, will be able to add, edit or remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected here.		
Allow creation of peer admin users	Checkbox	Enables the new administrator to add new administrators from their management interface.
Allow editing of peer admin users	Checkbox	Enables the new administrator to edit roles of existing administrators from their management interface.
Allow deleting of peer admin users	Checkbox	Enables the new administrator to remove existing administrators from their management interface.
Note: The new administrator can create, edit or delete the other administrators of their own tier and administrators of the lower tier.		
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. This checkbox will be active only for Administrators with MRAO role. Refer to the section Domains for more details.
Allow DCV	Checkbox	Enables the new administrator to initiate Domain Control Validation (DCV) process for newly created domains. The privilege is available

Form Element	Type	Description
		only for MRAO and RAO/DRAO SSL Administrators.
Allow SSL Details changing	Checkbox	Enables the new MRAO or RAO/DRAO SSL administrator to change 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.
MS AD Discovery	Checkbox	Enables the new administrator to access the Settings > MS Agents interface, integrate an AD server to CCM by downloading and installing the MS agent and view the certificates/web servers discovered by the MS agents by scanning respective AD servers.
Note: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.		
Role		
Administrator can assign the role to the new administrator.		
• MRAO Admin • RAO Admin SSL • RAO Admin S/MIME • RAO Admin Code Signing • RAO Device Cert • DRAO Admin SSL • DRAO Admin S/MIME • DRAO Admin Code Signing • DRAO Device Cert	Checkboxes	The new Administrator can be assigned to a particular Organization/Department by selecting the appropriate Organization/Department from the list that appears after selecting a role. All Organizations are listed by default. Clicking the '+' button beside the Organization name expands the tree structure to display the Departments associated with the Organization. • Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. • Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization.

- Complete the 'Add New Client Admin' form and click OK.

Once a template is created, you can allow new users to login to CCM without being pre-enrolled in two ways.
If you have opted for display of IdP links on your CCM Login page, you can communicate your CCM Login page URL to the new user. They can click the IdP login link on the login page and enter their IdP credentials to login to CCM.
If you have not opted for display of IdP links to be displayed, you can communicate the direct IdP login URL provided by your Comodo Account manager to the new user. They can visit the URL and enter the IdP login credentials to access CCM.

Once the user logs-in to CCM he/she will be assigned with roles and privileges as defined in the template.

Create IdP users and invite them

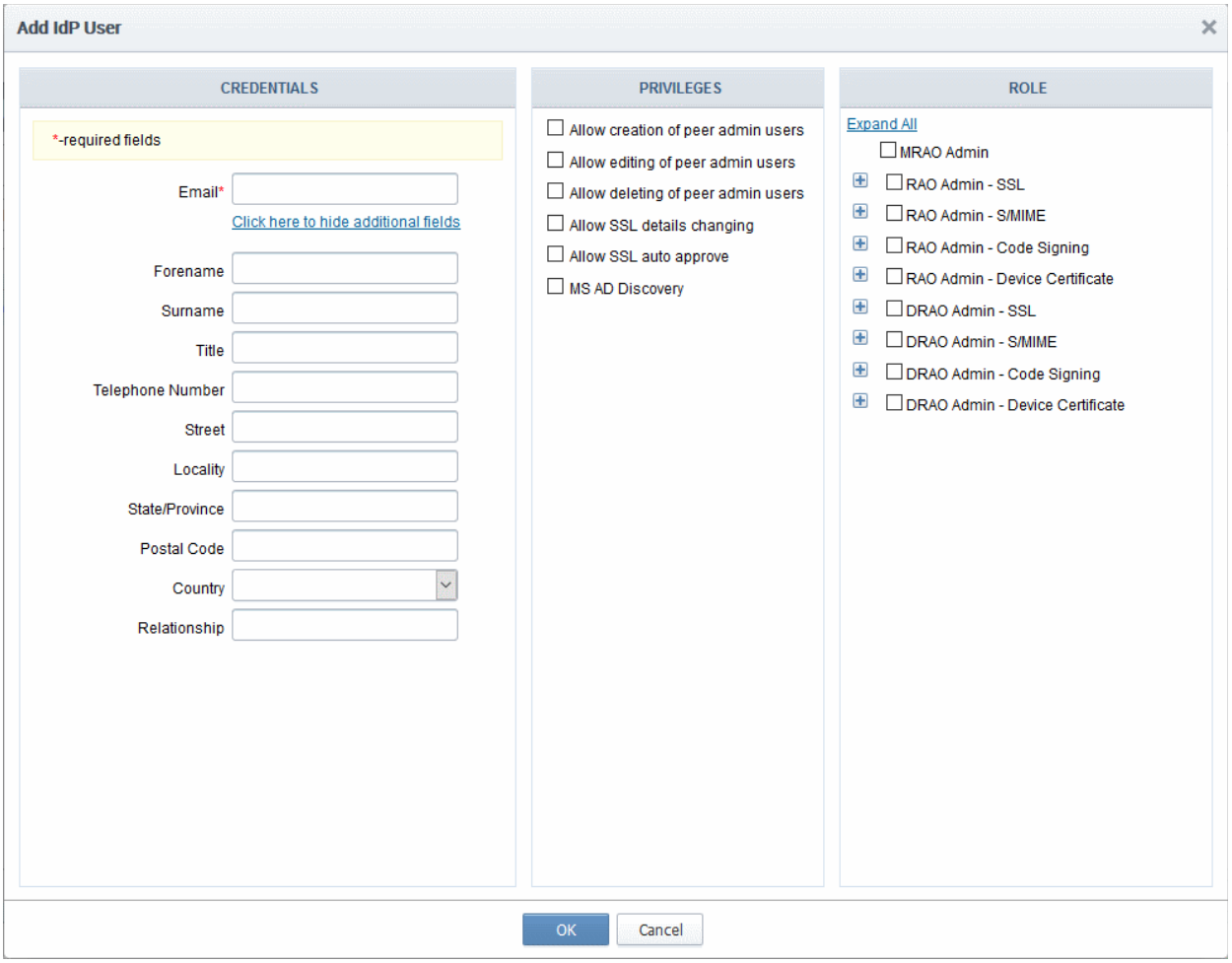
MRAO administrators or RAO administrators with admin creation privileges can add new IdP users, assign roles and define privileges for them. The newly created IdP Users need to be approved by another MRAO administrator and

