SECTIGO®

S/MIME Certificate Update Guide for Administrators

August 2023

Copyright, Trademark Notice, and Disclaimer

Copyright © 2008, 2023, Sectigo.

All rights reserved.

The documentation contains proprietary information; it is provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright and other intellectual and industrial property laws.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to Sectigo in writing. This document is not warranted to be error-free.

Except as may be expressly permitted in your license agreement, the documentation may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

The documentation is produced for general use with a variety of information management applications. It is not produced or intended for use with any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this documentation in conjunction with dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure its safe use. Sectigo and its affiliates disclaim any liability for any damages caused by such use of the documentation.

Sectigo, CodeGuard, Icon Labs are registered trademarks of Sectigo Limited and/or its affiliates. Other names may be trademarks of their respective owners.

The documentation may provide links to websites and access to content, products, and services from third parties. Sectigo is not responsible for the availability of, or any content provided on, third-party websites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Sectigo is not responsible for: (a) the quality of third-party products or services; (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Sectigo is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

1 Introduction

Sectigo Certificate Manager (SCM) is a certificate management platform for enterprise customers to automate or perform lifecycle management of certificates issued to applications and devices for secure transactions. SCM supports management of SSL/TLS, S/MIME, Code Signing and Device certificates through a unified interface.

SCM features full integration with Sectigo Certificate Authority and enables authorized administrators to manage the lifetime, issuance, deployment, renewal, and revocation of certificates on a per-organization, per-department, as well as per-user basis.

The SCM 23.8 release delivers new features and enhancements to existing functionality, including **two new S/MIME certificate profiles**, in accordance with CA/B forum S/MIME requirements.

SCM 23.8 will automatically create **two** certificate templates for each customer that meets the following criteria. Certificate profiles will NOT be automatically created.

- active
- client certificates enabled
- Sectigo Public CA backend configured
- Organization Validation (OV) enabled

Existing client certificate profiles used to issue publicly trusted S/MIME certificates will **no longer issue certificates after August 28th, 2023, at 9:00 UTC**. Renewal of any existing S/MIME certificate with old profiles is allowed only until that time.

To continue issuing publicly trusted S/MIME certificates, customers must create new certificate profiles based on two new certificate templates (see 2.3 Create a certificate profile) that will be available once SCM 23.8 is deployed.

NOTE: Once the new S/MIME profiles are created in the certificate profile section of SCM, you must replace the profiles in the enrollment endpoints.

2 New S/MIME certificate templates

To continue issuing publicly trusted S/MIME certificates, customers must create new certificate profiles based on two new certificate templates (see 2.3 Create a certificate profile) that will be available once SCM 23.8 is deployed.

2.1 Public organization-validated multipurpose S/MIME certificate

This template requires the organization to be revalidated as described below.

- It requires all domains included in email addresses to be domain validated (DCV).
- You will be able to configure in the profile whether the certificate's subject contains a commonName (CN) or emailAddress (E) attribute.
  - The CN, if included, will be identical to the organizationName (O) attribute.
  - The emailAddress (E), if included, will be the primary email address of the person.
- All email addresses will be included in the subject alternative name (SAN).
- The key usage will allow signing and encryption.
- The extended key usage will allow client authentication and email protection.

2.2 Public sponsor-validated multipurpose S/MIME certificate

This template requires the organization to be revalidated as described below.

- It requires all domains included in email addresses to be domain validated (DCV).
- It requires that persons being issued certificates are identity validated; do this by setting the person's validation type as High.
- You will be able to configure in the profile whether the certificate's subject contains a commonName (CN) or emailAddress (E) attribute.
  - The CN, if included, will be the concatenation of the person's First Name and Last Name fields. The person's Common Name field will not be used.
  - The emailAddress (E), if included, will be the primary email address of the person.
- All email addresses will be included in the subject alternative name (SAN).
- The key usage will allow signing and encryption.
- The extended key usage will allow client authentication and email protection.

NOTE: There is no replacement operation for these new client certificates.

