
Sectigo Certificate Manager

EV Anchors

Contents

Sectigo Certificate Manager (SCM) and EV Anchors.....	2
What is an EV Anchor?	2
Important to Know about EV anchor	2
Request EV Anchor	4
Approve the EV Anchor Request.....	8
Cancel an EV Anchor Request	10
Validation Process	12
Legal Existence	12
DBA (tradenname).....	12
Physical Existence	12
Operational Existence.....	13
Domain Control	13
Verify Agreement	13
Replace EV Anchor.....	14
Revoked an EV Anchor.....	16

Sectigo Certificate Manager (SCM) and EV Anchors

The following topics are explained in this guide:

- What is an EV Anchor?
- Important to know about EV anchor
- Request EV Anchor
- Submit EV Order
- Validation Process
- Revoke EV Anchor

What is an EV Anchor?

EV anchor is a Sectigo Certificate Manager (SCM) certificate type with pre-validated organization details and domain which can be used to auto issue subsequent EV certificate order requests. Subsequent EV orders must match the EV anchor exactly to be auto issued.

The EV anchor is validated using the applicant details:

- Organization details (name and address)
- Incorporating or registration details
- Contract signer
- Top-level domain

All of an organization's EV anchor details are stored in a different location called the Order Management System. SCM administrators do not have access to the Order Management System. But some of the EV anchor applicant details are stored in the EV details.

Important to Know about EV anchor

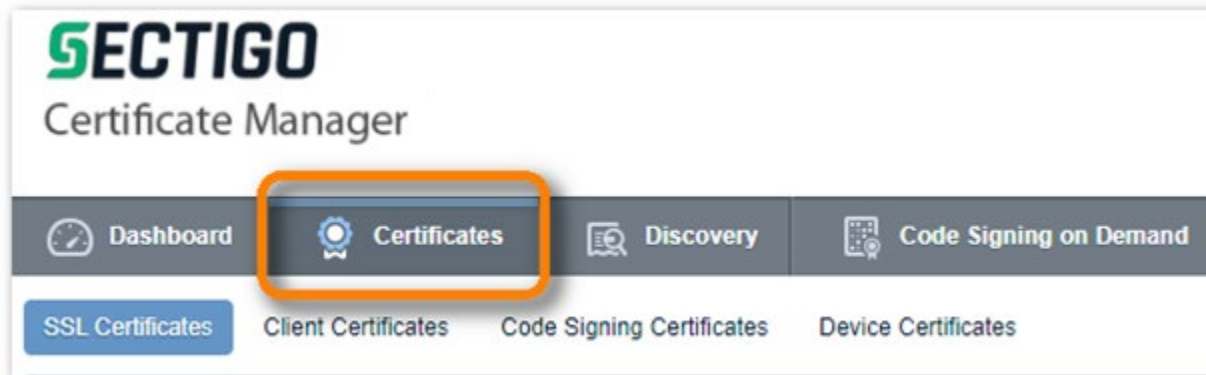
- How an EV anchor is setup and used in SCM is different from an OV anchor. OV anchors store and use the validated information in the organization general details in SCM. The validated applicant details for the EV anchor are stored in the anchor certificate template located outside of SCM. But the EV anchor usually matches the general and EV details listed in SCM
- There should only be one EV anchor for an organization. Multiple EV anchors can cause problems and should be avoided
- EV anchor is only a template and cannot be installed on a web server as a valid EV certificate
- After an EV anchor is validated. Subsequent EV orders must match the details on the anchor exactly to be auto issued. Including spaces, abbreviations, and upper/lower case.