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



Add New Client Admin Form - Table of Parameters::

Form Element	Type	Description
Credentials		
Email*	Text Field	Enter full email address of the new administrator.
• Click 'Click here to show more fields' to open the additional fields to enter the details of the new administrator. (Optional)		
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.

Form Element	Type	Description
Street Locality State/Province Postal Code Country	Text Field Text Field Text Field Text Field Drop-down	Enter the address details of the new administrator.
Relationship	Text Field	The role of the new administrator, for example, RAO SSL Administrator.
Privileges		
Administrator can assign admin management privileges to the new administrator. The new administrator will be able to add, edit or remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected here.		
Allow creation of peer admin users	Checkbox	Enables the new administrator to add new administrators from their management interface.
Allow editing of peer admin users	Checkbox	Enables the new administrator to edit roles of existing administrators from their management interface.
Allow deleting of peer admin users	Checkbox	Enables the new administrator to remove existing administrators from their management interface.
Note: The new administrator can create, edit or delete the other administrators of their own tier and administrators of the lower tier.		
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. This 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 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.
MS AD Discovery	Checkbox	Enables the new administrator to access the Settings > MS Agents interface, integrate an AD server to CCM by downloading and installing the MS agent and view the certificates/web servers discovered by the MS agents by scanning respective AD servers.
Note: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.		
Role		
Administrator can assign the role to the new administrator.		