3 Working with profiles and organizations

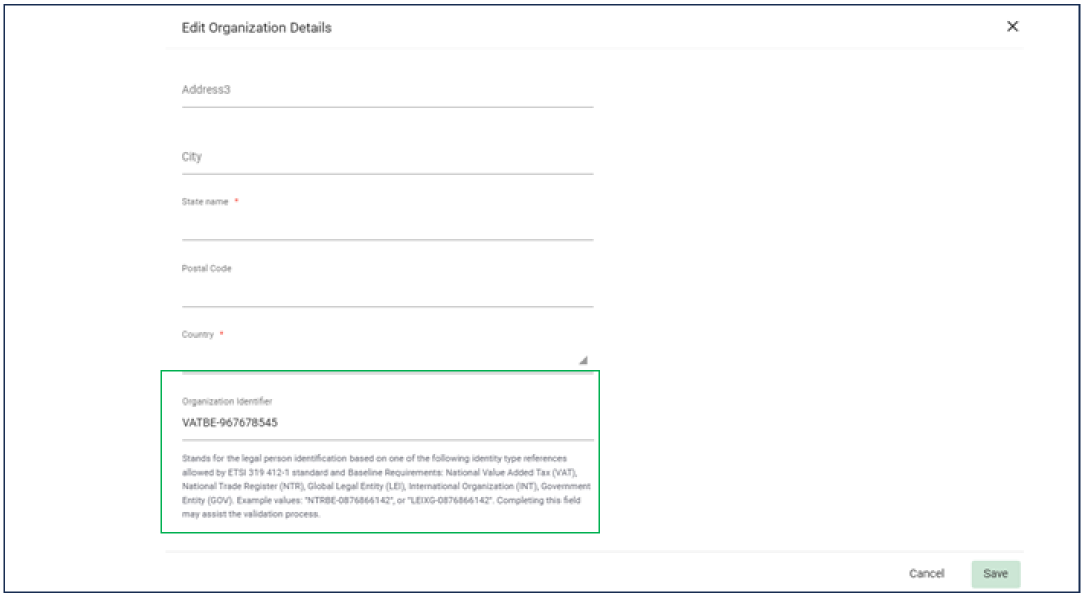
3.1 Organization identifier

Each organization now includes an optional organization identifier field built using the ETSI standard. Completing this field may assist the validation process.

The supported legal person identity types for S/MIME issuance are the following:

- National Value Added Tax (VAT)
- National Trade Register (NTR)
- Global Legal Entity (LEI)
- Government Entity (GOV)
- International Organization (INT)

Similar to the existing organization details, updating the organization identifier field will lead to cancelation of the current organization validation and will initiate the revalidation process.



Edit Organization Details

Address3

City

State name *

Postal Code

Country *

Organization Identifier

VATBE-967678545

Stands for the legal person identification based on one of the following identity type references allowed by ETSI 319 412-1 standard and Baseline Requirements: National Value Added Tax (VAT), National Trade Register (NTR), Global Legal Entity (LEI), International Organization (INT), Government Entity (GOV). Example values: "NTRBE-0876866142", or "LEIXG-0876866142". Completing this field may assist the validation process.

Existing validations will continue to work for OV SSL certificates until they would normally expire.