- An EV anchor is valid for 13 months. A new EV anchor will have to be requested and validated
- The EV details should not be changed. If the details need to be changed, a new validated EV anchor is required to auto issue EV certificate orders. Please contact support and validation for assistance

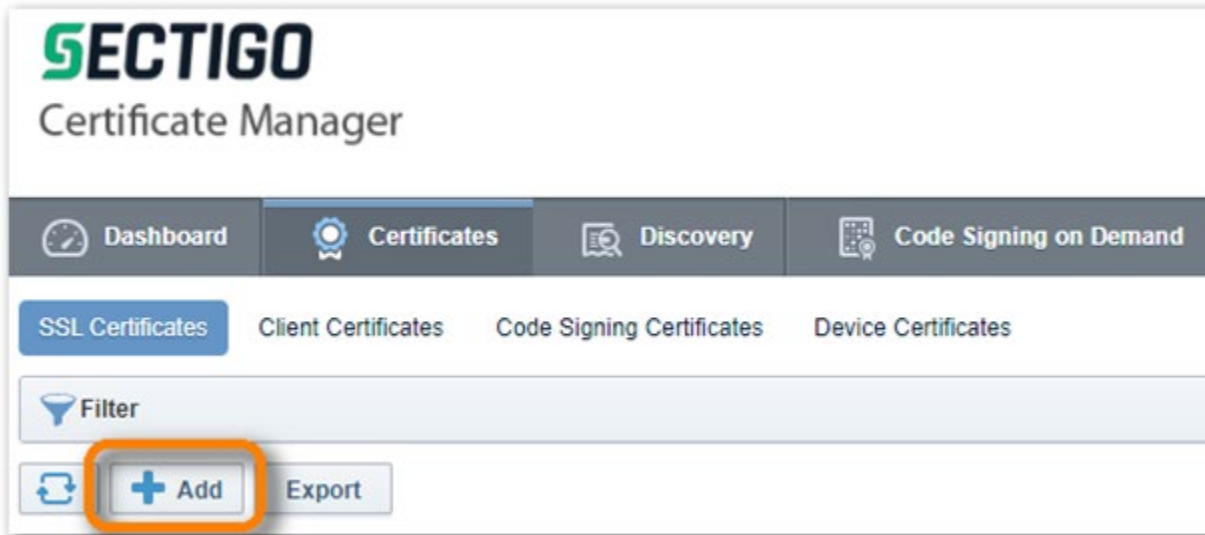
Request EV Anchor

EV anchor be requested prior to adding an EV certificate to the organization. The EV anchor request is a similar validation process as an EV certificate. But the EV anchor can be used to auto issue future EV certificate order request if the details match the EV anchor.

1. Login to SCM Dashboard
2. Navigate to the Certificates tab

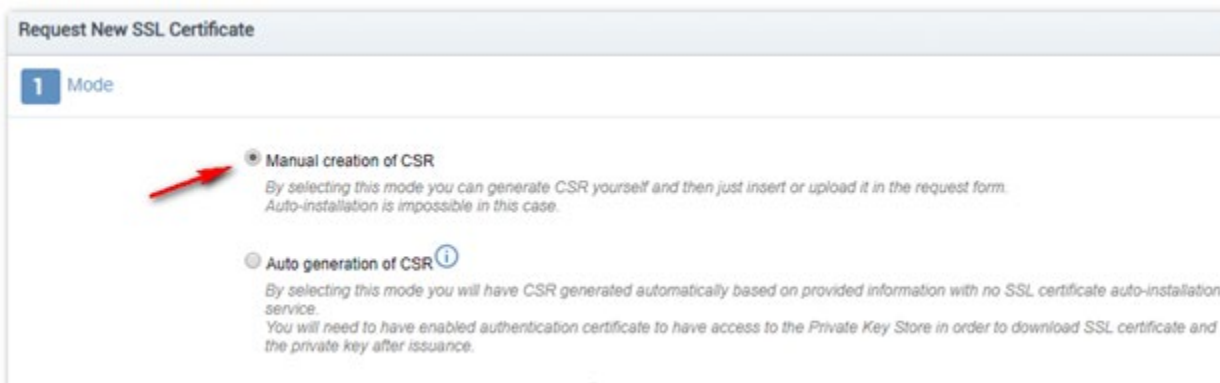


3. Click the Add button to add a new certificate request



4. Select Option "Manual Creation of CSR" and click NEXT to upload or Copy and Paste your CSR.

Note: if you need assistance creating a CSR, refer to the Knowledge Base https://support.sectigo.com/Com_KnowledgeSearchPage:



5. Proceed to the step 3, Basic info
 - a. Choose the Organization
 - b. Choose the certificate Type –EV Anchor Certificate*
 - c. Choose Term Length 1 Year
 - d. Enter the Common Name
 - e. Enter additional Subject Alternative Name in the SAN list. Enter all domains needed for the EV Anchor to secure. Use a comma to separate each domain
 - f. Server Software is not used for EV anchors. Any selection can be used. The EV anchor is only a template and not a certificate.

