

DigiCert CertCentral API Key Generation and CertSecure Manager Requirements

Purpose

This document explains how to generate an API key in DigiCert CertCentral and outlines the full set of requirements to integrate it with the CertSecure Manager Connector, including prerequisites related to account setup, domain validation, certificate availability, and billing balance.

Section 1: Prerequisites for API Key Generation

1. Active DigiCert CertCentral Account

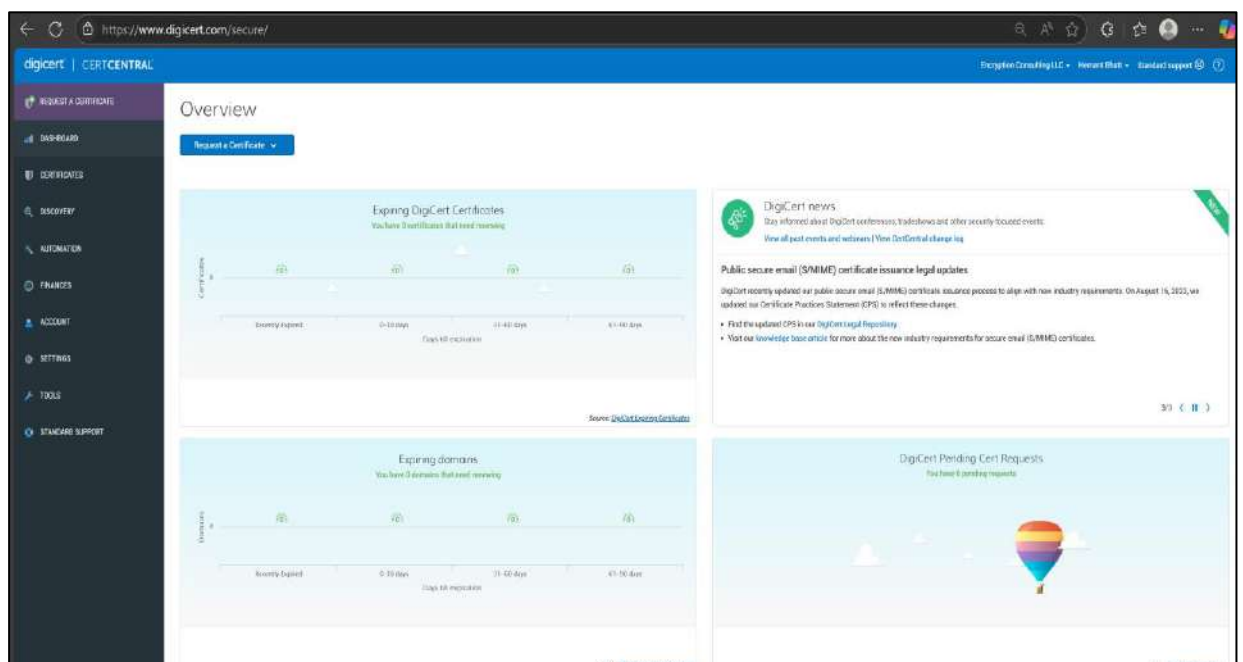
You must have a valid and accessible DigiCert CertCentral account.

2. User Role with API Permissions

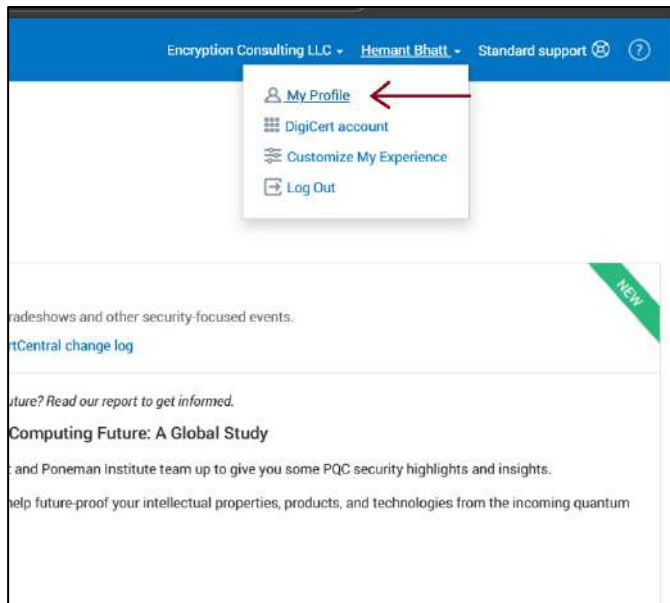
Recommended roles: Administrator or Manager. Other roles may have limited API access.