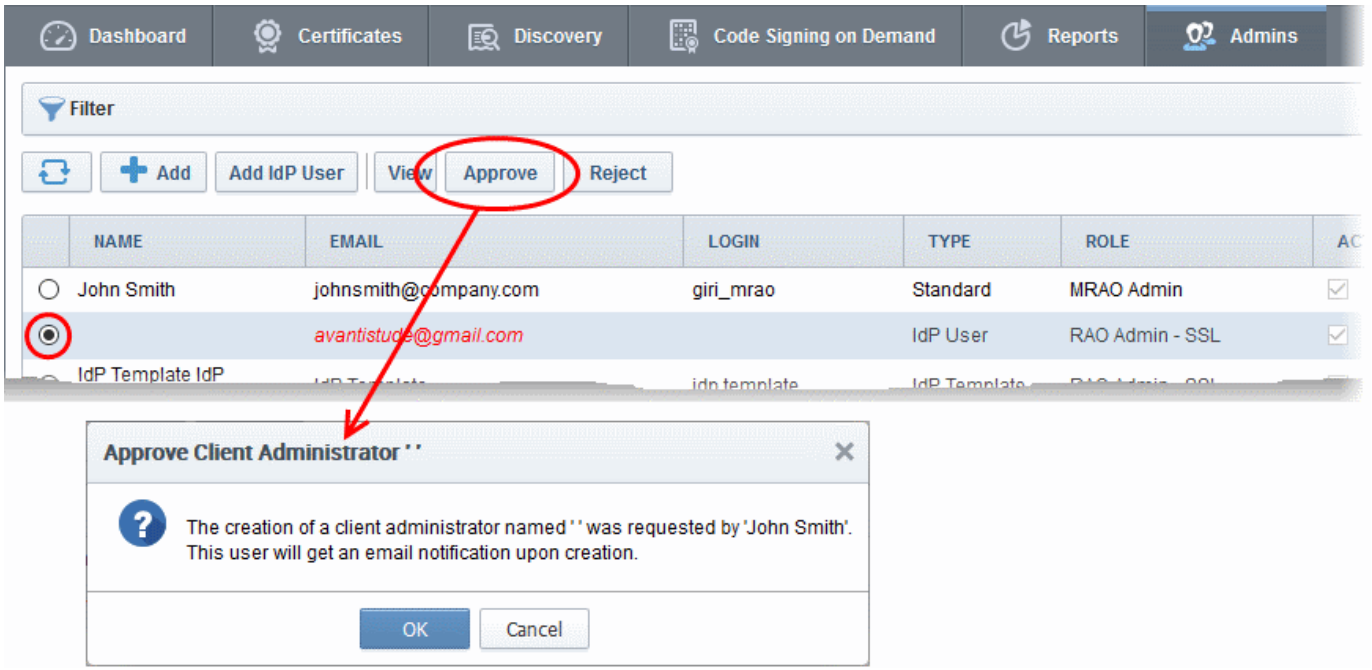
Form Element	Type	Description
• MRAO Admin • RAO Admin SSL • RAO Admin S/MIME • RAO Admin Code Signing • RAO Device Cert • DRAO Admin SSL • DRAO Admin S/MIME • DRAO Admin Code Signing • DRAO Device Cert	Checkboxes	The new Administrator can be assigned to a particular Organization/Department by selecting the appropriate Organization/Department from the list that appears after selecting a role. All Organizations are listed by default. Clicking the '+' button beside the Organization name expands the tree structure to display the Departments associated with the Organization. • Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. • Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization.

- Complete the 'Add New Client Admin' form and click OK.

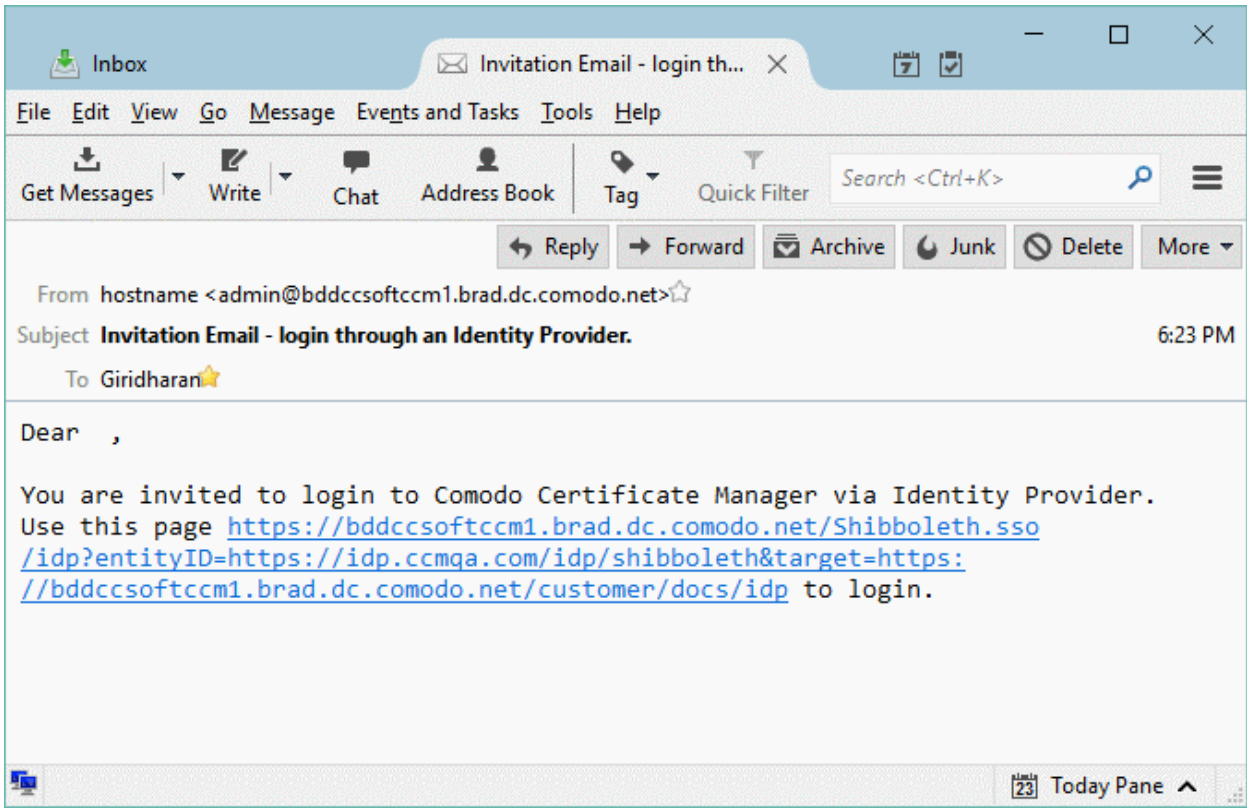
The new user will be added as a new administrator.