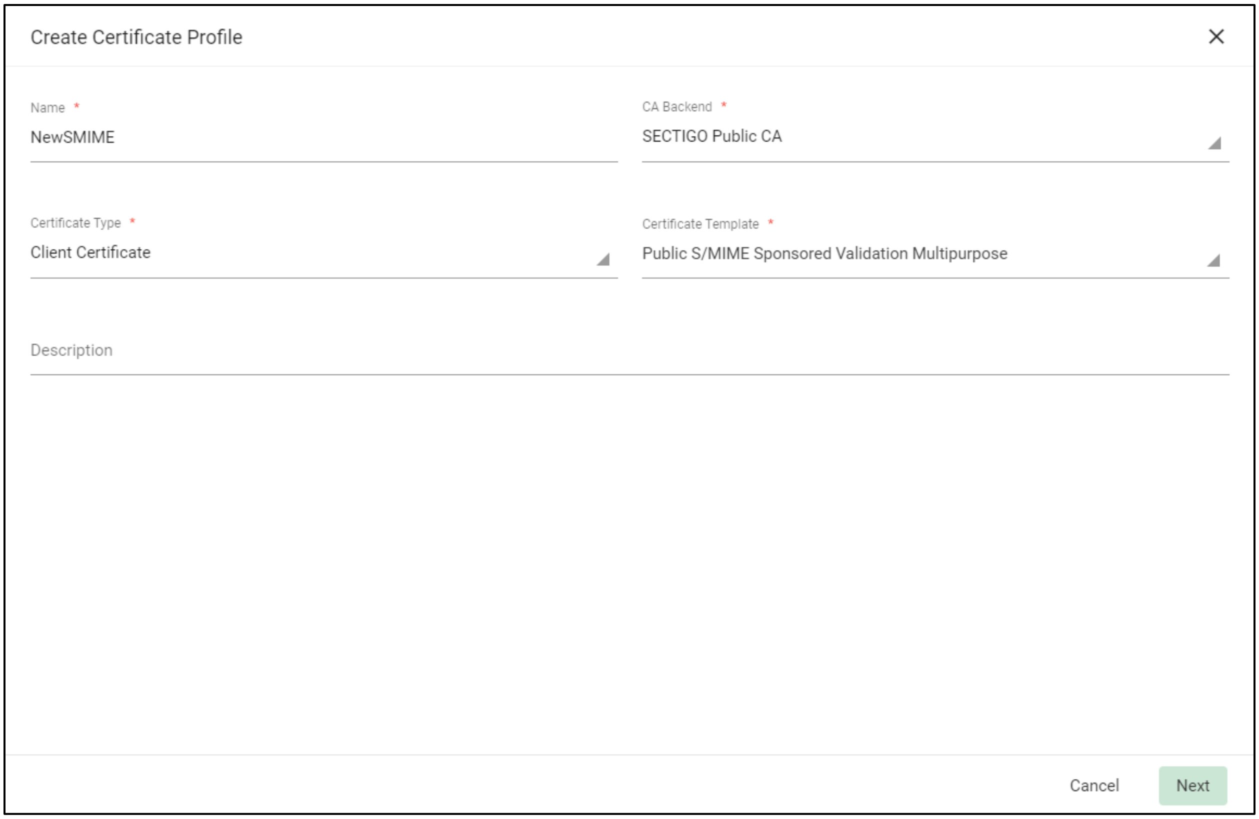
3.2 Create a certificate profile for client certificates

To add or modify a certificate profile, do the following:

1. Navigate to Enrollment > Certificate Profiles.

2. To add a certificate profile, click the **Add** icon.

   The **Create Certificate Profile** dialog is displayed.



