Jisc Certificate Service

Quick-start guide – v1.4 (20/05/2022)

1. Introduction

Congratulations on your purchase of the new 2020 version of the Jisc Certificate Service.

This guide serves as a quick-start guide to using the Jisc Certificate Service (JCS) via the SECTIGO Certificate Manager (SCM). It outlines the major concepts and tasks achievable through SCM and gives some guidance specific to the Jisc version of SCM.

However, there is far more functionality in SCM than covered in this quick-start guide, including things like support for code-signing certificates, advanced access control, discovery of certificates on your network via an agent, advanced reporting, connecting to SCM and managing most aspects of SCM via APIs, and many more things.

You can view a much more complete administrators guide provided by SECTIGO at:
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000bvJA

An API guide is available at:
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000XDkE

If you need clarification on anything in this document, or the SECTIGO guide, please just contact Jisc who will be happy to assist.

1.1. Terms used in this document

JCS – Jisc Certificate Service

SCM – SECTIGO Certificate Manager

MRAO – Master Registration Authority Officers (i.e. Jisc staff administering the JCS).

RAO – Registration Authority Officers (i.e. top level administrators for members of the JCS).

DRAO – Department Registration Authority Officers (i.e. departmental administrators if a JCS member has chosen to divide their organisation up into departments).

2. Onboarding onto the service

When Jisc has completed processing your application to the JCS your two nominated RAOs will be set up on SCM.

Note: Sectigo will need to validate your organisation before you are able to issue certificates. You can find the current state of this process by logging into SCM, browsing to Organisations, and next to your organisation in the "Validation status" you will either see "Pending" or "Validated". This process usually takes hours but can take a few days.

However, even while your organisation is still "Pending", you can do many of the preliminary steps listed below in advance.

Your next steps:

1. Consider how best to configure your organisation and how you want your users to request and manage certificates – see Managing your organisation & departments.

2. Add and configure other RAO / DRAO users within your organisation – see Managing Users. Note: if using SAML to log into SCM, ensure your Identity Provider is configured appropriately – see IdP users - using your SAML Identity Provider to authenticate.

3. Ensure that for every domain you try to add, if you have CAA DNS records for those domains (which is recommended) they include SECTIGO, otherwise you will not be able to complete the DCV process:
   ```
   issue "sectigo.com" issuewild
   "sectigo.com"
   ```

   Note: the CAA records will need to be in place during DCV and during issuance of any certificates for those domains.

4. Add the domains you wish to issue certificates under for your organisation and then follow the DCV process to validate your control over them – see Managing Domains & DCV.

5. If you wish to issue EV certificates, set up an EV anchor containing the domains covered by EV validation – see Extended Validation (EV) Certificates.

6. If you wish to issue code signing certificates, please open a ticket with us as we need to enable your account to do so in SCM.

Get issuing certificates!

3. Overview of SCM

3.1. Logging into SCM

There are two types of users in SCM:

- **Standard** ○ Users with a username & password for SCM.

    ○ These users are created within SCM (or via the Sectigo APIs).

- **IdP users**

    ○ Users invited to create an account via their UK federation IdP.

    ○ These users are invited via SCM to create an account associated with their federated login. They do not have a local username/password.

- **Hybrid users**

    ○ To complicate matters, Standard users can later be associated with a federated login and become hybrid users – they have a local username/password but can also be authenticated to via their federated login.

3.1.1. Standard users – logging in via username/password

To login to SCM with a local account, browse to the SCM login page - found at **https://cert**https://cert-manager.com/customer/JISC**manager.com/customer/JISC** - enter your username and password and click Login.
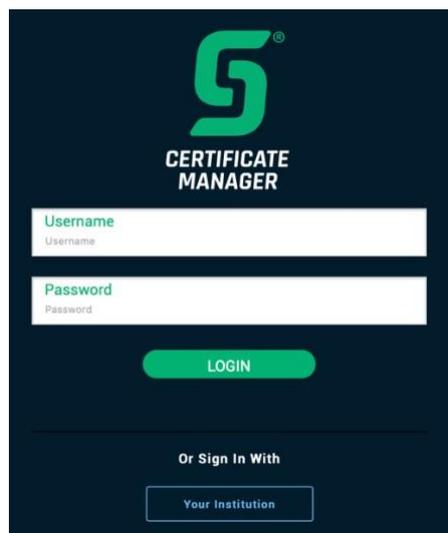
3.1.2. IdP users - using your SAML Identity Provider to authenticate

Configuring your Identity Provider

To enable login to SCM via your SAML Identity Provider, that Identity Provider needs to be registered on the UK federation, and configured to release the following attributes as follows:

- Release the following to the entity with entityID of **https://cert-manager.com/shibboleth**

- Mandatory attributes:

    ○ eduPersonPrincipalName - urn:oid:1.3.6.1.4.1.5923.1.1.1.6 - e.g.

    Joe.Bloggs@example.com ○   Mail -

    urn:oid:0.9.2342.19200300.100.1.3 - e.g. bloggs@example.com

- Optional Attributes:
  - ○ givenName - urn:oid:2.5.4.42 – e.g. Joe ○ sn - urn:oid:2.5.4.4 – e.g.

    Bloggs

To check if your IdP is configured correctly, browse to **https://cert-manager.com/customer/JISC/ssocheck/** where you will see a list of all attributes and the values received by SCM. If either "eppn" or "mail" show as "n/a" then your IdP is not releasing those attributes and needs to be configured to do so.

Logging into SCM

To login to SCM via your SAML Identity Provider, browse to the SCM login page – found at **https://cert**https://cert-manager.com/customer/JISC**manager.com/customer/JISC** - and click on the "Your Institution" link underneath the local username/password login area.

On the following page, choose your home organisation. If you've previously chosen, it should be remembered in your recent institutions list. Log in at your Identity Provider, and you should be sent back to SCM.

