



Sectigo

Authenticatie en Automation

versie 1.0.5, 9 april 2020

<https://wiki.surfnet.nl/display/SCERTS/Workshops+Sectigo>
> Attachments

RTFM

- Sectigo Knowledge Base:
<https://support.sectigo.com/>
- Sectigo® Certificate Manager Administrator's Guide
(SCMAG)
- Certificate Manager REST API
- Courant: versie 20.2, March 2020

Sectigo® Certificate Manager
Administrator's Guide
20.2

SCMAG

March 2020





SECTIGO

Certificate Manager

Login

Password

LOGIN

Or Sign In With

Your Institution

[SCM Support](#)

[Sectigo Certificate Manager Status](#)

[SCM Guides](#)

The use of Sectigo Certificate Manager is restricted to authorized users only. Access to Sectigo Certificate Manager may be monitored by Sectigo for operational or business purposes. Unauthorized access may lead to prosecution and/or disciplinary action.

Login via SURFconext

SAML login

- Voor RAOs:
 - login via username/password
 - login via SURFconext
- Voor eindgebruikers (persoons- en gridcertificaten):
 - login via SURFconext
- IdP moet beschikbaar zijn via *edugain*
- Optioneel: SURFsecureID

Inloggen via SURFconext

- Probeer in te loggen via SURFconext op <https://cert-manager.com/customer/surfnet/ssocheck/>
- Identity Provider niet in de lijst?
⇒ Publiceer IdP in eduGAIN-metadata
- Foutmelding “Dienst niet toegankelijk via instelling”
⇒ Dien koppelverzoek in



service.seamlessaccess.org/ds/?entityID=https%3A



Access to

Sectigo Certificate Manager

Find Your Institution

Your university, organization or company



Examples: Science Institute, Lee@uni.edu, UCLA

Rijksmuseum Amsterdam

rijksmuseum.nl

Hogeschool van Amsterdam

hva.nl

University of Amsterdam

uva.nl

Vrije Universiteit Amsterdam

vu.nl

Openbare Bibliotheek Amsterdam (OBA)

Amsterdam University of the Arts

Fout - Dienst niet toegankelijk via instelling

De instelling waarmee je wilt inloggen heeft toegang tot deze dienst niet geactiveerd. Dat betekent dat jij geen gebruik kunt maken van deze dienst via SURFconext. Neem contact op met de helpdesk van jouw instelling als je toegang wilt krijgen tot deze dienst. Geef daarbij aan om welke dienst het gaat (de 'SP') en waarom je toegang wilt.

Blijft deze foutmelding terug komen? Maak dan gebruik van de hieronder vermelde hulp opties.

Vermeld bij contact via helpdesk of mail de onderstaande code(s):

Idp Hash: **32171f5a7a012631cb41c6824947cf99**

EC: **25282**

SP: **<https://cert-manager.com/shibboleth>**

IP: **145.101.112.205**

SP Name: **Cert Manager | Sectigo**

UR ID: **5e7b3caf5a9dd**

Bezoek [de SURFconext support pagina's](#) voor ondersteuning bij deze foutmelding. Hier kun je ook vinden hoe je contact kunt opnemen met het supportteam als de fout aanblijft.

No Surfing



SURFconext Wiki



Helpdesk

SURFconext IdP Koppelen

- Via SURFconext Dashboard (<https://dashboard.surfconext.nl/>)
- Door *SURFconext-verantwoordelijke* van je instelling
- IdP in eduGAIN-metadata publiceren:
 - tabblad *Mijn Instelling*, wijzigingsverzoek 'gepubliceerd in eduGAIN'
- Dienst Koppelen:
 - Dien koppelverzoek in met dienst *Cert Manager* | *Sectigo* (Entity ID: <https://cert-manager.com/shibboleth>)
- Zie ook:
<https://wiki.surfnet.nl/display/surfconextdev/Identity+Provider+opnemen+in+eduGAIN>

Dashboard

dashboard.surfconext.nl/apps/7979/saml20_sp/overview

SURF CONEXT IdP dashboard SURFnet bv - Productie




Welkom, Joost van Dijk [Switch identiteit](#) [EN](#) [NL](#) [Help](#) [Uitloggen](#)

Statistieken Services Autorisatieregels Tickets Mijn instelling Uitnodiging

Terug Overzicht Consent Attributen Licentie Gebruikt door Service gebruik SURF Secure ID

Cert Manager | Sectigo

Entity ID: <https://cert-manager.com/shibboleth>

 **Dienst gekoppeld**  **Geen licentie-informatie beschikbaar** [Lees meer](#)  **SURFsecureID aangezet**

Beschrijving

Er is geen beschrijving voor deze service.