Steps to Generate an API Key

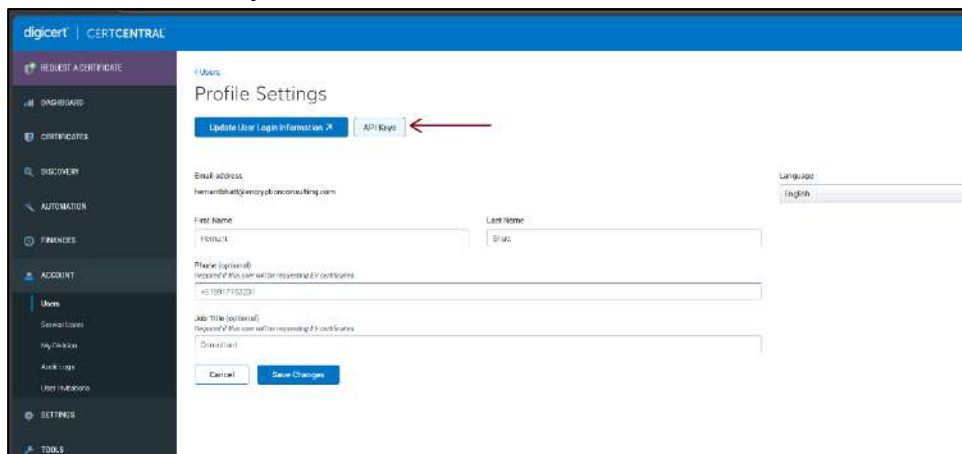
1. Log in at <https://www.digicert.com/account/login.php>



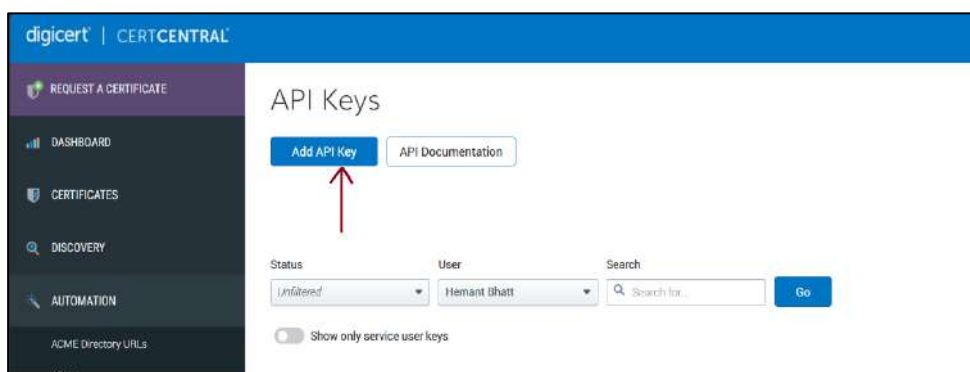
2. Click your username in the top-right corner
3. Select "My Profile"



4. Click on the “API Keys” button.



5. Click on “Add API Key”



6. In the Add API Key dialog box, enter the following details:
 - Description: Provide a brief explanation of where or how the API key will be used.
Example: CSM Connector Integration
 - User: Select a valid user account with the necessary permissions. The key will inherit this user’s access rights.