Note: if you wish to bookmark a link that skips this step, craft a URL with the following content: `https://cert-`

`manager.com/Shibboleth.sso/geant?target=https://cert-manager.com/customer/JISC/idp&entityID=XXX`

Where XXX should be the URL-encoded version of the entityID of your UK federation registered Identity Provider.
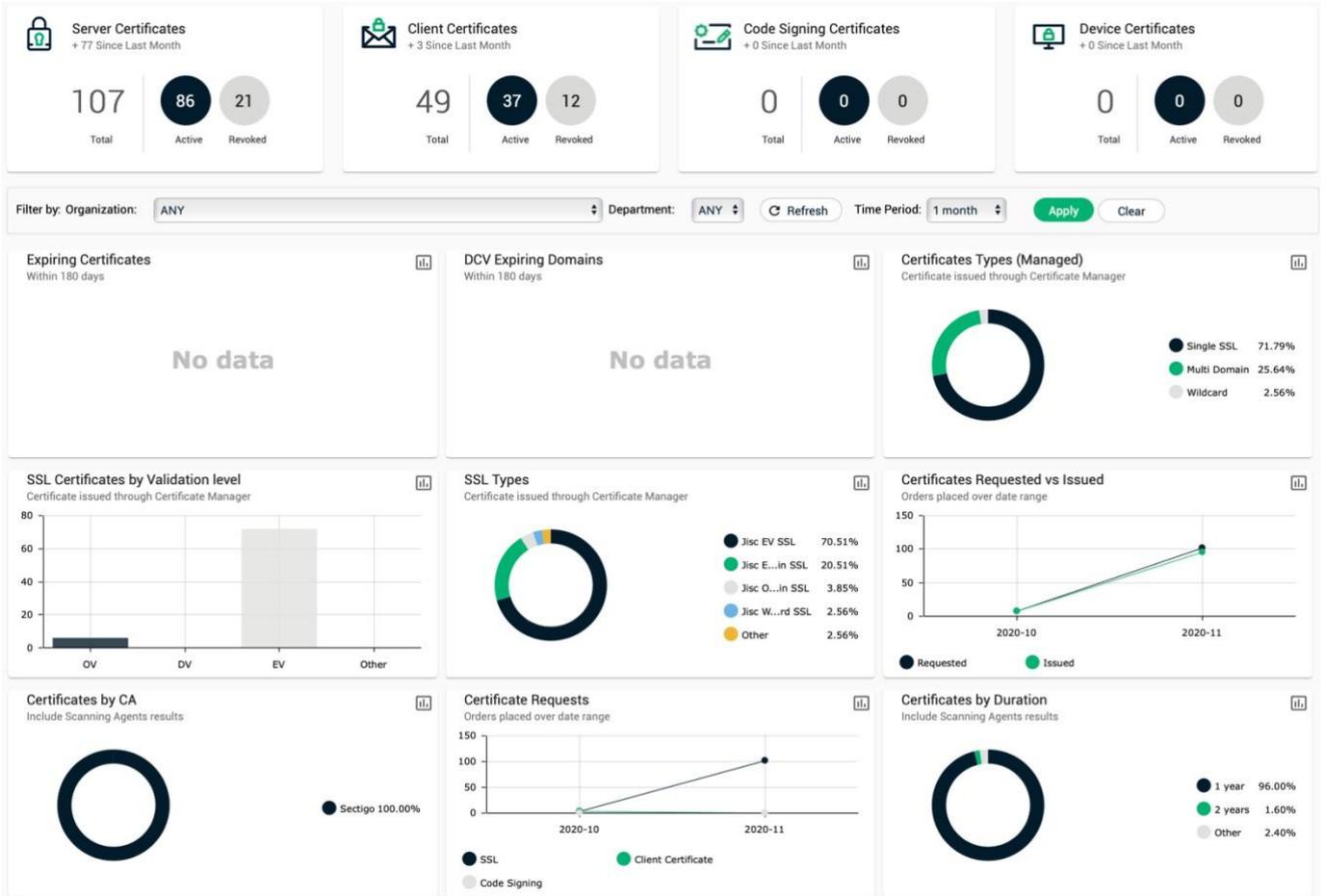
3.1.3. Adding a federated login to a standard user

If you have a local user account and wish to add a federated login option to it so you can gain the benefits of SSO, do the following:

1. Ensure your IdP is configured appropriately (see the "Configuring your Identity Provider" in the previous subsection).

2. Another RAO user should log into SCM (you can't do this to your own account).

3. They should find your account in the Settings -> Admins section, select it, and click the "Send IdP invitation" button.

4. SCM will email the email address configured on their local account with a link to click on. That link will get them to log in via their chosen IdP, and associate the eduPersonPrincipalName of their account with the local account.

5. You can now log in via username/password **or** via a federated login.

   Note: After following the link and associating your local account with a federated login, the first time you login again using a local username/password, you will be required to reset it to a new password.

3.2. Your Dashboard

In SCM, the first link is to your dashboard. This will give you a quick view of the basic statistics of (almost) all of the certificates issued by your organisation(s), along with important things like upcoming expiring certificates and DCVs.

Server Certificates
+ 77 Since Last Month

107 | 86 | 21
Total | Active | Revoked

Client Certificates
+ 3 Since Last Month

49 | 37 | 12
Total | Active | Revoked

Code Signing Certificates
+ 0 Since Last Month

0 | 0 | 0
Total | Active | Revoked

Device Certificates
+ 0 Since Last Month

0 | 0 | 0
Total | Active | Revoked

Filter by: Organization: ANY   Department: ANY   C Refresh   Time Period: 1 month   Apply   Clear

Expiring Certificates
Within 180 days

No data

DCV Expiring Domains
Within 180 days

No data

Certificates Types (Managed)
Certificate issued through Certificate Manager

- Single SSL   71.79%
- Multi Domain   25.64%
- Wildcard   2.56%

SSL Certificates by Validation level
Certificate issued through Certificate Manager

80
60
40
20
0
OV   DV   EV   Other

SSL Types
Certificate issued through Certificate Manager

- Jisc EV SSL   70.51%
- Jisc E...in SSL 20.51%
- Jisc O...in SSL   3.85%
- Jisc W...rd SSL   2.56%
- Other   2.56%

Certificates Requested vs Issued
Orders placed over date range

150
100
50
0
2020-10   2020-11

- Requested   - Issued

Certificates by CA
Include Scanning Agents results

- Sectigo 100.00%

Certificate Requests
Orders placed over date range

150
100
50
0
2020-10   2020-11

- SSL   - Client Certificate
- Code Signing

Certificates by Duration
Include Scanning Agents results

- 1 year   96.00%
- 2 years   1.60%
- Other   2.40%

4. Managing Users

Your organisation should have at least two RAO users defined and actively using the service – certain operations, if triggered by one user, need to be approved by a different user.

Your institution is responsible for ensuring that access to accounts is well-managed and that access to accounts is revoked when users change role or leave the organisation.

