Extended Validation (EV) and Anchor Certificates

InCommon Certificate Service 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 this wiki page for details.

The InCommon Certificate Service issues unlimited Extended Validation (EV) SSL/TLS certificates at no additional cost to subscribers. Because EV certificates require additional levels of validation for the requesting organization, our partner Comodo must handle all of the paperwork as well as the validation process for EV certificates.

InCommon and Comodo also offer Anchor Certificates, which pre-validates domains for future EV certificate requests. When you create an Anchor Certificate, you go through the same validation process as an EV certificate, with the anchor valid for approximately 13 months. The anchor is not an actual certificate, but when applied to all of your domains, you can request EV certificates with no further validation during the life of the anchor.

What are EV Certs?

An extended validation certificate is a X.509 public key infrastructure (PKI) digital certificate in which identifying information about the business entity holding the certificate for a web site or other server has been validated by the certificate authority (CA). The CA uses a standardized set of requirements that also set requirements for auditing, revocation and certificate content. Extended validation certificates are generally considered to be high assurance certificates as that term is used within the PKI community.

Why the additional paperwork?

EV certificates have higher validation requirements and are issued by Comodo under a separate Certification Authority (CA). Because of the formal requirements that all EV certificates must comply with, Comodo must manage the validation process with separate governing legal terms. For EV certificates, InCommon subscription covers the fees and the same Certificate management interface, while Comodo directly engages with the university on legal and validation terms.

First-time EV Cert Requests

1. Confirm Domain Approval - Confirm that the domain for which you are requesting the EV certificate has already been approved by InCommon.
2. Request an EV Cert via the Certificate Manager (CM)
3. Comodo CA requires the completion of two documents for EV Validation. The Subscriber agreement is accepted when the initial EV certificate is requested. The Certificate Request form is emailed to the requestor with instruction on how to click thru to complete the process.
    a. EV SSL Certificate Subscriber Agreement - The EV SSL Certificate Subscriber Agreement is separate from the InCommon Certificate Service Addendum. There is no additional charge for EV certificates, but this agreement with Comodo is required. This is required once per organization.
    b. EV SSL Certificate Request Form

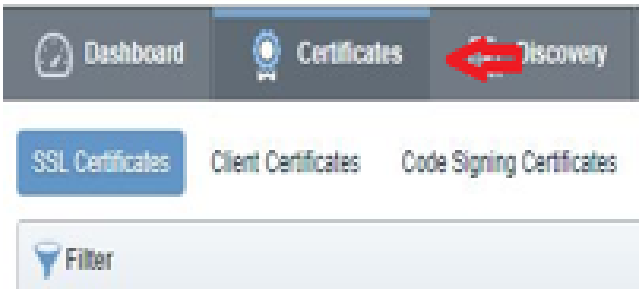
Be sure to list all domains for which you intend to request EV certificates in both the Legal Opinion and the EV Certificate Request Form. Listing the parent domain will cover all sub-domains. For example, listing foo.edu is sufficient to cover web1.foo.edu, web2.foo.edu, etc.

Requesting an EV Anchor

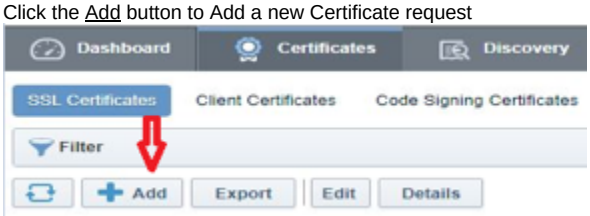
An anchor certificate will pre-validate domains for future EV certificate requests. All domains that require an EV certificate should be included in this request. If a domain is not listed in this request, you can still request an EV certificate; however, there the order will need to be processed manually by a validatior.

There is no prerequisite to create an EV anchor certificate yet we suggest every organization follow the following steps. Please note there is only one EV anchor certificate that can be applied to each organization (school). This procedure does not change current certificate ordering process - it is simply to help make EV processing more efficient. The EV Anchor is NOT an actual certificate that can be used.