- **API Key Restriction (Optional):** Define specific areas where the key is allowed to operate, such as certificate order or domain management. This helps limit the key's scope and improves security.

Add API Key

Description
CertSecure Manager Connector Key

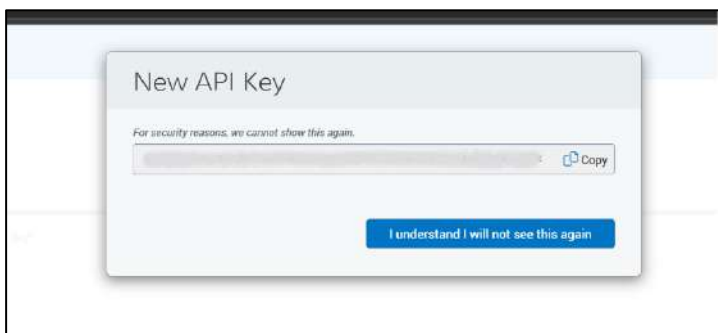
User
When you assign an API key to a user, you link the user's permissions to the key.
Hemant Bhatt

API key restrictions (optional)
Further restrict the API key permissions to a defined set of actions.

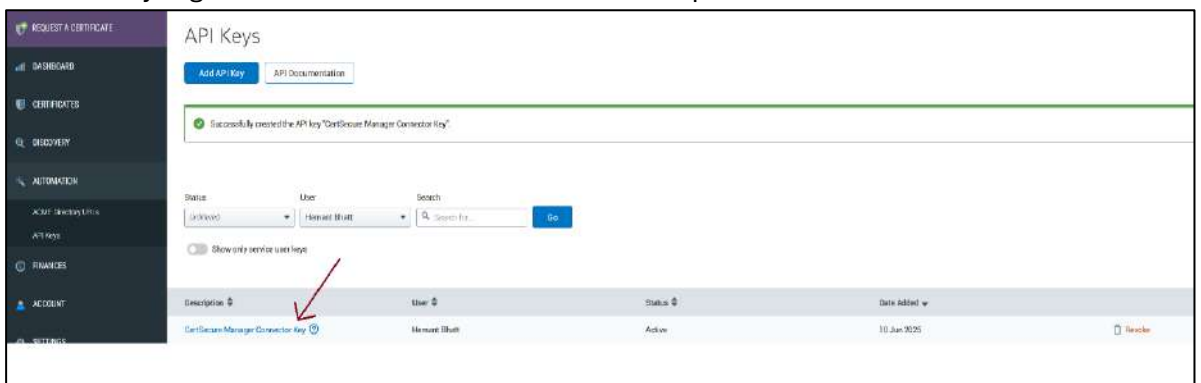
None
Orders
Orders, Domains, Organizations
View Only
User Management

Click on “Add API Key” button then.

7. Copy the API key generated and store it at a secure location, as it will not be shown again.



8. Now the key is generated and listed on the CertCentral platform.



Section 2: Additional Requirements for CertSecure Manager Connector Integration

1. Domain Control Validation (DCV)

The domains you plan to request certificates for must be pre-validated in DigiCert. You can check domain status from the CertCentral dashboard under the “Certificates” → “Domains” section.

2. **Available Certificate Types**

You must have at least one type of certificate available in your CertCentral account.

Examples:

- SSL/TLS Certificates (OV, DV, EV)
- Code Signing Certificates
- Client Authentication Certificates
- Document Signing Certificates

3. **Sufficient Account Balance or Contracted Product Access**

- Either pre-paid balance or contract entitlements must be available for API-based issuance to succeed.
- You can check this under Billing or by contacting your DigiCert account manager

4. **CertSecure Manager Connector Configuration**

Once the API key is generated, and the above conditions are met:

- The CLM Connector must be configured with the API key
- Ensure the connector has access to the DigiCert API endpoint <https://www.digicert.com/services/v2>
- All required template parameters (like commonName, SANs, validity) must match your DigiCert product configuration