All user management tasks are done by logging into SCM and browsing to Settings -> Admins.
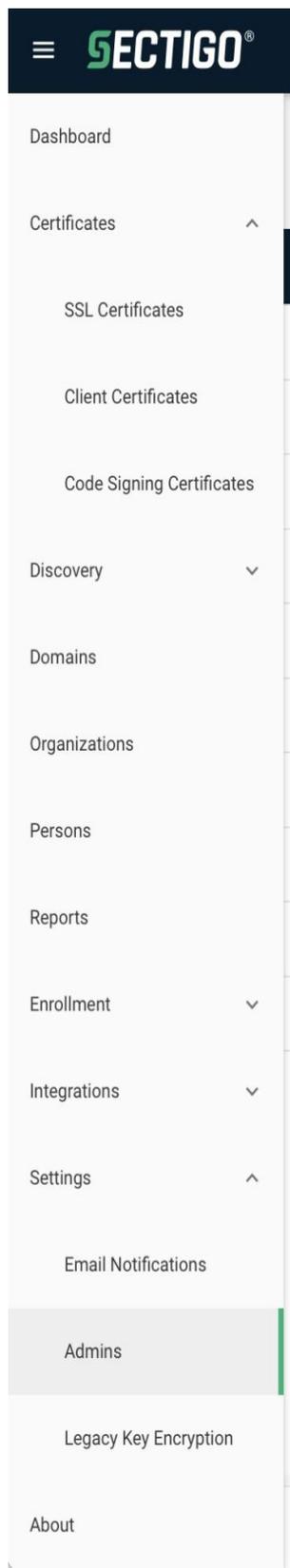
4.1. Adding a new user

Adding a new user consists of two main steps: creating the new user, and (for IdP users) approving that new user.

4.1.1. Creating a user

1. If your organisation has a SAML IdP registered on the UK Access Management Federation, click on the "Add IdP User" button (top right), otherwise choose the green + icon (top right) to add a local user. A dialogue will appear.

2. You will need to fill out the email address of the user you wish to invite. If adding a local user, you'll also need to fill out some details such as the user's name. Then hit Next.

3. Choose the relevant role(s) for the user. You can give the user the rights to manage SSL certificates, client certificates, and/or code signing certificates, for whichever organisation(s) you have RAO/DRAO rights, and you can give the user top level or departmental administrative rights:

    a. Choose:

        i. *RAO admin* if you want the user to administer your organisation at the top level; or

        ii. *DRAO admin* if you want the user to administer a particular department that you've set up within your organisation.

4. Next, you need to set what privileges the user will have. If an option is greyed out, you do not have the privileges to in turn set those privileges for other users.

    a. *Allow SSL Details Changing*: will allow the user to change certain details of SSL Certificates.

    b. *Allow SSL auto approve:* will enable some certificate types to be automatically approved.

    c. ***NOTE: If you need the user you're creating to have privileges which are currently unavailable to you (i.e. greyed out), please follow the rest of this guide to create the user, and contact Jisc to make those change on your behalf (make sure you provide us the created user's details)!***

5. For local users, you will need to set an initial password (click the "authentication" tab).

6. Click on Save.

    a. For local users – you now need to share the username/password with that user, and no further actions are required. On first login the user will be required to change it.

    b. For IdP users - ***nothing will now happen until the approval step is completed!***

4.1.2. Approving an IdP user

1. *A different RAO/DRAO admin* for your organisation will need to log into SCM and find the user you added. IdP users awaiting approval will appear in italics and highlighted in red.
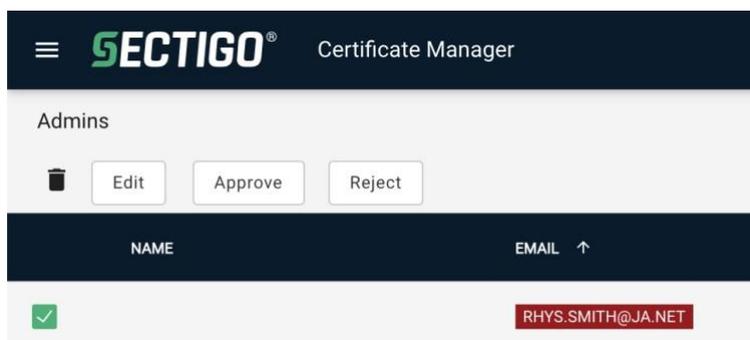
2. The other RAO admin will then need to select that user and hit the approve button.

3. The new user will now be emailed a link to follow to onboard themselves onto the service.

5. Managing your organisation & departments

There are multiple ways you can deploy the certificate service across your organisation:

1. You can split your organisation up into departments to allow for delegated management of all aspects of SCM.

    o Users can be configured as RAOs (for the organisation) or DRAOs (for departments within).

    o Pretty much all things that can be configured at the organisational level (e.g. the methods of issuing certificates detailed in Methods of issuing certificates) can also be configured at a departmental level.

    o Users within each department can then be responsible for issuing and approving certificates with the top-level RAOs only being involved for shared domains, etc.

2. You can allow your organisation's users to use self-enrolment so they can request certificates without having to have RAO/DRAO SCM accounts.

    o RAO/DRAO users would be responsible for domain management, the DCV process, and approving requests.

5.1. Delegated management by using departments

5.1.1. Managing departments

To split up an organisation into multiple departments:

1. Log in to SCM

2. Browse to Organisations, select your organisation and click the Departments button.
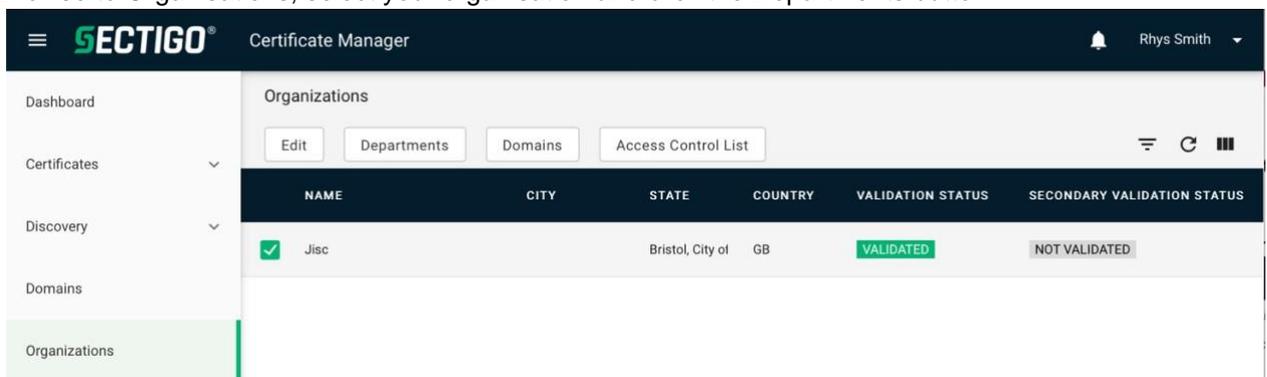
3. In the dialogue that pops up, you can add/edit/delete departments within your organisation.

5.1.2. Managing users in departments

Follow the guide in Adding a new user. When selecting the role(s) for the users, you can choose whether they are an RAO for your organisation, or DRAO for one of the departments within your organisation.