The new IdP user needs to be approved by another MRAO administrator.

Another MRAO administrator can approve the new user by selecting the new IdP user and clicking the 'Approve' button at the top.



Once approved, an invitation mail will be sent to the new IdP user with a link to access the login page.



The user account will be activated after clicking the link. The user will be taken to the IdP login page to login to CCM using his/her IdP credentials.

Enable Existing Admins for IdP Login

Existing MRAO, RAO and DRAO admins can be enabled for IdP login in two ways:

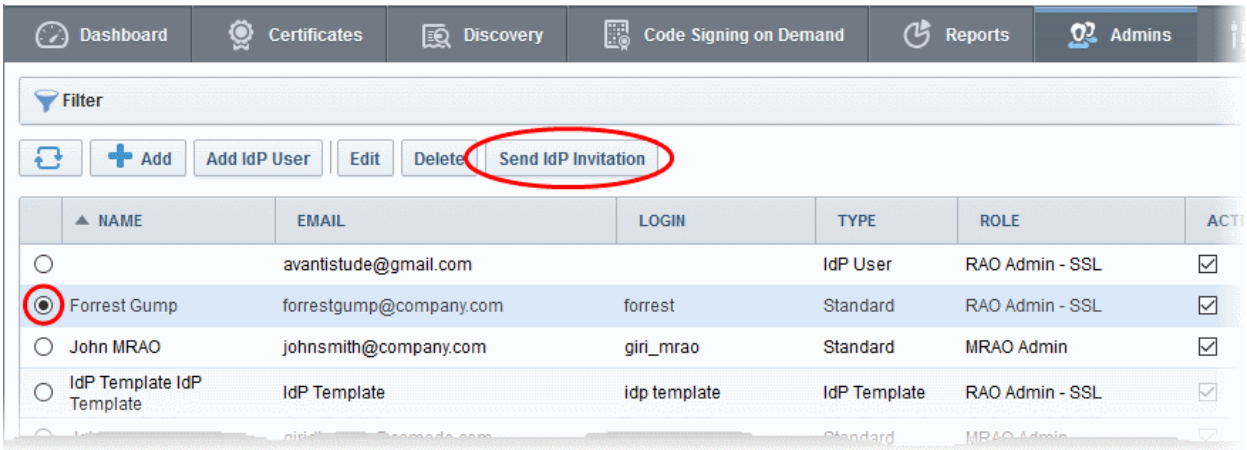
- Send an IdP Invitation
- Edit the administrator

Send an IdP Invitation

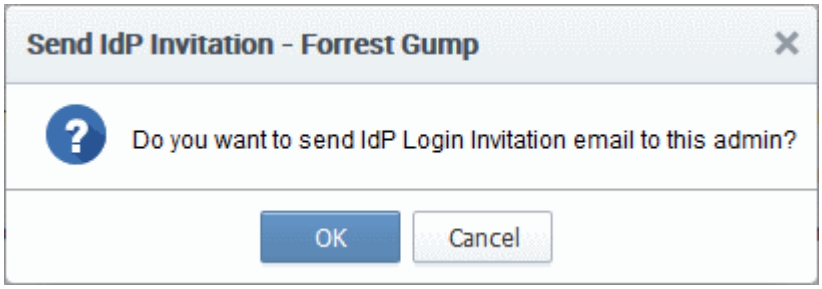
MRAOs (and RAOs with admin creation privileges) can facilitate IdP logins by sending an invitation from the CCM interface.