SURFsecureID aangezet

Voor het inloggen op deze dienst is authenticatie met een tweede factor middels SURFsecureID vereist. Alle gebruikers moeten een token gebruiken van minimaal zekerheidsniveau (Level of Assurance / LoA): 1oa2. Voor meer informatie zie de [wiki](#)

Contractuele basis

Dienst aangeboden door op SURFconext aangesloten instelling. Voor meer informatie zie de [wiki](#).

Privacy-informatie

De leverancier heeft geen privacy-informatie aangeleverd.

[Website](#)

[Privacyverklaring](#)

Deze Service Provider is beschikbaar in SURFconext via [eduGAIN](#). De Service Provider is door de volgende federatie geregistreerd: <https://incommon.org>.

[SURFnet](#) [Gebruikersvoorwaarden](#) support@surfconext.nl

RAO koppelen met IdP

- Twee manieren:
 1. RAO account vooraf aanmaken, koppelen met gefedereerd account
 2. Invite IDP user (mail scs-ra@surfnet.nl voor approval)
- Account mapping via `edupersonPrincipalname` (ePPN) attribuut
Voorbeeld: `jd@example.edu`
- Note:
≠ `email` attribuut
case sensitive
- Mismatch?
IdP user with `idpPersonID=jd@example.edu` is not available for customer Example Edu and new IdP user creation ability is switched off

SECTIGO

Certificate Manager

Certificate Manager SSO Check page

You have successfully authenticated to the configured IdP so basic functionality seems to be work correctly.
The Your Institution IdP (<https://idp.surfnet.nl>) authenticated using <http://surfconext.nl/assurance/loa2>.
The returned attributes are as follows:

Name	Value	Required?
ePPN	jd@example.edu	Y
givenName	John	
sn	Doe	
email	johndoe@example.edu	Y

Add New Client Admin ✕

CREDENTIALS	PRIVILEGES	ROLE
*-required fields		
Login*	<input checked="" type="checkbox"/> Allow creation of peer admin users	Expand All
Email*	<input checked="" type="checkbox"/> Allow editing of peer admin users	<input type="checkbox"/> MRAO Admin
Forename*	<input checked="" type="checkbox"/> Allow deleting of peer admin users	<input checked="" type="checkbox"/> RAO Admin - SSL
Surname*	<input checked="" type="checkbox"/> Allow DCV	<input checked="" type="checkbox"/> RAO Admin - Client Certificate
Title	<input checked="" type="checkbox"/> Allow SSL details changing	<input checked="" type="checkbox"/> RAO Admin - Code Signing
Telephone Number	<input type="checkbox"/> Allow SSL auto approve	<input type="checkbox"/> DRAO Admin - SSL
Street	<input type="checkbox"/> WS API use only ⓘ	<input type="checkbox"/> DRAO Admin - Client Certificate
Locality		<input type="checkbox"/> DRAO Admin - Code Signing
State/Province		
Postal Code		
Country		
Relationship		
Certificate Auth		
Identity provider		
IdP Person Id		
Password*		
Confirm Password*		

OK Cancel



CREDENTIALS

*-required fields

Email*

[Click here to show additional fields](#)

PRIVILEGES

- Allow creation of peer admin users
- Allow editing of peer admin users
- Allow deleting of peer admin users
- Allow DCV
- Allow SSL details changing
- Allow SSL auto approve

ROLE

[Expand All](#)

- RAO Admin - SSL
- RAO Admin - Client Certificate
- RAO Admin - Code Signing
- DRAO Admin - SSL
- DRAO Admin - Client Certificate
- DRAO Admin - Code Signing

OK

Cancel



SECTIGO

Certificate Manager

LOGIN

Or Sign In With

Your Institution

[SCM Support](#)
[Sectigo Certificate Manager Status](#)
[SCM Guides](#)