Jisc Certificate Service 🡒 Managing your organisation & departments

6. Managing Domains & DCV

To be able to issue certificates under a given domain, that domain needs to be added, appropriately delegated, and then control of that domain demonstrated (through the DCV process).

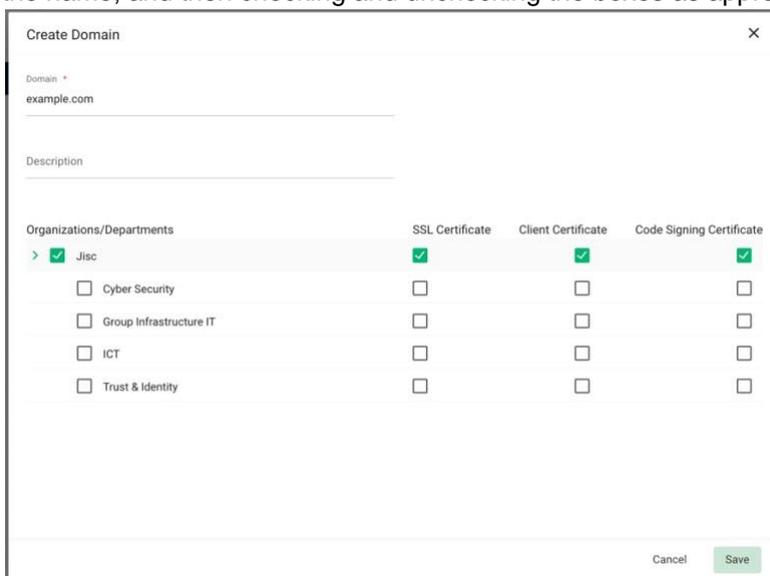All domain management steps outlined above are managed by logging into SCM and browsing to Domains.

Note: when viewing domains, all domains in the ac.uk namespace show under an ac.uk container, click on it and that section will expand and your .ac.uk domains will be listed there. All domains under other apex domains will just list in alphabetical order.
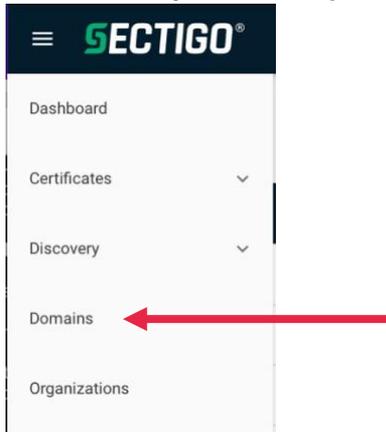
6.1.1. Adding a Domain

To add a domain:

1. Click on the Add button (the green + button in the top right).

2. Enter the domain you wish to add (e.g. *example.com)* and an optional description*.*

3. Choose which organisation the domain should be added to (you will probably only see one, unless you're an RAO for multiple organisations), and which certificate types can be issued under that domain.

4. You can also allow or deny specific departments within your organisation the use of that domain (see Section **Managing Domain Delegation**) by expanding the organisation using the drop down to the left of the name, and then checking and unchecking the boxes as appropriate, and then hit Save.

5. The domain has now been added but will show in your Domains list with a Validation Status of "Action Required"; when you click on it the DCV box to the right will show "DCV Status" of "Not Validated". You will now need to DCV the domain (see next section).

# 6.2. Validating Control of a Domain

6.2.1. Triggering Validation

Once your domain has been added, <u>you will need to demonstrate (or have previously demonstrated) control of that domain</u>.

There are three main methods to demonstrate control:

1. Via DNS – you will need to add a given CNAME to the DNS zone of the specified domain. DNS DCVs are valid for a year, but you can re-validate at any point during that year.

2. Via a HTTP/HTTPS challenge – you will need to add a .txt file with a given hash value and filename in a specified location and served by a webserver responded to requests on that specified domain. **Note: according to the latest CA/B forum rules, HTTP/HTTPS challenges are single use challenges.**

3. Via email – you will need to respond to an email sent to one of a small number of predefined email addresses on your domain (such as hostmaster@). Email DCVs are valid for a year, but you can revalidate at any point during that year.

To trigger the DCV process using one of these methods:

1. Browse to the Domains tab, select the domain you wish to validate that you added in step 6.1, in this case, a Jisc domain. You can see the DCV Status is "Not Validated" and there's no "Expires" listed for it.
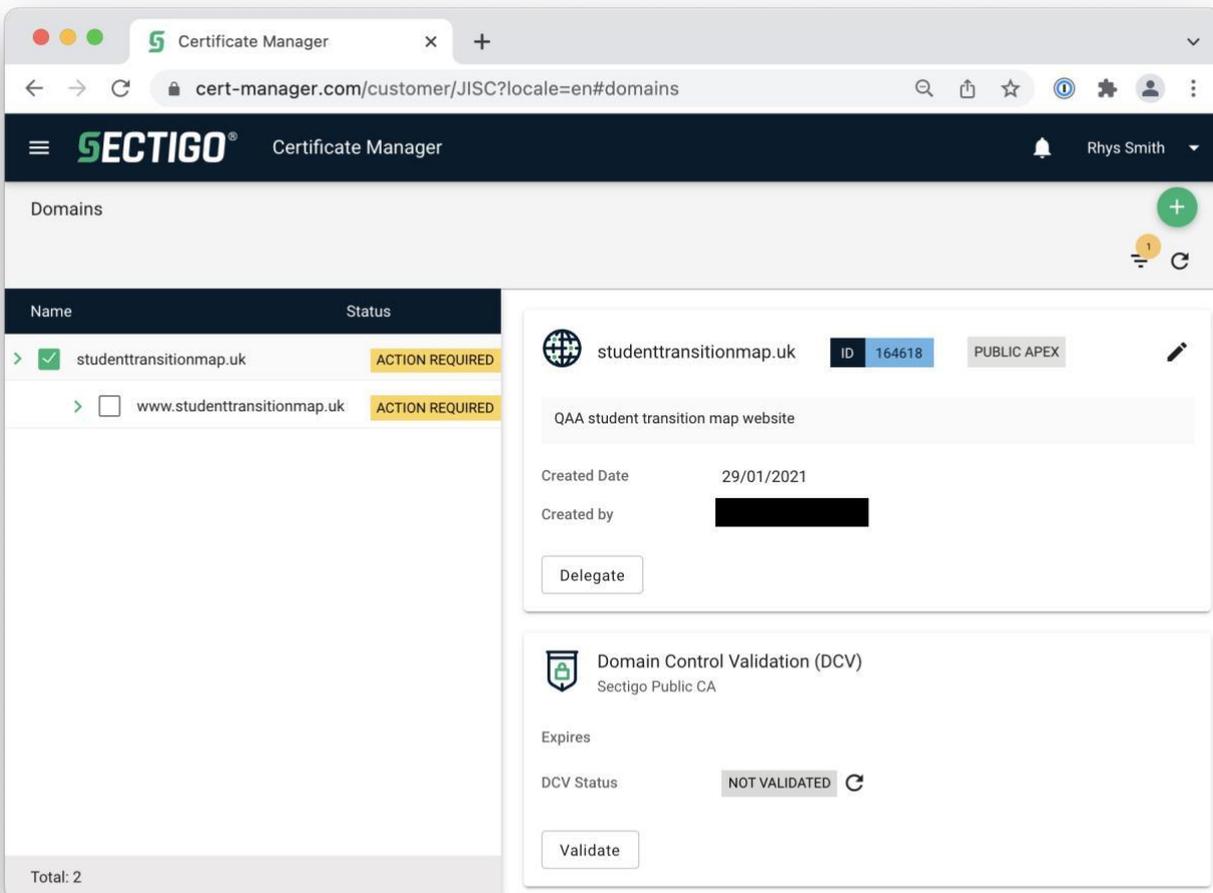
2. Click the Validate Button at the bottom of the DCV section, and then on the next page choose the DCV Method you wish to use (as previously discussed).