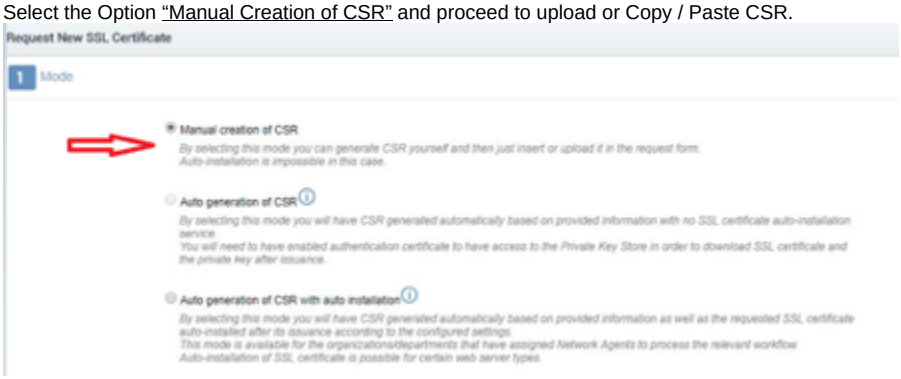
1. Login to CCM Dashboard
2. Navigate to the Certificates Tab



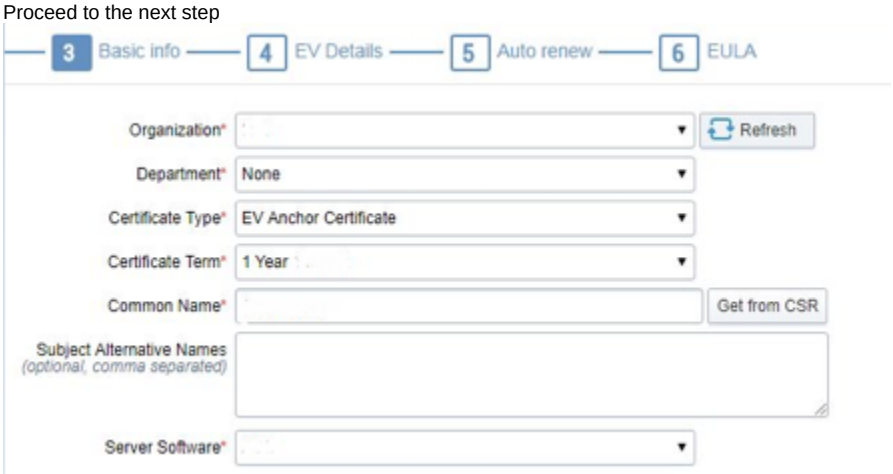
3. Click the Add button to Add a new Certificate request