Create Certificate Profile

Name *
NewSMIME

CA Backend *
SECTIGO Public CA

Certificate Type *
Client Certificate

Certificate Template *
Public S/MIME Sponsored Validation Multipurpose

Description

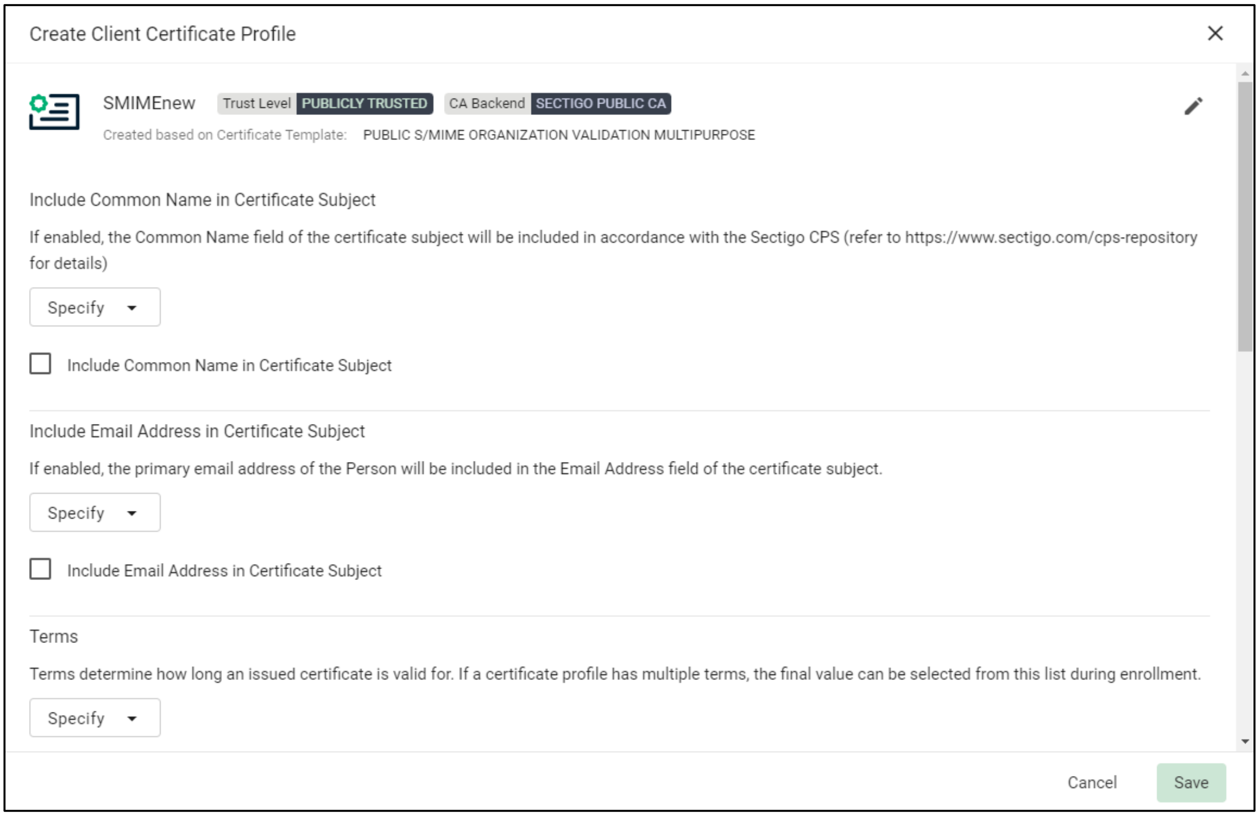
3. Complete the certificate profile fields, referring to this table.

Field	Description
Name	The name of the certificate profile
CA Backend	The backend from which certificates using this profile are enrolled
Certificate Type	The type of certificate that can be issued using this certificate profile (Client Certificate, SSL, Code Signing, or Device Certificate).
Certificate Template	The template controls the certificate policies as set by Sectigo. The features that can be customized are determined by the template and will vary depending on which template is selected. For more information on the templates available to you, contact your Sectigo account manager.
Description	A description of the profile that is shown during enrollment if the enrollment method has UI.

4. In the CA Backend field, select Sectigo Public CA.

5. Select **Client Certificate** for the certificate type.

6. Select one of the S/MIME certificate templates:
   - Public S/MIME Organization Validation Multipurpose
   - Public S/MIME Sponsored Validation Multipurpose
7. Click **Next**.



Create Client Certificate Profile

SMIMEnew Trust Level PUBLICLY TRUSTED CA Backend SECTIGO PUBLIC CA

Created based on Certificate Template: PUBLIC S/MIME ORGANIZATION VALIDATION MULTIPURPOSE

Include Common Name in Certificate Subject

If enabled, the Common Name field of the certificate subject will be included in accordance with the Sectigo CPS (refer to https://www.sectigo.com/cps-repository for details)

Specify ▾

□ Include Common Name in Certificate Subject

Include Email Address in Certificate Subject

If enabled, the primary email address of the Person will be included in the Email Address field of the certificate subject.