   a. Via a DNS CNAME – you will be given the DNS CNAME that you must insert into the zone of the relevant domain.
   Note: the FQDN under sectigo.com that SCM tells you to point your CNAME at does not point to a real DNS record and will not resolve. THIS IS NOT AN ERROR.

> **Note: you can now click the validate button at any point in the domain lifecycle, not just within the last month of it.**

    b.   Via HTTP/HTTPS – you will be given the filename and contents that you must place on the web server serving content at the relevant domain in its /.well-known/pki-validation directory.
   **Note: according to the latest CA/B forum rules, HTTP/HTTPS challenges are now single use challenges.**

    c.   Via Email – you will choose one of the pre-defined email addresses to receive a validation email.

3. Notes: For DNS CNAME or HTTP/HTTPS

- If you can make the change straight away, do so then hit submit, and SCM will check the DNS/HTTP straight away.

- If you need time to make the change, hit "Save & Close" instead, make the change, then when ready come back to SCM, find the domain in the DCV sub-tab, hit DCV again and you should be presented with the same screen – hit submit and SCM will check.

4. Notes: For Email
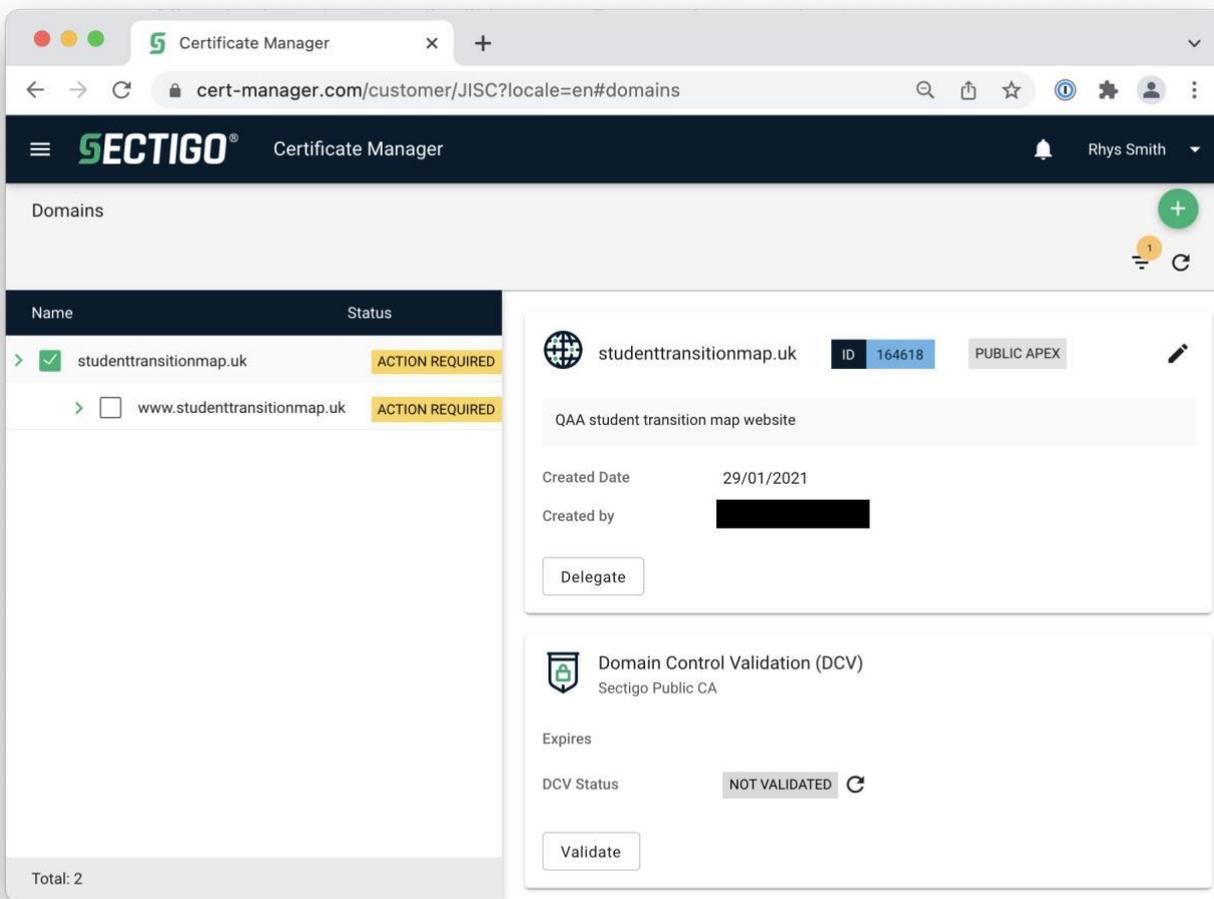
6.2.2. Having validation issues?

SECTIGO's systems regularly (once an hour) check to see if the CNAME/HTTP checks have been put in place yet. If you think you've done everything on your end, and this doesn't change within a few hours, first try the following steps to double check:

- For DNS CNAMES, use a free web-based DNS tool like **https://toolbox.googleapps.com/apps/dig/** to double check the CNAME exists for external users.

- For HTTP/HTTPS, use a free web-based HTTP checking tool like **https://httpstatus.io** to double check the URL to file exists for external users.