The use of Sectigo Certificate Manager is restricted to authorized users only. Access to Sectigo Certificate Manager may be monitored by Sectigo for operational or business purposes. Unauthorized access may lead to prosecution and/or disciplinary action.



service.seamlessaccess.org/ds/?entityID=https%3A



Access to

Sectigo Certificate Manager

Find Your Institution

Your university, organization or company



Examples: Science Institute, Lee@uni.edu, UCLA

Rijksmuseum Amsterdam

rijksmuseum.nl

Hogeschool van Amsterdam

hva.nl

University of Amsterdam

uva.nl

Vrije Universiteit Amsterdam

vu.nl


Openbare Bibliotheek Amsterdam (OBA)


Amsterdam University of the Arts

Cert Manager | Sectigo needs your information before logging in

The service needs the following information to function properly. These data will be sent securely from your institution towards Cert Manager | Sectigo via [SURFconext](#) .

The following information will be shared with Cert Manager | Sectigo:

 SURFnet bv Are the details below incorrect?	
Display Name	<u>John Doe</u> ?
Full Name	<u>John Doe</u> ?
First name	<u>John</u> ?
Surname	<u>Doe</u> ?
Email address	<u>johndoe@example.edu</u> ?
Institution user ID	<u>jd@example.edu</u> ?
Entitlement	<u>urn:mace:terena.org:tcs:personal-user</u> ?

 SURFconext Explanation	
Identifier	<u>9f14a47ceaa0d670fe52a6a93063d73ebd63ae98</u> ?

Do you agree with sharing this data?

[Yes, proceed to Cert Manager | Sectigo](#) [No, I do not agree](#)

You are using 171 services via SURFconext. [View the list of services and your profile information.](#) ↗

RAO login versterken

- Met persoonscertificaat
 - Op basis van Certificate Serial
 - Let op:
 - ▶ autorevoke: serial aanpassen indien nieuw certificaat
 - ▶ Authenticatie met certificaat *niet* bij SURFconext login
- Met SURFsecureID
 - SURFconext Dashboard:
koppilverzoek “Cert Manager | Sectigo”
met minimum loa 2 of 3

CREDENTIALS

*-required fields

Login* johndoe

Email* john.doe@example.edu

Forename* John

Surname* Doe

Title

Telephone Number

Street

Locality

State/Province

Postal Code

Country Netherlands

Relationship

Certificate Auth 42:48:B2:63:88:A1:BE:91:9

Identity provider Your Institution

IdP Person Id*

Password*

Confirm Password*

PRIVILEGES

- Allow creation of peer admin users
- Allow editing of peer admin users
- Allow deleting of peer admin users
- Allow DCV
- Allow SSL details changing
- Allow SSL auto approve
- WS API use only ⓘ

ROLE


[Expand All](#)

- MRAO Admin
- RAO Admin - SSL
- RAO Admin - Client Certificate
- RAO Admin - Code Signing
- DRAO Admin - SSL
- DRAO Admin - Client Certificate
- DRAO Admin - Code Signing

OK

Cancel

Cert Manager | Sectigo



[Website](#)

[Privacy statement](#)

This Service Provider is available in SURFconext through [eduGAIN](#). The Service Provider is registered by the following federation: <https://incommon.org>.

SURFsecureID

With [SURFsecureID](#) you can better secure access to services with strong authentication.

A user logs in with username and password (the first factor) and SURFsecureID takes care of the second factor authentication like via a mobile app or USB key.

SURFsecureID Level of Assurance (LoA)

LoA 2 (see the wiki for more info)

Selecteer token voor login



Yubikey

Selecteer



Tiqr

Selecteer

[Annuleren](#)

[Help](#)

SECTIGO

Certificate Manager

Certificate Manager SSO Check page

You have successfully authenticated to the configured IdP so basic functionality seems to be working correctly.
The Your Institution IdP (<https://idp.surfnet.nl>) authenticated using <http://surfconext.nl/assurance/loa2>.
The returned attributes are as follows:

Name	Value	Required?
ePPN	jd@example.edu	Y
givenName	John	
sn	Doe	
email	johndoe@example.edu	Y

Automation

Automation

- Docs: [Sectigo Knowledge Base](#)
- Check your CAA records
- Sectigo ACME service
- SCM - Sectigo Certificate Manager REST API
- Agents (discovery, MS AD integration, ...)