To send an invitation to an administrator

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

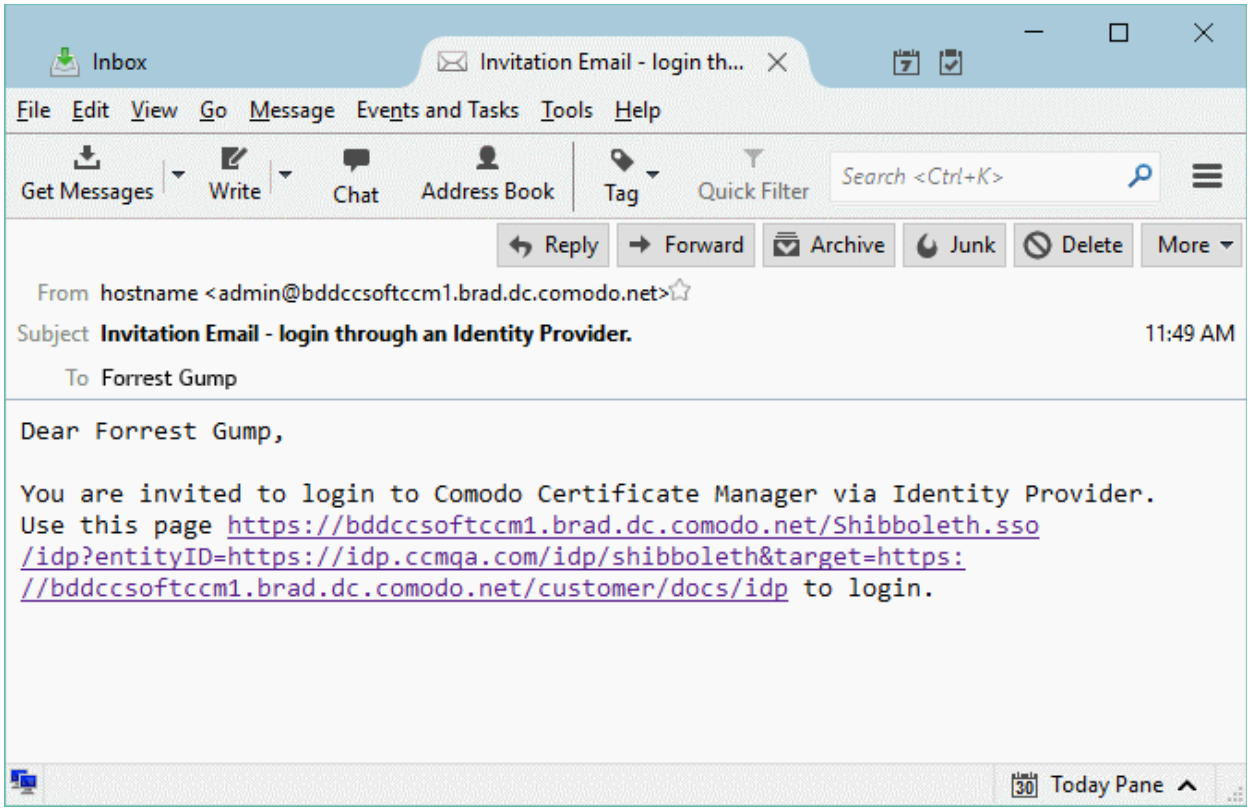


A confirmation dialog will appear.



- Click 'OK' to send the invitation.

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



After clicking the link, the admin account will be activated. The administrator will be taken to the IdP login page to login with his/her IdP credentials.