- Via a DNS CNAME – you will be given the DNS CNAME that you must insert into the zone of the relevant domain.
  Note: the FQDN under sectigo.com that SCM tells you to point your CNAME at does not point to a real DNS record and will not resolve. THIS IS NOT AN ERROR.

If you are still having problems, contact Jisc for further assistance.

6.2.3. Widening delegation for hosts and subdomains within the domain

You will **almost** certainly want to issue certificates under the domain you've added, not just for that literal domain just added as a CN; to do so involves one more step.

1. Add a new domain as in Section 6.1.1, but this time, enter a wildcard to allow anything under that domain (e.g. '*.example.com'), or anything under a specific subdomain (e.g. '*.internal.example.com'); making sure the domain delegation is set up correct for your organisation.

   Note: this will allow certificates to be issued for 3 levels of subdomain, e.g. '*.example.com' would allow a certificate with CN 'a.b.c.example.com' but not 'a.b.c.d.example.com'. To issues certificates more than 3 sublevels deep, simply add a new delegation 3 levels down, e.g. '*.b.c.d.example.com'.

7. Issuing and Managing SSL Certificates

7.1. SSL Certificate types available

Certificate Profile	Validation level	Notes
Jisc OV SSL	OV	A certificate for a single specified hostname, and a SAN of 'www.{the specified hostname}'. *Note: SECTIGO automatically issues the certificate with a SAN of www.{your specified hostname}, we have no control over this. If you **do not** want this, instead choose a "Jisc OV Multi-Domain SSL certificate" and **do not specify any SANs**.*
Jisc OV Multi-Domain SSL	OV	A certificate for the specified hostname and set of optional SANs.
Jisc Unified Communications Certificate	OV	Usually only required for specific purposes, e.g. Exchange servers.
Jisc Wildcard SSL	OV	A certificate for the specified wildcard hostname (e.g. '*.example.com').
Jisc EV SSL	EV	A higher assurance certificate for a single specified hostname, and 'www.{the specified hostname}'. *Note: SECTIGO automatically issues the certificate with a SAN of www.{your specified hostname}. If you **do not** want this, instead choose a "Jisc EV Multi-Domain SSL certificate" and **do not specify any SANs.***
Jisc EV Multi-Domain SSL	EV	A higher assurance certificate for the specified hostname and set of optional SANs.
Jisc IGTF Multi-Domain SSL	IGTF	A certificate for the specified hostname and set of optional SANs – but only for interoperation with IGTF services.
Jisc EV Anchor (Validation Only)		A pseudo-certificate – used by SECTIGO to manage which domains are included in the EV level validation, and that you are thus able to issue EV certificates under. **Important: You should only ever have one of these active for your organisation.**

Note: the Jisc Certificate Service supports RSA and ECC algorithms, simply create your private keys and CSRs using your choice of algorithm and the certificate will be issued as appropriate.

7.2. Extended Validation (EV) Certificates

To be able to issue EV certificates, you need to add further information about your organisation, and then apply for an EV Trust Anchor that covers all domains you wish to issue EV certificates under. SECTIGO then validate it.

Note that if you're entered the relevant information into the JCS signup page, most of the following will have been automatically entered for your. If, however, you need to do this yourself, then the following will tell you what to do.

## 7.2.1. Adding further information about your organisation

The first step is to provide further details about your organisation to Jisc who will enter this for you into the EV details tab of your organisation in SCM. You CANNOT do this yourself. To view the details that we'll need:

1. In SCM, browse to the Organizations tab, choose you organisation and hit Edit. In the EV Details tab you will be able to view, but not edit, the currently recorded information. Only Jisc can edit this for you.

2. Contact Jisc to let us know you want to issue EV certs, providing as much of the information as possible.

3. Jisc will add this detail on your behalf.

7.2.2. Configuring an EV Trust Anchor

The second step is to issue a special certificate – using the "Jisc EV Anchor (Validation Only) profile", covering the domains under which you wish to issue EV certificates. To do this:

1. Create a new private key and CSR with a subject of '/C=GB/CN=your_main_domain'.

   a. E.g. Jisc's cert would have a subject of '/C=GB/CN=jisc.ac.uk'.

2. In SCM, go to Certificates > SSL Certificates, and click on Add (the green + button in the top right).

3. Choose the "Using a Certificate Signing Request (CSR)" option. On the next screen, paste in the CSR you generated.

4. Configure your EV anchor as appropriate:

   a. Choose your organisation from the list.

   b. Choose the "Jisc EV Anchor (Validation Only)" certificate profile.

   c. Ensure the "common name" contains your primary domain name, it will populate from your CSR.

   d. Include a comma separated set of other domains you wish to issue EV certificates for in the SANs field.

   e. **Note: the domains listed in both fields need to previously have been added and DCV'ed successfully.**
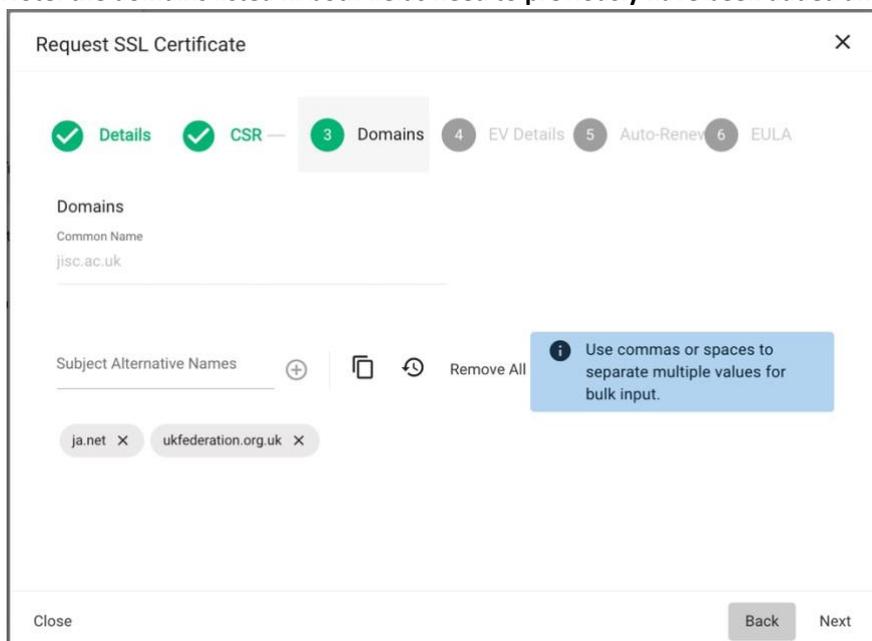
    f.   Click next, view your organisation EV details, click next, configure auto-renew options, click next, read and accept the EULA, and then submit.

    g.   **Note: another RAO will next need to go to SCM, find the EV anchor request, and Approve it.**

    h.   Your request will be passed to SECTIGO for validation. After validating your organisation to this higher level of assurance, your EV Anchor should be issued. You can now issue EV certificates for the domains listed.