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Auto renew

Organization* Refresh

Department*

Certificate Type* i

Certificate Term*

Common Name* Get from CSR

Subject Alternative Names
(optional, comma separated)

Server Software*

Requester

External Requester i

[Click here for advanced options](#)

Note: If the certificate type EV Anchor is not available, please contact tech support for assistance

Please DO NOT include sub-domains in this certificate unless you are only authorized to order EV certificates for a sub-domain. The industry regulatory requirements for EV Enterprise RA allow unfettered issuance only of certificates at 3rd and higher domain levels from a fully validated, active EV anchor.

Including example.com will allow you to obtain EV certs for sub1.example.com, sub2.example.com or sub1.sub2.sub3.example.com, BUT including www.example.com will only allow sub1.www.example.com, etc. Do not include any wildcards, only root domains.

6. The auto-renewal step is optional and can be edited in the certificate details later.

The screenshot shows the 'Request New SSL Certificate' form at step 4, 'Auto renew'. The progress bar at the top indicates the following steps: 1 Mode, 2 CSR, 3 Basic info, 4 Auto renew (current step), and 5 EULA. Below the progress bar, a text box states: 'Here you can set auto-renewal of this certificate in advance of its expiration. These settings can be edited in the certificate details later on.' Below this text box, there is a checkbox labeled 'Enable auto renewal of this certificate' which is currently unchecked. To the right of the checkbox is a text input field labeled 'Number of days before expiration to start auto renewal' with the value '30' entered.

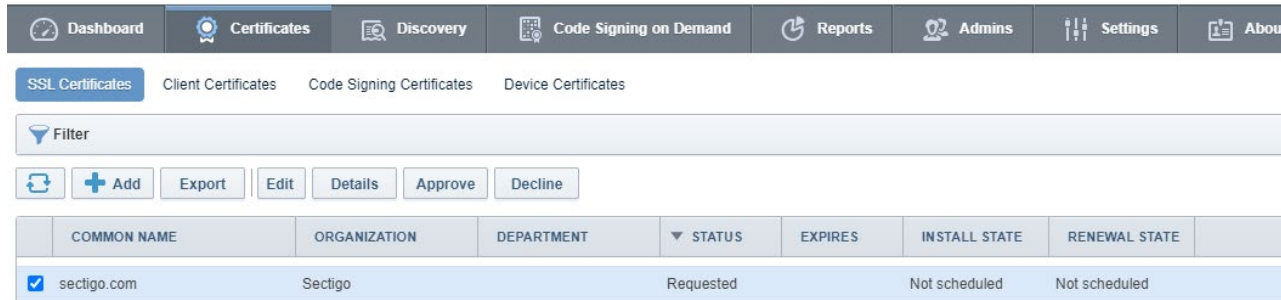
7. Proceed to Subscriber and Certification agreement and select the **I agree** checkbox.