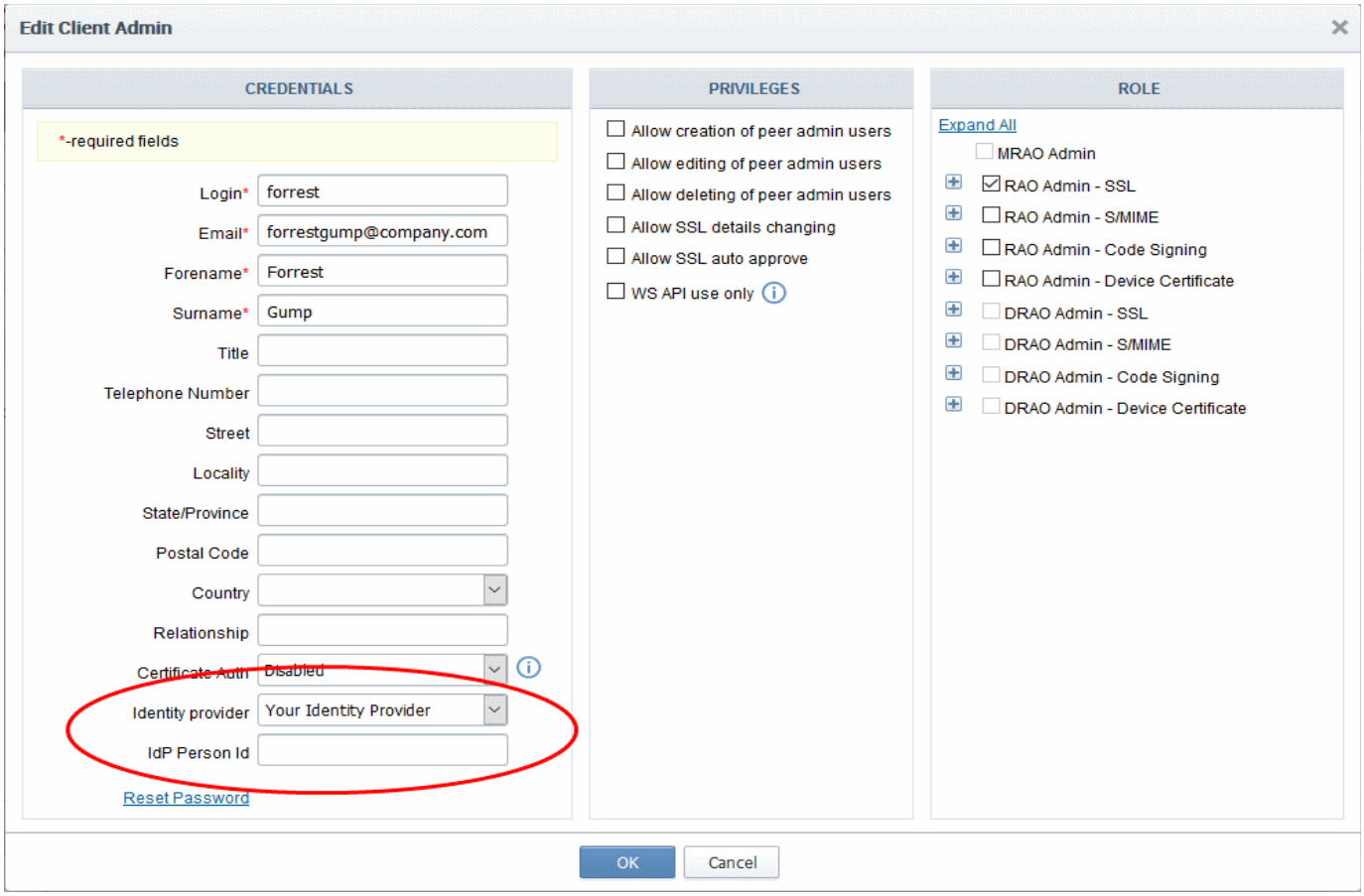
Edit the Administrator

A standard administrator can be enabled for IdP login by specifying the IdP account to be used and the unique identifier for the administrator in the IdP database.

To edit an administrator for enabling IdP

- Click the 'Admins' tab from 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 the following fields:
  - **Identity Provider** - Choose the Identity Provider account to be used by the administrator from the drop-down.
  - **IdP Person Id** - Enter the unique identifier for the administrator in the IdP realm. The identifier can be obtained from the meta data provided by the IdP service provider.

Tip: Usually the 'IdP Person Id' value for a user can be obtained from the value of the 'Person Principal Name' (PPn) field in the meta data, but this may differ for different IdP service providers. Contact your IdP service provider for help on this.

- Click 'OK' to for your settings to take effect

If you have chosen to display IdP links on your CCM Login page, the administrator can click the IdP login link on the login page and enter their IdP credentials to login to CCM.

If you have not chosen to display IdP links, you can communicate the direct IdP login URL provided by your Comodo Account manager to the administrator. They can visit the URL and enter the IdP login credentials to access CCM.

About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767