Specify ▾

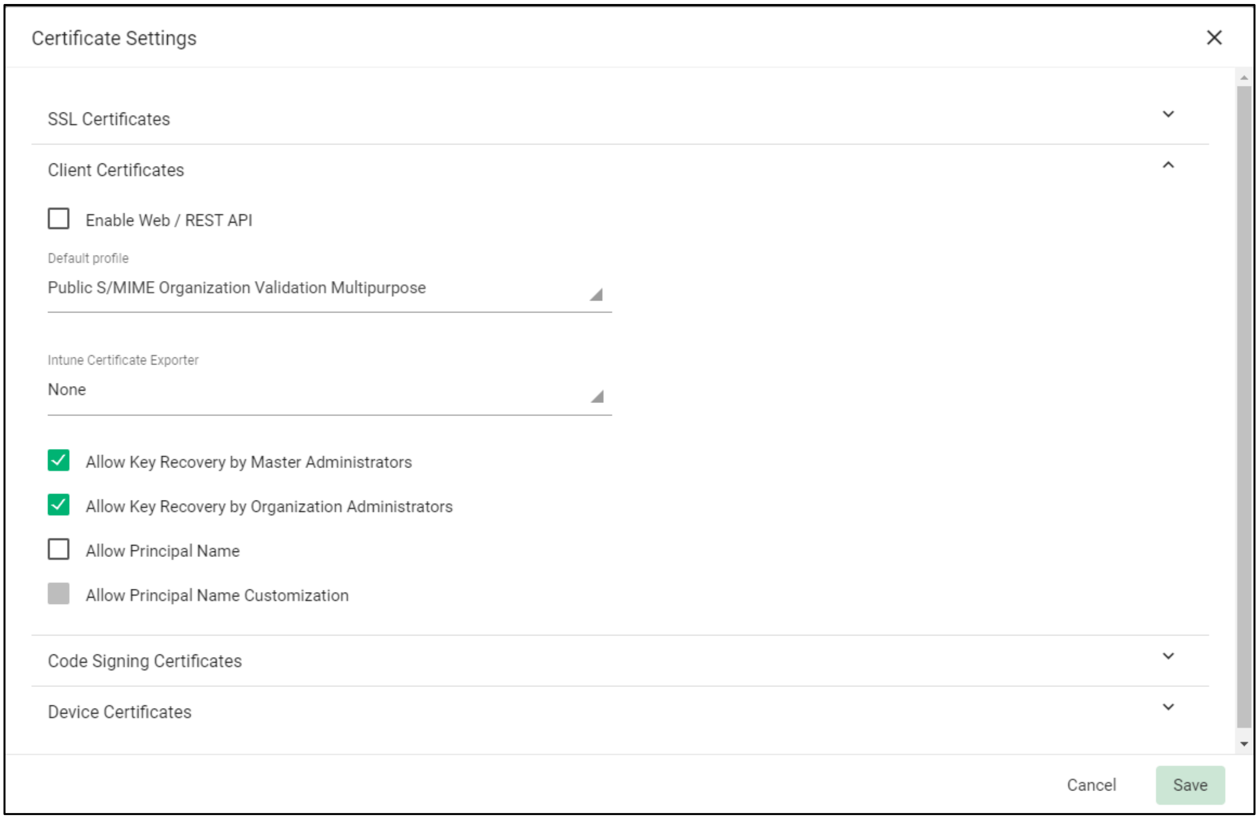
□ Include Email Address in Certificate Subject

Terms

Terms determine how long an issued certificate is valid for. If a certificate profile has multiple terms, the final value can be selected from this list during enrollment.

Specify ▾

8. Complete the client certificate profile options:
   - **Include Common Name in Certificate Subject** – If enabled, the Common Name of the certificate subject will be included.
   - **Include Email Address in Certificate Subject** – If enabled, the primary email address of the Person will be included in the Email Address field of the certificate subject.
   - **Terms** – The term for the S/MIME certificates can be either 1 or 2 years.
   - **Allowed Key Types** – Determines what public key algorithms can be used.
   - **Auto Revoke** – If enabled, the old certificates will be revoked when the maximum number of valid certificates is reached. By default, the maximum amount is 1. Contact Sectigo Support if you need a different amount.
9. Click **Save**.



