# CertCentral Immediate Certificate Issuance Guide

## Reducing the Number of API Calls

# Table of Contents

# Certificates Issued Immediately

When using the API to order certificates, too often time is spent just waiting for the certificate to be issued. What if, with a little preparation, you could get your certificates issued immediately? What if this included a way to reduce the API calls from 3 to 1?

In CertCentral, the immediate certificate issuance feature allows certificates to be issued immediately if the following certificate request prerequisites are met:

- The domain(s) on the order is preapproved.
- The organization associated with the domain is preapproved.
- The Auto Approve Request feature is configured for your account. See How to Configure the Auto Approve Request Feature.
- The requestor has permissions to approve certificate requests.

If all of these prerequisites are met, we return your submit request call with an issued certificate. It's that easy. If any of the prerequisites are missing, immediate certificate issuance cannot happen. For example, if the domain was not preapproved, the request cannot be issued until our Validation team has validated your domain control. Also, if the requestor doesn't have approval permissions, an admin or manager must approve the request before we can issue the certificate.

## Submit Order Endpoints

When configuring the API Submitting Order's endpoints, setting up each endpoint remains the same (Request Endpoint, JSON Request Parameters, etc.). What will change are the responses you may receive. Instead of one possible response, you can now receive two different types of responses: An i**mmediate certificate issuance** response, requiring only a single call, and a **request status** response, with the status of the request, requiring three calls before it can be issued (no immediate certificate issuance).

## Example: Configuring the Order Standard SSL Certificate Endpoint

### Request Endpoint

| Method | URL |
|---|---|
| **POST** | https://www.digicert.com/services/v2/order/certificate/ssl_plus |

### Request Body

The request for body for this endpoint must be in one of the following formats:

1. application/json
2. application/xml

**Immediate Certificate Issuance Note:** You must configure the auto-approve request feature in your CertCentral account before the request can skip the certificate approval process, and the certificate can be returned in the response body.

## JSON Request Parameters

| Parameter Name | Req/Opt | Allowed Values | Default | Description |
|---|---|---|---|---|
| **Certificate** | **Required** | **[object]** | | |
| common_name | Required | [string] | | The name to be secured in the certificate |
| csr | Required | [string] | | Certificate Signing Request. To create a CSR from you server, visit the DigiCert website (https//www.digicert.com/csr.creation.htm). |
| organization_units | Optional | [array] | [blank] | The OU field for the certificate. |
| server_platform | Optional | Reference: Server Platforms | -1 | The server platform type defaults to *other*. |
| Id | Required | [int] | | The id of the server platform |
| signature_hash | Required | sha256, sha384, sha512 (sha1 accepted on private certs) | | The certificate's signing algorithm hash.<br>**For Code Signing certificates** only sha256 is supported. |

| Parameter Name | Req/Opt | Allowed Values | Default | Description |
|---|---|---|---|---|
| **organization** | **Required** | **[object]** | | |
| id | Required | [int] | | The organization's identifier |
| validity_years | Required | [int] | | Number of years that the certificate is valid. |
| Custom_expiration_date | Optional | [date] | | A custom expiration date that overrides the standard validity period. Date must be formatted in format YY-MM-DD. |
| Comments | Optional | [string] | [string] | Comments about this request that the approver will see. |
| Disable_renewal_notifications | Optional | [bool] | false | If this is true, then no renewal notifications will be sent for the certificate. |
| Renewal_of_order_id | Optional | [int] | | If this order is a renewal of a previous order, add the previous order's id to this parameter |
| payment_method | Optional | balance, card, profile | balance | How to pay for the certificate.<br>If there is a default payment profile, it will default to "profile", otherwise it will default to "balance". |

## JSON Response Parameters

You can receive two types of responses: Immediate Certificate Issuance and Request Status.