DNS CAA Tester

[DNS Certification Authority Authorization \(CAA\)](#) uses your DNS records to let you specify which certificate authorities are allowed to issue certificates for the domains you own.

To test your domain's CAA record, enter it below.

↳ Domain:

✓ All looks good

```
-----  
0 issue "digicert.com"  
0 issue "sectigo.com"
```

If you're not quite ready to test your DNS CAA record yet, then perhaps worth a visit to:

- [sslmate](#) for generating your DNS CAA records.
- [SSL Labs](#) for testing your complete SSL config.

CAA records toevoegen

- <https://sectigostore.com/ssl-tools/caa-record-generator.php>
- Via SURFdomeinen portal (<https://www.surfdomeinen.nl/>)
- Door *DNS-Beheerder* van je instelling

SURF DOMEINEN

SURFnet bv
[Logboek](#) | [Instellingen](#) | [Log uit](#)

[Overzicht](#) [Domeinregistratie](#) [DNS beheer](#) [Nameservers](#)

[Zones](#) [Zoeken naar records](#) [Handmatige reverse zones](#) [Automatische reverse zones](#)

Zone surfcertificaten.nl.

[Terug naar zones](#)

Zone surfcertificaten.nl. [Exporteer +](#) [Record toevoegen +](#)

[vorige pagina](#) [volgende pagina](#)

Type	FQDN	TTL	Waarde	Omschrijving
caa	surfcertificaten.nl.	0	iodef "mailto:so@surf.nl"	edit delete
caa	surfcertificaten.nl.	0	issue "digicert.com"	edit delete
caa	surfcertificaten.nl.	0	issue "sectigo.com"	edit delete

[vorige pagina](#) [volgende pagina](#)

Filter records

Type:

FQDN:


TTL:

Waarde:

Omschrijving:

[Filter](#)

DNSSEC



 **DNSSEC is ingeschakeld voor deze zone**

Wilt u deze zone verhuizen?
[Neem dan contact op met SURFnet](#) voor meer informatie over het verhuizen van zones met DNSSEC.

Sectigo ACME service



Sectigo ACME service

- Automated Certificate Management Environment (ACME) [RFC 8555](#)
- ACME account aanmaken met SCM via *Settings*
 *How to Configure ACME Accounts for Organizations and Departments*
- Alleen OV en EV (dus geen DV)
- Genereer client credentials (Key ID en HMAC Key)
- Beperk scope met domain whitelist
- Ondersteunde ACME client: [certbot](#)
 *Using the Sectigo ACME Service*
- <https://community.letsencrypt.org/t/beta-phase-of-certbot-for-windows/105822>

Filter



Edit Departments Domains **ACME Accounts**

	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
<input type="radio"/>	Coöperatie SURF U.A.	Utrecht	Utrecht	NL	VALIDATED
<input checked="" type="radio"/>	SURFnet B.V.	Utrecht	Utrecht	NL	VALIDATED


cert-manager.com/customer/surfnet?private#5

ACME Accounts - SURFnet B.V.

