

InCommon Certificate Service - Single Sign-on and MFA



SSO and MFA Available

The use of single sign-on and multifactor authentication for accessing the Comodo Certificate Manager is available to any subscriber that also operates an Identity Provider in the InCommon Federation. See the Identity Provider setup requirements [on this wiki page](#).

Also, in order to use this new service, your IdP must support the [REFEDS MFA Profile](#).

The InCommon Certificate Service offers single sign-on convenience, and the security of multifactor authentication (MFA), for logging in to the Comodo Certificate Manager (CCM) by those who administer their organization's certificates.

- Single sign-on (SSO) is available to both RAOs (Registration Authority Officers) and DRAOs (Departmental Registration Authority Officers)
- The organization must have an identity provider (IdP) in the InCommon Federation
- The organization's IdP must be configured to support the [REFEDS MFA profile](#)

Benefits

The benefits of using SSO and MFA include:

- Removes the need to maintain a separate set of login credentials with the Comodo Certificate Manager
- Eliminates the need for the RAO to request password resets from InCommon (which is time-consuming for both RAOs and InCommon staff)
- The InCommon Certificate service is used by organizations as the basis of internal and external trust. Protecting it with MFA reduces the likelihood of stolen credentials.
- MFA protected SSO increases security by leveraging protected campus credentials that RAOs already use in their local context to access higher security services.