7.2.3. Updating your EV Anchor

If you wish to update the list of domains in your EV Anchor:

1. In SCM, go to Certificates > SSL Certificates.

2. Find your existing EV Anchor certificate, select it, and click on "Replace"

3. Follow the guide above (you will have to provide the CSR again), but adding/removing SANs as appropriate from the existing certificate.

4. Submit the request for validation by SECTIGO (remembering that another RAO must approve it first).

5. **Note: if you encounter any issues in the renewal, contact Jisc and/or SECTIGO to progress the update.**

7.3. Auto-renewing certificates

When applying for a certificate, you have an option of enabling "auto renewal of this certificate" and choosing how many days before expiry it should auto-renew.

Turning on this option for a certificate means that however many days you specified before the certificate was due to expire, a new certificate would automatically be issued and the requester emailed to notify them that a replacement is available, with a link to download it.

7.4. Methods of issuing certificates

There are four main ways of issuing SSL certificates with varying degrees of central control vs self-service for your users.

7.4.1. …via SCM

The simplest way and the way that retains most control is to only issue and manage certificates via registered users of SCM. You would have to give an SCM account to any of your users you wish to manage certificates, or act on their behalf by getting them to send you CSRs and you request the certificates for them.

To issues certificates via SCM, simply:

1. Log into SCM.

2. Browse to Certificates > SSL certificates.

3. Click on Add.

4. Follow the prompts. If requesting a certificate on behalf of someone else, you can enter their email address in this process.

5. Note that some types of certificates, e.g. EV Certificates, may require a further step of another RAO/DRAO approving your request.

    a. They will have to log into SCM, find your certificate in the Certificates > SSL Certificates list (with status of "Requested"), select it and hit the "Approve" button.

7.4.2. …via self-enrolment (with shared access code)

Another option the requires fewer users to be registered on SCM is to allow certificates to be requested via self-enrolment. When enabled, you can give a link and a shared secret to your users which allows them to request certificates without having to have an SCM account.

To enable self-enrolment via access code:

1. Login to SCM.

2. Browse to Enrolment > Enrolment Forms, choose "SSL Web Form" and click on the "Accounts" button.

3. In the dialogue that pops up, click on "Add".

    a. Give the account a name (e.g. "Camford University SSL Self-enrolment Account")

    b. Choose the organisation, and optionally department, associated with these settings.

    c. Choose which certificate types are available through this self-enrolment configuration by choosing them and clicking the right arrow to include them in the "Assigned Certificate Profiles" list. **Note: to avoid confusing self-enrolment users, we recommend you do NOT include the EV Anchor (Validation only) certificate profile type.**

4. Specify an access code; this will need to be shared with your users authorised to self-enrolment.

5. By default, self-enrolment certificate requests will require approval by an RAO/DRAO user. If you check the "Automatically Approve Self Enrolment Requests" then relevant certificate types will be automatically approved without an RAO/DRAO having to get involved (EV certificates will always require approval).

7.4.3. …via self-enrolment (with SAML authentication)

Similar to the previous self-enrolment option, except instead of sharing a link and a shared secret, you just share a link that makes the user first authenticate via your SAML IdP. This ensures only users with valid live accounts within your organisation can request certificates.

To enable self-enrolment with SAML authentication:

1. Login to SCM.

2. Browse to Settings > Enrolment Forms.

3. Click on Add.

4. In the dialogue that pops up:

    a. Choose "the SSL SAML self-enrolment form" type.

    b. Give the account a name (e.g. "Camford University SSL SAML Self-enrolment Account")

    c. Choose the organisation, and optionally department, associated with these settings.

    d. Choose which certificate types are available through this self-enrolment configuration by choosing them and clicking the right arrow to include them in the "Assigned Certificate Profiles" list. **Note: to avoid confusing self-enrolment users, we recommend you do NOT include the EV Anchor (Validation only) certificate profile type.**

5. Click on the "regenerate" button to create a random secret that becomes a part of the URL to share.

6. The link shown underneath is the link to share with your users.

7.4.4. …via ACME/certbot

A final option is to use the ACME protocol and the certbot tool to directly request certificates from the command line. See **Using ACME/certbot automation** for further details.

7.5. Revoking Certificates

To revoke a certificate:

1. Login to SCM

2. Browse to Certificates > SSL Certificates.

3. Find the certificate you wish to revoke, select the certificate, and hit the "revoke" button.

Note: You cannot currently revoke ACME issued certificates via SCM; to do so please contact Jisc or SECTIGO directly as SECTIGO will need to revoke them on your behalf.

7.6. Certificate Formats

When downloading your certificate, you are provided with a selection of certificate formats via the email you receive. You can also download the certificate from the Sectigo Portal where these formats are also.

Certificate formats that we offer:

Certificate Format	Included on Certificate
As Certificate Only, PEM Encoded	Server Certificate Only.
As Certificate (w/ issuer after), PEM Encoded	Server and Intermediate Certificates
As Certificate (w/ chain), PEM Encoded	Root, Intermediate and Server Certificates
As PKCS#7: .pb7	DER Format - Full Chain
As PKCS#7, PEM Encoded	PKCS7 PEM Format – Full Chain

Issuing CA Certificates Only:

1. As Root/Intermediate(s) only, PEM Encoded: Issuing Certificates only Root > Intermediates.
2. As Intermediate(s)/Root only, PEM Encoded: issuing Certificates only Intermediates > Root.

8. Issuing and Managing Client Certificates

8.1. Client Certificate types available

Certificate Profile	Notes
Jisc Personal Certificate (RSA/ECC)	The standard type of client certificate to be used for e.g. S/MIME email signing/encryption.
Jisc IGTF-Classic-Robot Email (RSA/ECC)	These are all variations of IGTF (Interoperable Global Trust Federation) client certificates. If you are not specifically wanting to interoperate with IGTF services or users, you almost certainly want a "Jisc Personal Certificate".
Jisc IGTF-MICS-Personal (RSA/ECC)	
Jisc IGTF-MICS-Robot Personal (RSA/ECC)	

Note: the Jisc Certificate Service supports RSA and ECC algorithms, simply choose the type you want when applying for a new certificate. **RSA certificates are better supported in clients (e.g. Outlook).**

8.2. Methods of issuing certificates

There are three main ways of issuing client certificates with varying degrees of central control vs self-service for your users.