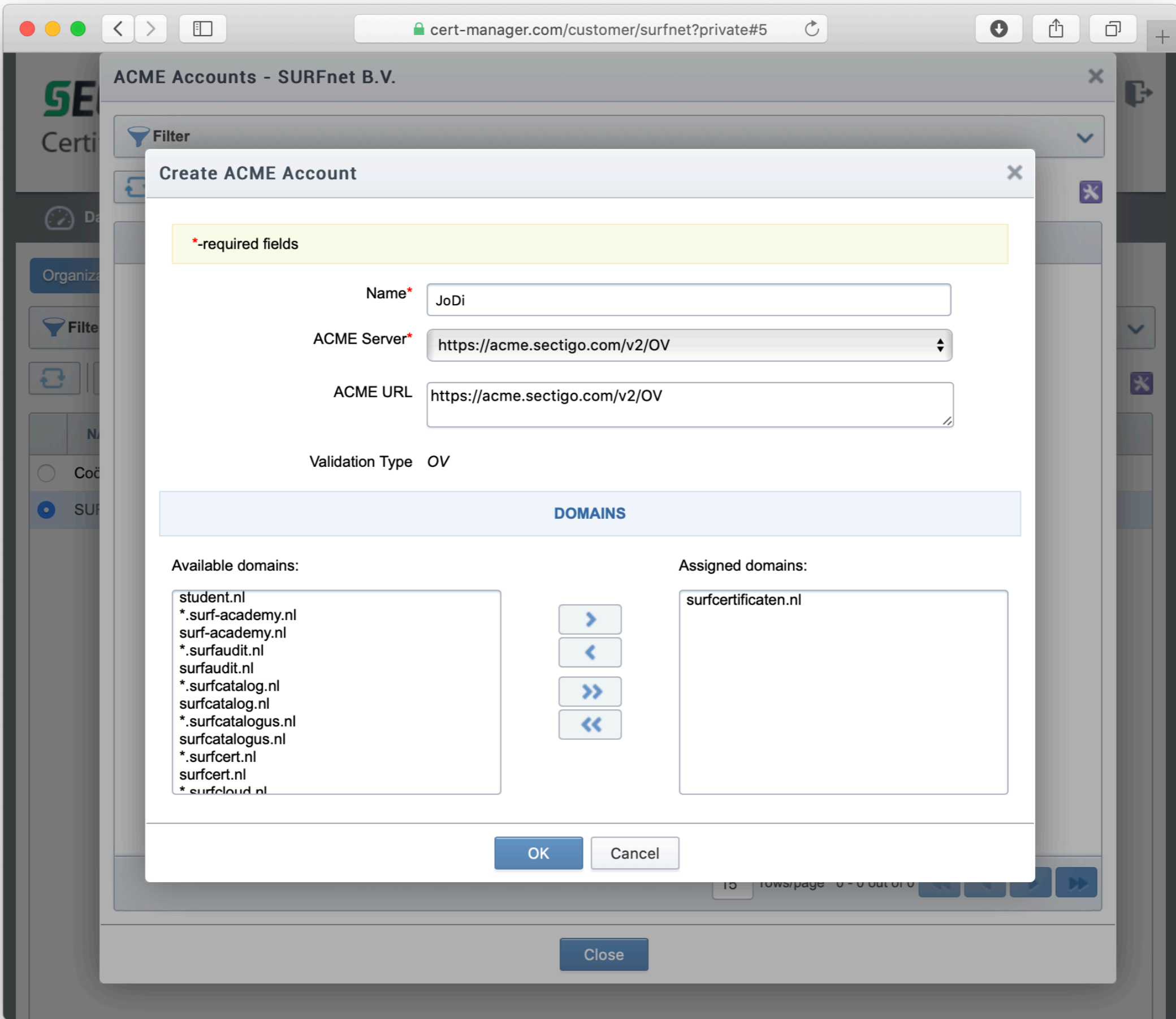
Filter

 **+ Add** 

NAME	SERVER	VALIDATION TYPE	STATUS
No data			

15 rows/page 0 - 0 out of 0 

Close



Create ACME Account

*-required fields

Name* JoDi

ACME Server* https://acme.sectigo.com/v2/OV

ACME URL https://acme.sectigo.com/v2/OV

Validation Type OV

DOMAINS

Available domains:

- student.nl
*.surf-academy.nl
surf-academy.nl
*.surfaudit.nl
surfaudit.nl
*.surfcatalog.nl
surfcatalog.nl
*.surfcatalogus.nl
surfcatalogus.nl
*.surfcert.nl
surfcert.nl
*.surfcloud.nl

Assigned domains:

- surfcertificaten.nl



OK

Cancel

Close

cert-manager.com/customer/surfnet?private#5

ACME Accounts - SURFnet B.V.