The screenshot shows the 'Request New SSL Certificate' form at step 5, 'EULA'. The progress bar at the top indicates the following steps: 1 Mode, 2 CSR, 3 Basic info, 4 Auto renew, and 5 EULA (current step). Below the progress bar, there is a 'Certification' section with a scrollable text area containing the 'Comodo ePKI Certificate Manager Agreement'. Below the text area is a 'Print' button and a checkbox labeled 'I agree'. A red arrow points to the 'I agree' checkbox. Below the checkbox, there is a small text note: 'I agree.' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

8. The request for an EV anchor is complete. The request must be approved.

Approve the EV Anchor Request

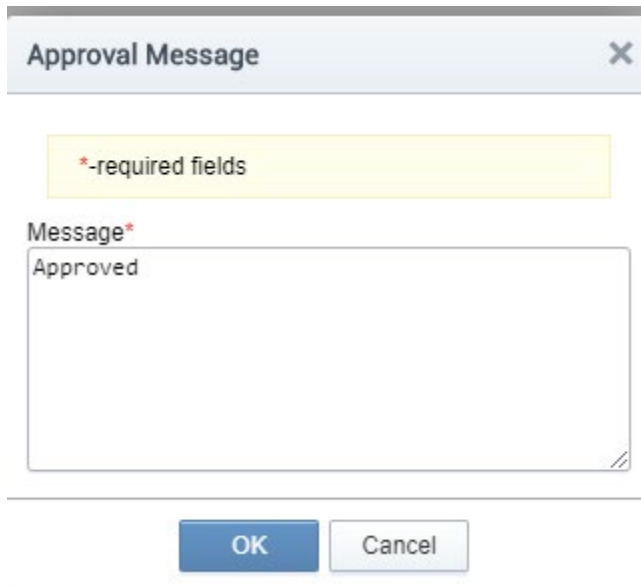
1. Once the request is submitted, another MRAO administrator approves the request



The screenshot shows a web interface for managing certificates. At the top, there is a navigation bar with tabs for Dashboard, Certificates, Discovery, Code Signing on Demand, Reports, Admins, Settings, and About. Below this, there are sub-tabs for SSL Certificates, Client Certificates, Code Signing Certificates, and Device Certificates. A 'Filter' dropdown is present. Below the filter, there are buttons for Refresh, Add, Export, Edit, Details, Approve, and Decline. A table displays a list of certificates with columns for Common Name, Organization, Department, Status, Expires, Install State, and Renewal State. One entry is visible for 'sectigo.com' with a status of 'Requested'.

COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input checked="" type="checkbox"/> sectigo.com	Sectigo		Requested		Not scheduled	Not scheduled

2. Approve the request.



The screenshot shows a dialog box titled 'Approval Message' with a close button (X). Below the title bar, there is a yellow box containing the text '*-required fields'. Underneath, the label 'Message*' is followed by a text area containing the word 'Approved'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

3. After the request is approved, an order number is generated, and the request is sent to be validated.

Information ✕

i Please expect an email from our Validation team that details the EV validation process.

OK

4. Review the EV anchor details by clicking on Details

SSL Certificate: sectigo.com

Certificate has not enrolled yet

CERTIFICATE DETAILS

Common Name	sectigo.com
Status	Applied
Order Number	354492099
Vendor	N/A
Discovery Status	Not deployed
Self-Enrollment Certificate ID	1811065
Type	EV Anchor Certificate
Server Software	Apache/ModSSL
Server Software State	
Term	395 days
Owner	Rebecca Sandiford
Requested by	Rebecca Sandiford
External Requester	
Requested	05/28/2020

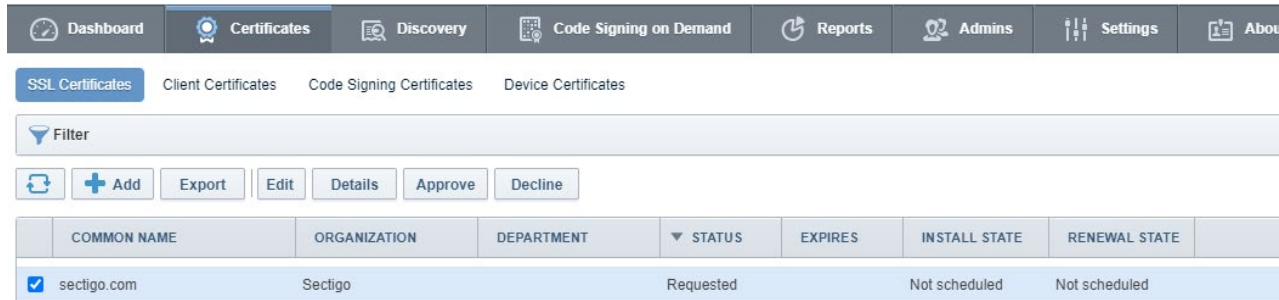
EV DETAILS

Note: The details display the order number that can be used when communicating with the Support and Validation teams.