Note: Client certificates issued through SCM are created by SECTIGO, including the private keys. These keys are held in escrow, encrypted by Jisc's master key. If you need to recover key material for any of your users, contact Jisc who will verify the identity of the requester and validate the request; upon successful completion of this process we would be able to recover this key material for you.

8.2.1. …via SCM

The simplest way and the way that retains most control is to only manage certificates via registered users of SCM. You would have to give an SCM account to any of your users you wish to manage certificates.

To issues certificates via SCM, simply:

1. Log into SCM.

2. Browse to Certificates > Client certificates.

3. If this is a client cert for a new user (one who hasn't had a client cert before):

    a. Click on Add and fill out the form with the user's details. You will specify the relevant values and click OK. **Note: The "common name" field will usually be the user's full name.**

4. If this is a new client cert for an existing user:

    a. Browse to the user in the list, select them, and click on the Certificates button. Click on the "Send Invitation" button, choose the correct certificate type and period, and click OK.

5. The user should be emailed a link to follow to create and download their certificate.

8.2.2. …via self-enrolment (using an access code)

Another option the requires fewer users to be registered on SCM is to allow certificates to be requested via self-enrolment. When enabled, you can give a link and a shared secret to your users which allows them to request certificates without having to have an SCM account.

To enable self-enrolment via Access Code:

1. Login to SCM.

2. Browse to Enrolment > Enrolment Forms.

3. Choose "Client Certificate Web Form" and click on the "Accounts" button.

4. In the dialogue that pops up, click on "Add".

    a. Give the account a name (e.g. "Camford University Client Cert Account")

    b. Choose the organisation, and optionally department, associated with these settings.

    c. Choose which certificate types are available through this self-enrolment configuration by choosing them and clicking the right arrow to include them in the "Assigned Certificate Profiles" list. **Note: to avoid confusing self-enrolment users, we recommend you only include the Certificate profiles beginning with Jisc, exclude the GÉANT profiles (which are functionally identical to the Jisc counterparts).**

5. Specify an access code; this will need to be shared with your users authorised to self-enrolment.

Note: Self-enrolment certificate requests will require approval by an RAO/DRAO user.

8.2.3. …via self-enrolment (using SAML authentication)

To allow users to self-enrol for client certificates by authenticating through your SAML IdP, the URL to give them is

https://cert-manager.com/customer/JISC/idp/clientgeant

For this to work, you will have to do two things: configuring your organisation in SCM, and configure your SAML Identity Provider.

In SCM:

1. Browse to Settings > Organizations, choose your organisation and hit Edit.

2. In the general tab, set the value for "Academic code (SCHAC Home Organization)" to the value to the same value your SAML Identity Provider will be sending for the schacHomeOrganization attribute for your users. It will typically be primary domain (e.g. jisc.ac.uk) but confirm this with your SAML Identity Provider administrators.

3. If you plan to issue any of the IGTF profile client certificates via this self-enrolment method, then ensure the "Secondary Organization Name" is set to the name used in grid certificates (ASCII) for your organisation. Please check existing certificates. *As grid certificate subjects are used as "usernames" in systems, it is vital that the whole subject string is kept as it was before for your users.*
Note: if you do not plan to issue any IGTF profile client certificates via this self-enrolment method, simply leave this field blank.

On your SAML Identity Provider:

1. Ensure your Identity Provider is configured to support the following attributes for any user you wish to use this self-enrolment method. Your attribute release policy should allow the release of all of these attributes to the SCM SAML SP. Its entityID is **https://cert-manager.com/shibboleth**

Friendly Name	SAML 2 Name	Example	Description
displayName	urn:oid:2.16.840.1.113730.3.1.241	Johnny Doe	USED for CN.
cn	urn:oid:2.5.4.3	John Doe	fallback for CN.
sn	urn:oid:2.5.4.4	Doe	fallback for CN.

givenName	urn:oid:2.5.4.42	John	fallback for CN.
mail	urn:oid:0.9.2342.19200300.100.1.3	**johndoe@example.ac.uk**	REQUIRED
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	**jd@example.ac.uk**	REQUIRED
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	urn:mace:**terena.org**:tcs:personal-user	REQUIRED
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	**example.ac.uk**	REQUIRED

8.3. Revoking Client Certificates

To revoke a certificate:

1. Login to SCM

2. Browse to Certificates > Client Certificates.

3. Find (or search for) the user in the list, select them, and click the "Certificates" button.

4. In the list of certificates issued for that user, select the certificate you wish to revoke, and hit the "revoke" button.

9. Managing Notifications

By default, only a limited set of notifications will be issued by SCM – for example, letting requesters know when a new certificate is able to be downloaded. Custom notifications can be set up at the organisational level, however.

All notification management steps outlined above are managed by logging into SCM and browsing to the Settings > "Email Notifications" tab.

Types of notifications available to be customised include notifications of upcoming certificate expiry, upcoming DCV expiry, actions awaiting approval, issuance of new certificates, failure to issue certificates, and many more.

To add a new notification, simply click the Add button, and in the dialogue that follows, a "Notification Type" dropdown list will show all types of notifications available. Simply choose the type you wish to add and configure appropriately.

All notifications can be customised for the organisation as a whole, or for individual department(s).

10. Overview of ACME/certbot automation

Sectigo supports the installation and renewal of server certificates via the ACME protocol (see RFC 8555), using the certbot tool (or other ACME compatible client), in a similar manner to using free Let's Encrypt certificates.

Please see the separate document describing in detail how to use ACME and Sectigo.

11. Common Issues and Errors

11.1.   When Issuing SSL Certificates

Error	Explanation
SSL issuance fails (request is marked as Invalid) with the error: "Anchor Certificate address details are different".	The subject specified in your CSR did not match that registered for your organisation. Go to Settings > Organisations, choose your organisation and click Edit and ensure the details in your CSR match those in the General sub-tab for your organisation. For example, if your CSR had a subject of "C=GB, L=Bristol, O=Jisc, CN=foo.example.com" but your organisation had a city of Manchester, the details do not match and issuance would fail.
SSL issuance fails with the error: You cannot order certificates for the following or additional domains: [your domain]. Please doublecheck correctness of entered information or navigate to 'Domains' subtab of 'Settings' tab to request/activate/delegate them or enable this type of certificate for them in terms of the selected organization.	Delegation of your domain has not been configured to allow the FQDN you have requested as the CN of your certificate. See **Managing Domain Delegation** for details on how to do this properly. You may have forgotten to delegate subdomains of your domain (i.e. adding a delegation of '*.example.com').

12. Help Videos

12.1 Adding Users

12.2 Adding and Validating Domains

12.3 Requesting a Certificate

12.4 Setting up a department

12.5 EV Anchor