Filter

+ Add

NAME	SERVER	VALIDATION TYPE	STATUS
<input type="radio"/> JoDi	https://acme.sectigo.com/v2/OV	OV	pending

ACME Account successfully created: JoDi

ACME URL

EXTERNAL ACCOUNT BINDING

Account ID *3YR-KXZ9hI09FRd3coisFw*

Key ID

HMAC Key

15 rows/page 1 - 1 out of 1

```
# install certbot
# See instructions at https://certbot.eff.org

# Register using ID and key for external account binding:

sudo certbot register \
  --server https://acme.sectigo.com/v2/OV \
  --eab-kid 3YR-KXZ9hI09FRd3coisFw \
  --eab-hmac-key DVJx8GBjZCdU3rRQ2ueVMXJg...Qw \
  --email jd@example.edu


# Issue certificate for Apache Web Server:

sudo certbot \
  --apache
  --domain acme-demo.surfcertificaten.nl \
  --server https://acme.sectigo.com/v2/OV
```

Apache2 Ubuntu Default Page: It x +

acme-demo.surfcertificaten.nl

Apache2 Ubuntu Default Page



ubun

This is the default page of the Apache2 web server after installation on Ubuntu systems. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** in the `apache2-doc` package was installed on this server.

If you are a normal user of the web server, this probably means that the site is controlled by its administrator. Please contact the site's administrator for more information.

configuration, and

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

USERTrust RSA Certification Authority

- Sectigo RSA Organization Validation Secure Server CA
- acme-demo.surfcertificaten.nl**

acme-demo.surfcertificaten.nl

Issued by: Sectigo RSA Organization Validation Secure Server CA

Expires: Sunday, 28 March 2021 at 00:59:59 Central European Standard Time

✔ This certificate is valid

Details

OK

SCM REST API

- Docs: [Sectigo Knowledge Base](#)
SCM - Sectigo Certificate Manager REST API
- All certificates types

Certificate Manager 20.2 REST API

Search Google or type a URL

Table of Contents

- Overview
- HTTP verbs
- HTTP status codes
- Authorization
 - User Login via Password
 - User Login via Certificate
 - Developer Login
- Errors
- Resources
- SSL certificates
 - Get SSL certificate
 - Update SSL certificate
 - Listing SSL certificates
 - Listing SSL types
 - Listing of custom fields for SSL
 - Enroll SSL certificate
 - Enroll SSL certificate with Key Generation
 - Link to download private key or whole certificate
 - Collect SSL certificate
 - Revoke SSL certificate by Id