Certificate Settings

SSL Certificates

Client Certificates

☐ Enable Web / REST API

Default profile: Public S/MIME Organization Validation Multipurpose

Intune Certificate Exporter: None

☑ Allow Key Recovery by Master Administrators

☑ Allow Key Recovery by Organization Administrators

☐ Allow Principal Name

☐ Allow Principal Name Customization

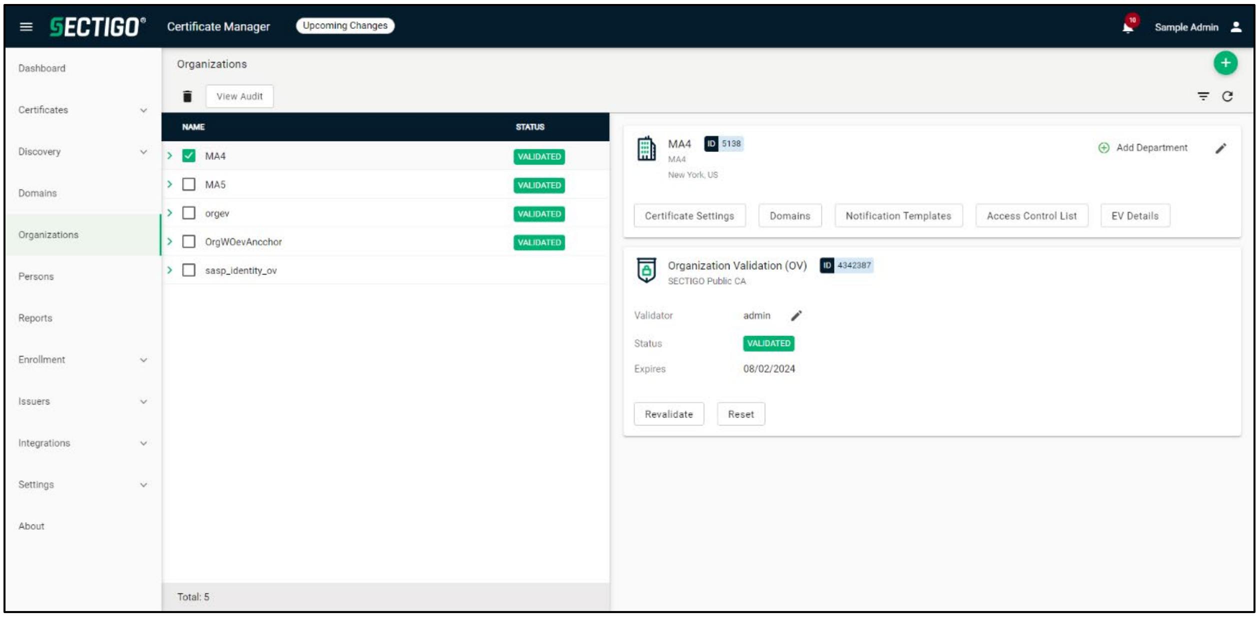
Code Signing Certificates

Device Certificates

3.3 Organization validation

With the new S/MIME baseline requirements, the existing organization validations are not sufficient for the new validation rules. After deployment of SCM 23.8, organizations must be revalidated manually before the new client certificate profiles can be used.

SCM will enforce prevalidation on the new S/MIME requests and only allow requests when the organization is correctly validated.



Organizations

NAME	STATUS
☑ MA4	VALIDATED
□ MA5	VALIDATED
□ orgev	VALIDATED
□ OrgWOevAncchor	VALIDATED
□ sasp_identity_ov	

