COMODO
Creating Trust Online®

# Comodo
# Certificate Manager

## Authentication at Web Service API

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

# 1. Introduction to Authentication at Web Service API

CCM offers two ways to authenticate users accessing its various services via SOAP API and REST API services. The authentication methods are:

- **Authentication via Login and Password**
- **Authentication via Login and a Client Certificate**

# 2. Authentication via Login and Password

**Prerequisite**

- Users should have CCM login credentials and the correct customer login URI
- For the Web Service API, access must be enabled for the customer by Comodo and for each org/dept by admins on the client side.

The URLs for the login/password authentication method are:

**SOAP API Service**

- https://<*CCM Server*>:<*port*>/ws/<*Service Name*>

| Parameter | Description |
|---|---|
| <CCM Server> | The address of the CCM server you use. For example, '*cert-manager.com*' *or hard.cert-manager.com.* |
| <port> | The default port number is 443. |
| <Service Name> | The name of the web service you want to login to. |

Example:

*https://cert-manager.com:443/ws/ EPKIManager*

**REST API Service (for Code Signing on Demand)**

- https://<*CCM Server*>:<*port*>/api/csod/v1/requests

| Parameter | Description |
|---|---|
| <CCM Server> | The address of the CCM server you use. For example, '*cert-manager.com*' *or hard.cert-manager.com.* |
| <port> | The default port number is 443. |

Example:

*https://cert-manager.com:443/api /csod/v1/requests*

Authentication is performed by sending the AuthData parameter to the web service API. This includes the login, password and Customer URI. After successful authentication, the admin can proceed to the CCM management interface. If authentication is not successful (login and/or password are incorrect, password has expired), the admin will see an error and will be denied access to the Web Service API. The same admin could, however, still authenticate themselves via a client certificate (refer to the **next section**).

# 3. Authentication via Login and a Client Certificate

**Prerequisite**

- Admins should have the Customer URI
- For the Web Service API, access must be enabled for the customer by Comodo and for each org/dept by admins on the client side.
- Admins should have 'Certificate Auth' enabled. The authentication certificate must requested and issued via CCM and active at the moment of authentication.

The URLs for the login/certificate authentication method are:

**SOAP API Service**

- https://<*CCM Server*>:<*port*>/private/ws/<*Service Name*>

| Parameter | Description |
|---|---|
| <CCM Server> | The address of the CCM server you use. For example, '*cert-manager.com*' *or hard.cert-manager.com.* |
| <port> | The default port number is 443. |
| <Service Name> | The name of the web service you want to login to. |

Example:

*https://cert-manager.com:443/private/ws/ EPKIManager*

**REST API Service (for Code Signing on Demand)**

- https://<*CCM Server*>:<*port*>/private/api/csod/v1/requests

| Parameter | Description |
|---|---|
| <CCM Server> | The address of the CCM server you use. For example, '*cert-manager.com*' *or hard.cert-manager.com.* |
| <port> | The default port number is 443. |

Example:

*https://cert-manager.com:443/private/api /csod/v1/requests*

The certificate must be provided by the admin's client at the time of login. After receiving the authdata parameter (customer URI and login), CCM will verify that the certificate matches the one specified in the 'Certificate Auth' area of the admin's profile. After successful authentication, the admin can proceed to the CCM management interface. If authentication is not successful (login and/or password are incorrect, certificate is not correct/revoked), the admin will see an error and will be denied access to the Web Service API. The same admin could, however, still authenticate themselves using the login and password method (see **previous section**).

# 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