Cancel an EV Anchor Request

An EV anchor request can be cancelled or declined. Declining the request will not generate an order for validation

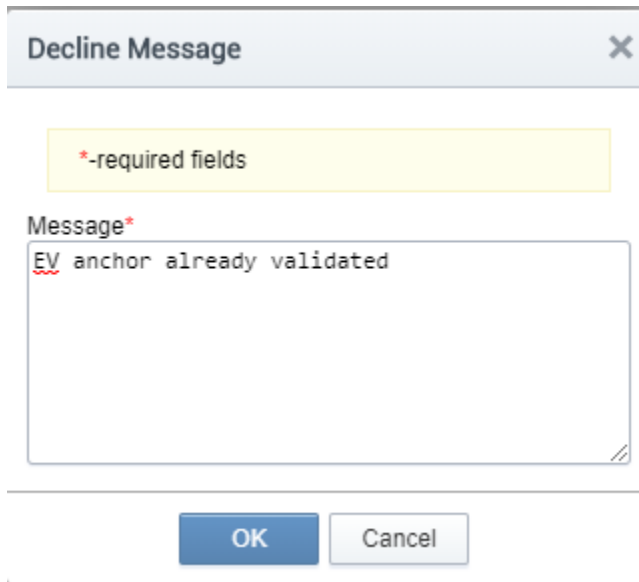
1. Once the request is submitted, another MRAO administrator decline the request



The screenshot shows a web interface for managing certificates. The top navigation bar includes Dashboard, Certificates, Discovery, Code Signing on Demand, Reports, Admins, Settings, and About. Below the navigation, there are tabs for SSL Certificates, Client Certificates, Code Signing Certificates, and Device Certificates. A filter bar is present, followed by action buttons: Add, Export, Edit, Details, Approve, and Decline. A table displays a list of requests with columns for Common Name, Organization, Department, Status, Expires, Install State, and Renewal State. One request for 'sectigo.com' is highlighted, with a status of 'Requested' and 'Not scheduled' for both install and renewal.

COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
sectigo.com	Sectigo		Requested		Not scheduled	Not scheduled

2. Approve the request.



The screenshot shows a 'Decline Message' dialog box with a close button (X). A yellow box indicates that asterisks (*) denote required fields. The 'Message*' field contains the text 'EV anchor already validated'. At the bottom, there are 'OK' and 'Cancel' buttons.

Decline Message X

*-required fields

Message*

EV anchor already validated

OK Cancel

3. After the request is declined, the status updated to declined. No order is generated and no validation occurs.

<input type="checkbox"/>	sectigo.com	Sectigo	Declined	Not scheduled	Not scheduled
--------------------------	-------------	---------	----------	---------------	---------------

4. Review the EV anchor details by clicking on Details. The status is declined and there is no order number for support and validation teams

CERTIFICATE DETAILS

Common Name sectigo.com

Status Declined

Order Number N/A

Vendor N/A

Discovery Status Not deployed

Self-Enrollment Certificate ID 1582294

Type EnterpriseSSL Pro

Server Software Microsoft IIS 5.x and later

Server Software State

Term 1 year

Validation Process

The Validation team conducts a manual process to verify:

- Legal existence
- DBA (trade name)
- Physical existence
- Operational existence
- Domain control
- Verify agreement signer's / requestor's authority, agency, and title

Legal Existence

Legal existence is processed to verify the organization legally exists and the legal name of the organization. The EV anchor organization name must be the legally registered name of the organization. The sources used are a government registering agency or other government source that are approved by industry regulatory guidelines as a qualified government information source.