Total: 5

MA4 ID 5138
MA4
New York, US

Organization Validation (OV) ID 4342387
SECTIGO Public CA

Validator admin

Status VALIDATED

Expires 08/02/2024

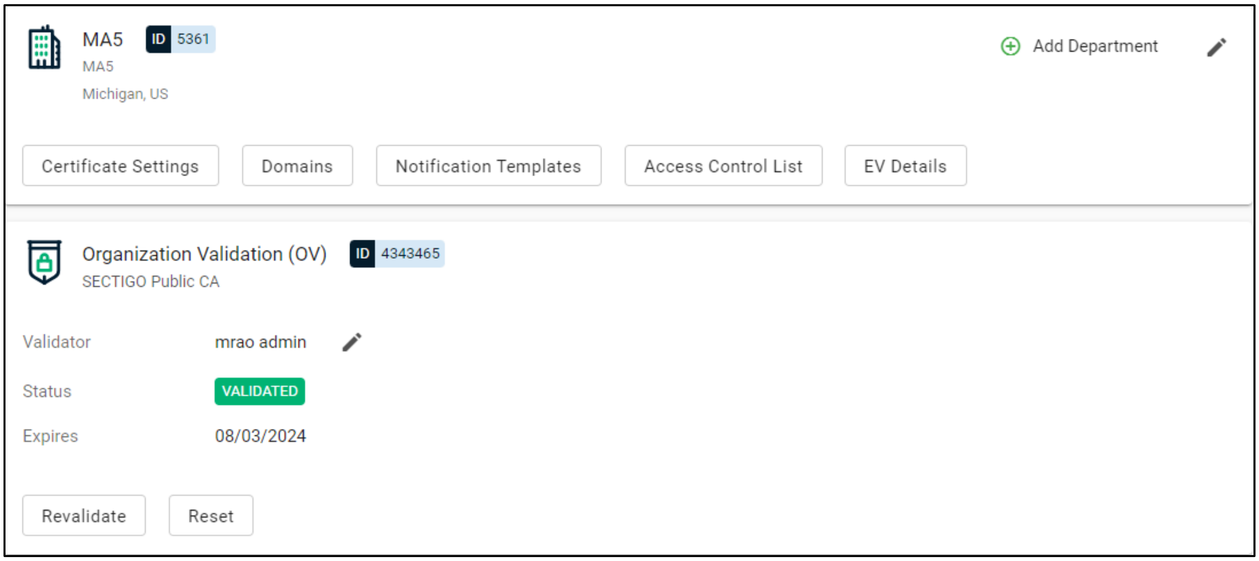
The badge on organization validation cards will now be showing “ID” if the current validation is also compliant with the S/MIME Baseline Requirements. If the organization has not been revalidated yet, the badge shows “Anchor” and is only appropriate for public OV SSL issuance.

3.3.1 Organization revalidation

All organizations managing client certificates must be revalidated manually to start using new client certificate profiles.

To revalidate the organization:

1. Navigate to **Organizations** and select the organization to be revalidated.
2. Click Revalidate.



MA5 ID 5361
MA5
Michigan, US

Organization Validation (OV) ID 4343465
SECTIGO Public CA

Validator mrao admin

Status VALIDATED

Expires 08/03/2024

NOTE: Until validation is completed, enrollment of OV certificates will not be available from Sectigo Public CA backend.

Once the revalidation is completed, the status becomes **Validated**.

3.3.2 Background revalidation

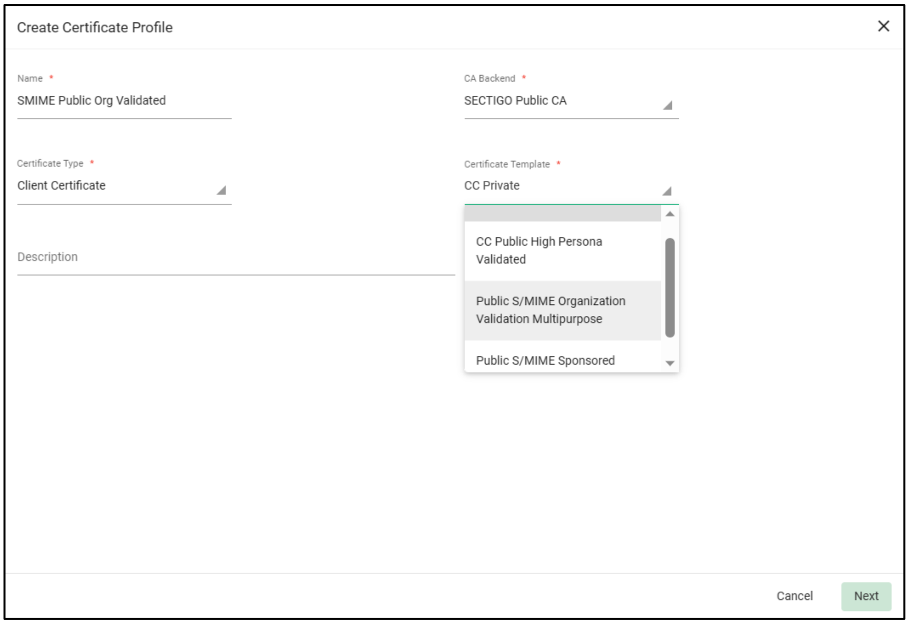
The background revalidations of organizations which are not completed at the time of SCM 23.8 release will be terminated and will need to be initiated manually.