### Immediate Certificate Issuance Response Parameters

When all prerequisites are met (domains pre-validated, auto approval configured, etc.), we send back the parameters in the response body.

| Parameter Name | Data Type | Description |
|---|---|---|
| id | [int] | The order's identifier |
| requests | [array] | |
| id | [int] | |
| status | [string] | approved |
| **certificate_chain** | [array] | SSL, intermediate, and root certificates |
| subject_common_name | [string] | The name to be secured in the SSL certificate |
| pem | [string] | The SSL certificate in pem format |
| subject_common_name | [string] | The name of the DigiCert intermediate certificate |
| pem | [string] | The intermediate certificate in pem format |
| subject_common_name | [string] | The name of the DigiCert root certificate |
| pem | [string] | The root certificate in pem format |

### Request Status Response Parameters

If any of the prerequisites are missing (requestor does not have approval permissions, auto approval not configured, etc.), we send back these in the response body.

| Parameter Name | Data Type | Description |
|---|---|---|
| id | [int] | The order's identifier |

| | | |
|---|---|---|
| requests | [array] | |
| id | [int] | |
| status | [string] | Statuses: pending, approved, rejected |

# Sample Request

## Endpoint

https://www.digicert.com/services/v2/order/certificate/ssl_plus

## Headers

X-DC-DEVKEY: Your-API-Key-Generated-In-Your-Account
Content-Type: application/json

## Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "example.com",
    "csr": "------ [CSR HERE] ------",
    "organization_units": [
      "Developer Operations"
    ],
    "server_platform": {
      "id": 45
    },
    "signature_hash": "sha256"
  },
  "organization": {
    "id": 1234567
  },
  "validity_years": 2,
  "comments": "Comments for the approver",
  "disable_renewal_notifications": false,
  "payment_method": "balance"
}
```

# Sample Response

**Status Code: 201**

## Headers

Content-Type: application/json

## Body

You can receive two types of responses: Immediate Certificate Issuance and Request Status.

## Immediate Certificate Issuance Sample Response

In this response, because the request was automatically approved and all prerequisites were met, we send the request id, status (approved), the certificate_id, and certificate_chain back in the response body.

**JSON (application/json)**