DBA (tradenname)

A DBA or tradenname can be listed on an EV anchor, but it can not be used as the legal name. DBA is verified as a registered tradenname to be listed on the EV anchor.

The DBA and legal name appear on the anchor in this format. DBA (legalname) to conform to industry regulatory requirements.

Physical Existence

Physical existence is processed to verify the organization's address when business is conducted. The sources used are third-party reliable source that verified organization details or other government source that are approved by industry regulatory guidelines as a qualified independent information source.

Validation must check the street address, city, state/province/county and postal code fields are formatted correctly and adhere to ISO standards. During verification, the data fields may need to be changed to meet ISO standard and regulatory guidelines. Validation is required to make necessary changes to avoid a mis-issued EV anchor.

Note: ISO standards for address fields may not confirmed to popular local naming conventions but are necessary to avoid mis-issuing an EV anchor

Industry regulatory guidelines allow for certain combination of address fields to be blank. But the EV anchor must have a combination of address field to properly define the organization location.

For example, the state/province/county field can be blank if the street address, city and country are present. Or the street address can be blank if the city, state/province/county, and country are present. The specific combinations can be complex, but the validation team can assist during the EV anchor validation process if certain field do not have a proper ISO standard or if the EV anchor is to have only certain address fields.

Operational Existence

Operational existence is processed to verify the organization is conducting business operations. The sources used are third-party reliable source that verified organization details or other government source that are approved by industry regulatory guidelines as a qualified independent information source.

Domain Control

Domain control validates the organization has control over the domain that will be associated with the EV anchor.

Verify Agreement

Industry regulatory guidelines mandate that we verify the signer on the agreement and requestor of the certificate. This is usually done with a click-through online agreement and a verification phone call.

The step can be bypassed in some instances and the validation team will let you know if it verifying the agreement is not needed.

Replace EV Anchor

Replacement is the process used to add a domain to an EV anchor. It is not recommended that the original anchor is revoked, and a new request is made to a domain.

Replacing allow for a quick validation process without the need to revalidate. If any organization details change during a replacement, revalidation is required.

1. Select the domain

	COMMON NAME	ORGANIZATION	DEPARTMENT
<input checked="" type="checkbox"/>	su nl	SL	B.V.

2. Click on Replace

Replace existing SSL for domain 'surfnet.nl'

*-required fields

CSR*

Common Name*

Subject Alternative Names
(optional, comma separated)

Reason*

OK Cancel

3. Upload the CSR, complete all fields and click OK

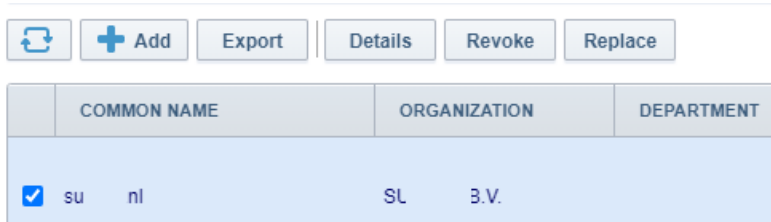
A replacement order is created, and validation begins on the new anchor.

Note: The EV anchor must be revoked after the replacement anchor is issued. Having 2 active EV anchors for a single organization can cause problem to auto issue subsequent EV certificate orders.

Revoked an EV Anchor

Revoking an EV Anchor

1. Select the domain



The screenshot shows a web interface with a table of EV anchors. Above the table are several buttons: a refresh icon, '+ Add', 'Export', 'Details', 'Revoke', and 'Replace'. The table has three columns: 'COMMON NAME', 'ORGANIZATION', and 'DEPARTMENT'. A single row is highlighted in light blue, with a checked checkbox in the first column. The values in this row are 'su nl' under 'COMMON NAME', 'SL' under 'ORGANIZATION', and 'B.V.' under 'DEPARTMENT'.

	COMMON NAME	ORGANIZATION	DEPARTMENT
<input checked="" type="checkbox"/>	su nl	SL	B.V.

2. Click on Revoke and follow the form to complete the revocation

Once revoked, the status updates to revoked.