We have added the ability for MRAO administrators to reset organization validation which allows them to cancel a pending validation or revoke a valid one.

We have added a badge on the organization validation card that shows renewal details (status and order number) when background validation is started.

3.4 New certificate profile creation

1. Log in to SCM.
2. Navigate to **Enrollment > Certificate Profile**.
3. Click the **Add** icon to add a new profile based on the S/MIME Global Templates.
4. Enter values for
   - Name
   - Certificate type: **Client Certificate**
   - CA backend: **Sectigo Public CA**
   - **Client Profile Certificate Template**



Create Certificate Profile

Name * SMIME Public Org Validated

CA Backend * SECTIGO Public CA

Certificate Type * Client Certificate

Certificate Template * CC Private

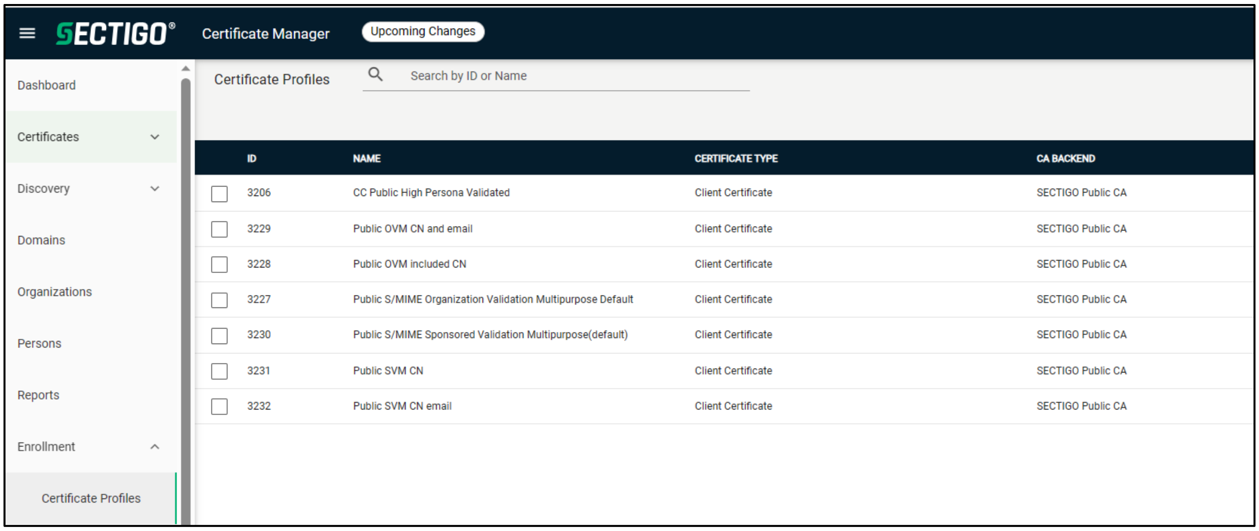
Description

CC Public High Persona Validated
Public S/MIME Organization Validation Multipurpose
Public S/MIME Sponsored
Cancel
Next

5. Click **Next** to configure details for the certificate.

6. Click **Save**.

A new profile for the S/MIME certificate template is created which can be used with the enrollment form for certificate issuance.



	ID	NAME	CERTIFICATE TYPE	CA BACKEND
□	3206	CC Public High Persona Validated	Client Certificate	SECTIGO Public CA
□	3229	Public OVM CN and email	Client Certificate	SECTIGO Public CA
□	3228	Public OVM included CN	Client Certificate	SECTIGO Public CA
□	3227	Public S/MIME Organization Validation Multipurpose Default	Client Certificate	SECTIGO Public CA
□	3230	Public S/MIME Sponsored Validation Multipurpose(default)	Client Certificate	SECTIGO Public CA
□	3231	Public SVM CN	Client Certificate	SECTIGO Public CA
□	3232	Public SVM CN email	Client Certificate	SECTIGO Public CA