4. Select the Option "Manual Creation of CSR" and proceed to upload or Copy / Paste CSR.



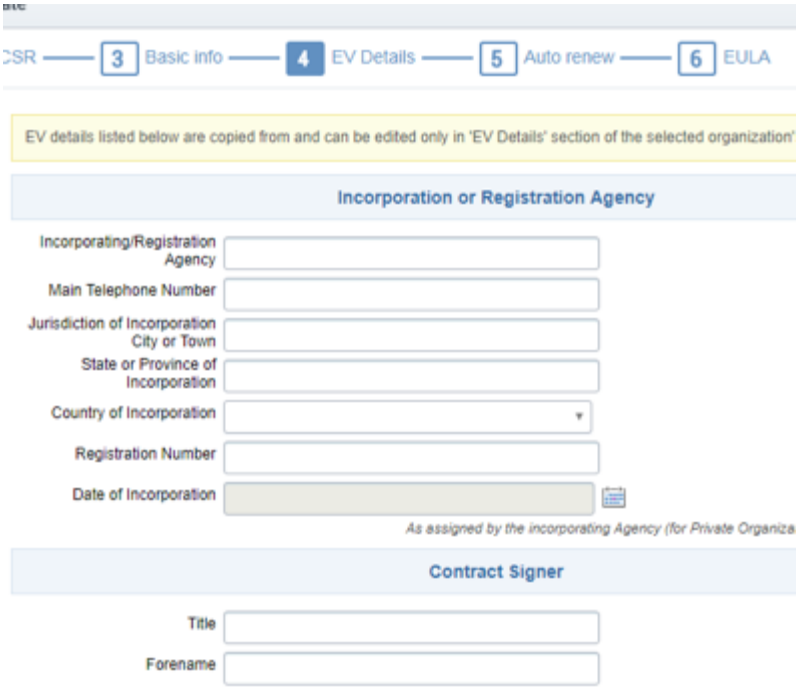
5. Proceed to the next step



- Choose the Organization
- Choose the certificate Type – EV Anchor Certificate
- Choose Term Length 1 Year
- Enter the Common Name (this can be any domain you need an EV cert for)
- In the SAN list enter all domains that you will need The EV Anchor to secure.
- Server Software does not matter in this case

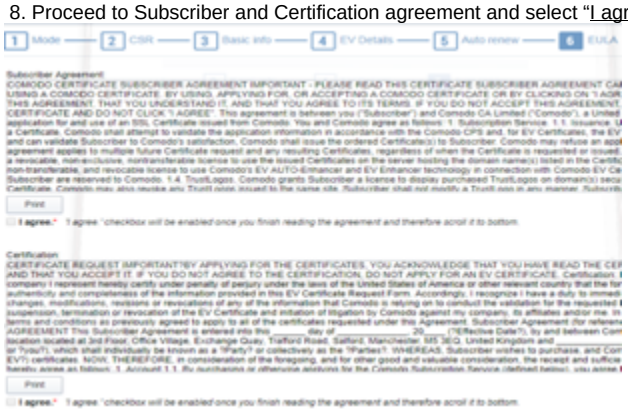
Note regarding domains: Please DO NOT include sub-domains in this certificate unless you are only authorized to order EV certificates for a particular sub-domain. The requirements for EV Enterprise RA laid out by the CA/B Forum allow unfettered issuance only of certificates at 3rd and higher domain levels from a fully validated, active EV SSL certificate. For example: 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. Continue to Enter your Incorporation, Registration Details and Contract signer Details



7. The option for auto-renewal is optional and can be edited in the certificate details later on.

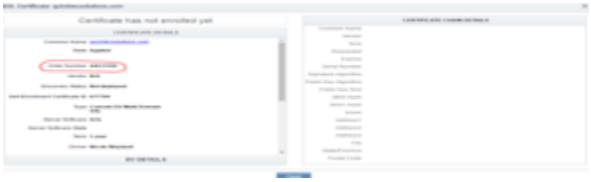
8. Proceed to Subscriber and Certification agreement and select "I agree" checkbox



*Once the request is submitted, you must have **another MRAO Admin** approve the request to finalize it. Once the request is approved, you will receive the order number.*

To find the order number in CCM Dashboard, go to Certificates > SSL Certificates > Filter option to locate the certificate applied for by the comm on name > select Details.

Under certificate details you will see the order number.



Submit a ticket to Comodo ccmvalidation@comodo.com and request an EV anchor certificate be set for your account and provide the order number. Please note the validation team may contact you with a request for additional information to verify ownership and company identity. Turnaround time for this request is dependent upon completion of this paperwork.

The EV anchor will be valid for approximately 13 months. DCV expiration notifications will be sent out for this certificate just like any other certificate from CCM. The certificate can be renewed in CCM or another certificate ordered. However, the validation team is to be contacted with the new order number (a renewal will generate a new order number) and request to make it an anchor certificate.

Please Note:

The primary organizational details will be set to match the details validated in the anchor cert order. IF those details are changed it will require a new anchor certificate to be created and then validated.

**The departments under the primary organization will NOT be allowed to have different details except for the Department Name. The street address, city, state, postal code, and country will become uneditable.*

For additional questions/concerns, please contact validation which can be reached Monday thru Friday 7 AM to 5 PM at 888-256-2608 Option #2. (Option #3 will bring you to technical support for CCM process/procedure questions).