Certificate Manager 20.2 REST API

Overview

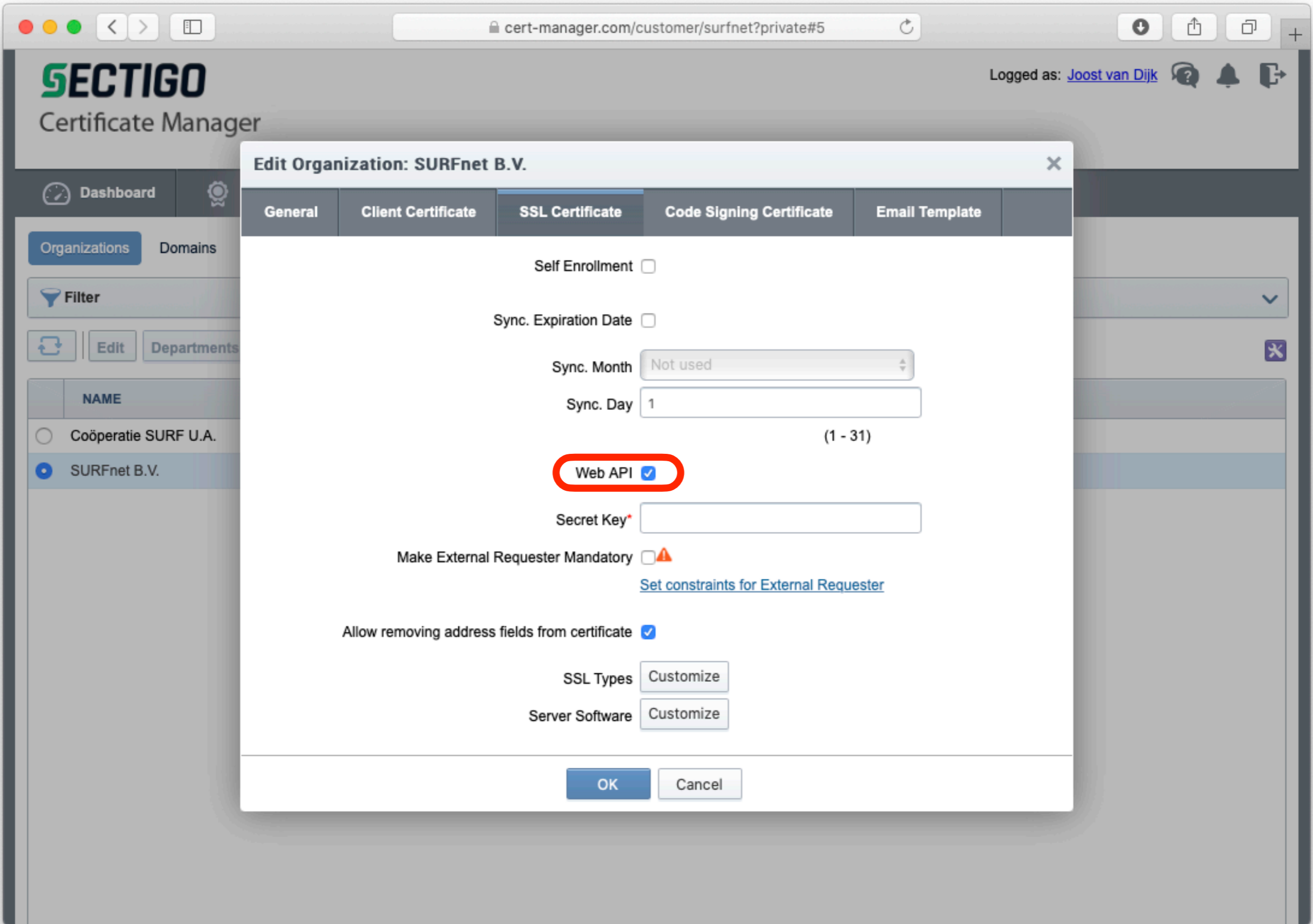
HTTP verbs

RESTful notes tries to adhere as closely as possible to standard HTTP and REST conventions in its use of HTTP verbs.

Verb	Usage
GET	Used to retrieve a resource
POST	Used to create a new resource
PATCH	Used to update an existing resource, including partial updates
DELETE	Used to delete an existing resource

SCM Setup

- Maak een API user met RAO Admin role types (SSL, Client Certificate, etc)
 - voor gebruik eerst inloggen en wachtwoord aanpassen
 - daarna: “WS API use only” (vraag scs-ra@surfnet.nl)
- *Settings | Organizations | SSL Certificate*: Enable “Web API” (dummy secret key)
- API Username/wachtwoord via HTTP headers
- SCM account URI: **surfnet** (customerURI header)
- orgID: zie organization API



NAME
<input type="radio"/> Coöperatie SURF U.A.
<input checked="" type="radio"/> SURFnet B.V.

Edit Organization: SURFnet B.V.

- General
- Client Certificate
- SSL Certificate
- Code Signing Certificate
- Email Template

Self Enrollment

Sync. Expiration Date

Sync. Month

Sync. Day

(1 - 31)

Web API

Secret Key*

Make External Requester Mandatory

[Set constraints for External Requester](#)

Allow removing address fields from certificate

SSL Types

Server Software

HTTP headers

```
Accept: application/json;charset=utf-8  
Content-Type: application/json;charset=utf-8  
customerUri: surfnet  
login: <your API user login>  
password: <your API user password>
```

SSL Certificate types

id	Name	Terms (#days)
423	GÉANT OV SSL	365, 730
424	GÉANT Wildcard SSL	365, 730
425	GÉANT Unified Communications Certificate	365, 730
426	GÉANT OV Multi-Domain	365, 730
427	GÉANT EV SSL	365, 730
428	GÉANT EV Multi-Domain	365, 730
429	GÉANT IGTF Multi Domain	365, 395
363	EV Anchor Certificate	395

orgID

```
$ curl -H @headers https://cert-manager.com/api/organization/v1
[
  {
    "id": 12345,
    "name": "Example Org",
    "certTypes": [
      "SMIME",
      "SSL"
    ],
    "departments": []
  }
]
```

```
{  
  "orgId": 12345,  
  "csr": "-----BEGIN CERTIFICATE REQUEST-----\nMII.. .",  
  "certType": 423,  
  "term": 365  
}
```

Vragen?

- scs-ra@surfnet.nl
- In progress:
<https://wiki.surfnet.nl/display/SCERTS/FAQ>