```
{
    "id": 1234567,
    "requests": [
        {
            "id": 1234567,
            "status": "approved"
        }
    ],
    "certificate_id": 1234567,
    "certificate_chain": [
        {
            "subject_common_name": "example.com",
            "pem": "------ [PEM HERE] ------"
        },
        {
            "subject_common_name": "DigiCert SHA2 Secure Server CA",
            "pem": "------ [PEM HERE] ------"
        },
        {
            "subject_common_name": "DigiCert Global Root CA",
            "pem": "------ [PEM HERE] ------"
        }
    ]
}
```

## Request Status Sample Response

In this response, because the request is now waiting for an approval, we only send the request id and status (pending) back in the response body.

**JSON (application/json)**

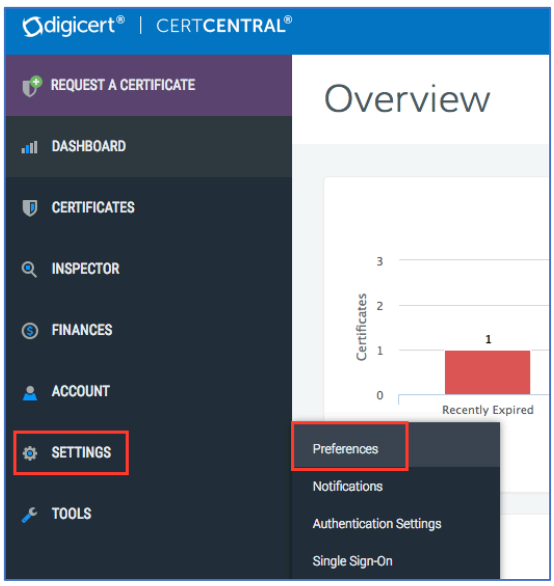
```
{
  "id": 1234567,
  "requests": [
    {
      "id": 1234567,
      "status": "pending"
    }
  ]
}
```

# How to Configure the Auto Approve Request Feature

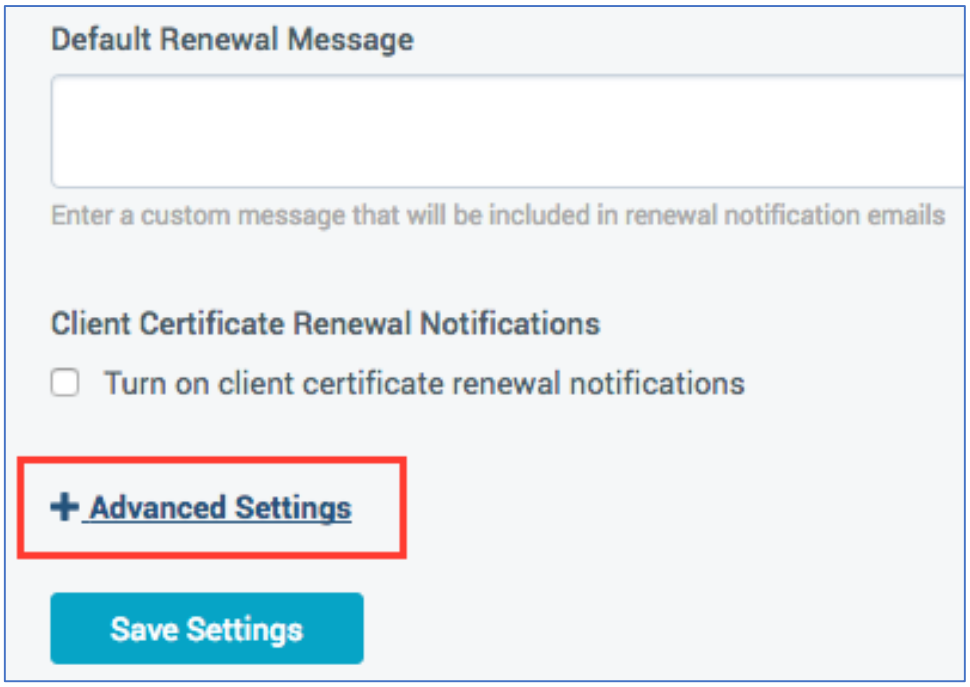
By default, your CertCentral account is configured for one-step certificate request approvals; however, you can set up automatic certificate request approvals for anyone who can approve certificate requests.

This feature only works for Administrators and Managers. By default, all admins and managers can approve SSL certificate requests; however, they can only approve EV SSL certificate requests if you have designated them as EV approvers.

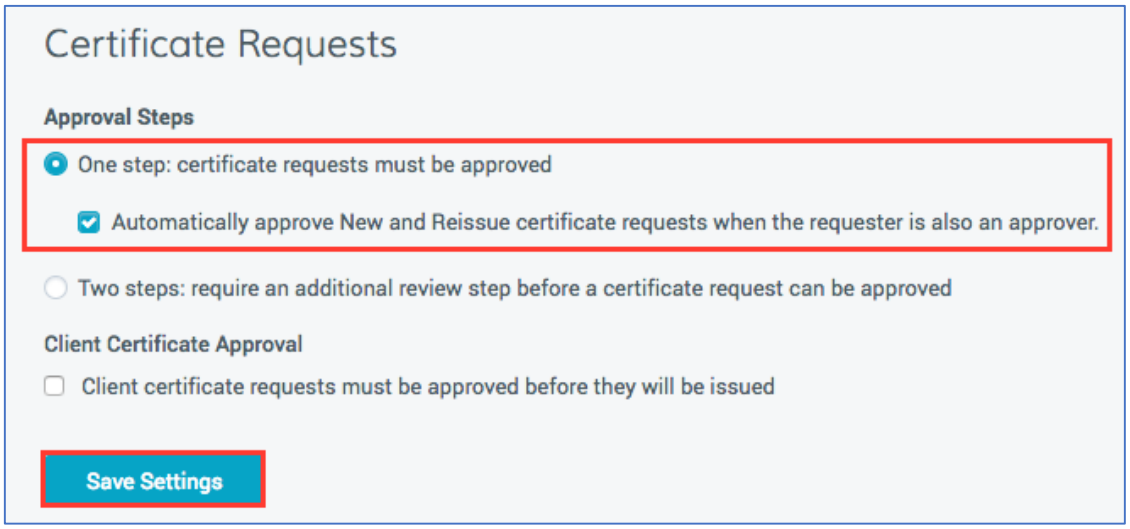
1. In your account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, scroll down and click **+ Advanced Settings**.




3. In the **Certificate Request** section, under **Approval Steps**, select **One step: certificate requests must be approved**.




4. Next, check **Automatically approve certificate requests when the requester is also an approver**.
5. When you are finished, click **Save Settings**.