

**IATA 1R CMS**  
**ONE Record Credentials Management**

**Web Console User Guide**

Date: June 2020

Version: 0.1

Authors: WISeKey SA

**Table of contents**

[1 Introduction 4](#_Toc43823253)

[1.1 Getting access to the platform verification 4](#_Toc43823254)

[2 Administrator Management 5](#_Toc43823255)

[2.1 Admin Profile 5](#_Toc43823256)

[2.2 Admin creation 6](#_Toc43823257)

[3 Subscribers Management 8](#_Toc43823258)

[3.1 Subscriber creation 8](#_Toc43823259)

[3.2 Subscriber list 11](#_Toc43823260)

[3.3 Subscriber details 11](#_Toc43823261)

[3.4 Subscriber Edit page 12](#_Toc43823262)

[3.5 Subscriber Homepage 13](#_Toc43823263)

[4 ONE Record IDs Management 14](#_Toc43823264)

[4.1 Register ONE Record ID 14](#_Toc43823265)

[4.1.1 Create a new ONE Record ID 14](#_Toc43823266)

[4.1.2 ONE Record ID List page 17](#_Toc43823267)

[4.1.3 ONE Record ID details page 17](#_Toc43823268)

[4.1.4 ONE Record ID edit page 18](#_Toc43823269)

[4.1.5 ONE Record ID delete page 19](#_Toc43823270)

[4.2 Approve/Reject a registered ONE Record ID 20](#_Toc43823271)

[4.2.1 Approve a registered ONE Record ID 20](#_Toc43823272)

[4.2.2 Reject a registered ONE Recored ID 21](#_Toc43823273)

[5 Certificate Management 24](#_Toc43823274)

[5.1 Client Certificate 24](#_Toc43823275)

[5.1.1 Creating a Client Certificate request 24](#_Toc43823276)

[5.1.2 Client Certificate Request List Page 27](#_Toc43823277)

[5.1.3 Client Certificate Request Detail page 28](#_Toc43823278)

[5.1.4 Delete a client certificate request 30](#_Toc43823279)

[5.1.5 Approve a Client Certificate Request 31](#_Toc43823280)

[5.1.6 Reject a Client Certificate Request 32](#_Toc43823281)

[5.1.7 Download an Issued Client Certificate 34](#_Toc43823282)

[5.1.8 Revoke a Client Certiifcate 35](#_Toc43823283)

[5.2 Server Certificate 36](#_Toc43823284)

[5.2.1 Domain Validation 36](#_Toc43823285)

[5.2.2 Create a Server Certificate Request 38](#_Toc43823286)

[5.2.3 Server Certificate request list page 40](#_Toc43823287)

[5.2.4 Server Certificate Request Detail page 41](#_Toc43823288)

[5.2.5 Delete a Server certificate request 42](#_Toc43823289)

[5.2.6 Approve a Server Certificate Request 43](#_Toc43823290)

[5.2.7 Reject a Server Certificate Request 45](#_Toc43823291)

[5.2.8 Download an Issued Server Certificate 47](#_Toc43823292)

[5.2.9 Revoke a Server Certificate 47](#_Toc43823293)

[6 User Profile Management 49](#_Toc43823294)

[6.1 Update Profile 49](#_Toc43823295)

[6.2 Reset password 50](#_Toc43823296)

# Introduction

The **IATA 1R CMS** provides these Components and Features:

* IATA 1R Web portal:
  + Provides a GUI, accessible with authorized login credentials
  + Implements different management capabilities per user role: Admin, and Subscriber
  + Implement various type of Subscriber role: Carrier, Customs, Forwarder, Ground Handler, RFS, Shipper, IT Provider…
  + Allows managing all entities:
    - Administrators and Subscribers accounts
    - “ONE Record IDs” and request management.
    - Certificate management: Client certificates, Server certificates.
    - Managing activity log
* IATA 1R API
  + Allows to interact with the IATA 1R via REST API
* Definitions
* ONE Record ID: URI that refers to a ONE Record identifier from the Internet of Logistics, with the form https://<FQDN>/<COMPANYID>.
* ONE Record Server: Application that accepts ONE Record API requests from a client.
* ONE Record Client: Application that sends ONE Record API requests to a server.
* IAP: Identity and Authentication Provider.

## Getting access to the platform

The portal implements the following user roles:

* **Admin**: full access control to create Administrators, manage all Subscribers, approve/reject all pending registered One Record IDs, approve/reject all pending client/server certificate requests, managing all issued certificates (download, revoke), Audit log…
* **Subscriber:** Managing their own One Record IDs (register/view/update/delete pending 1R IDs, view/update approved 1R IDs), Create/Delete their own certificate request (client, server), managing their own issued certificates (download, revoke).

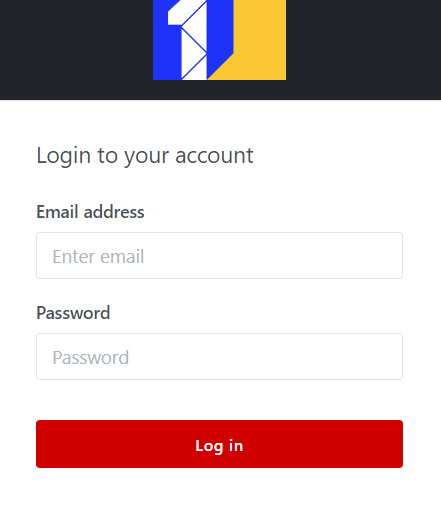
All accesses to the platform are authenticated at least with username and password, and optionally with a digital certificate as strong authentication method.

Please ask IATA for your initial credentials to connect to the platform.

The demo environment is available for tests in the URL:

<https://iatacms.wisekeydemo.com/web>

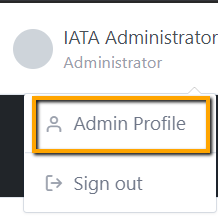
Login with Username/Password:



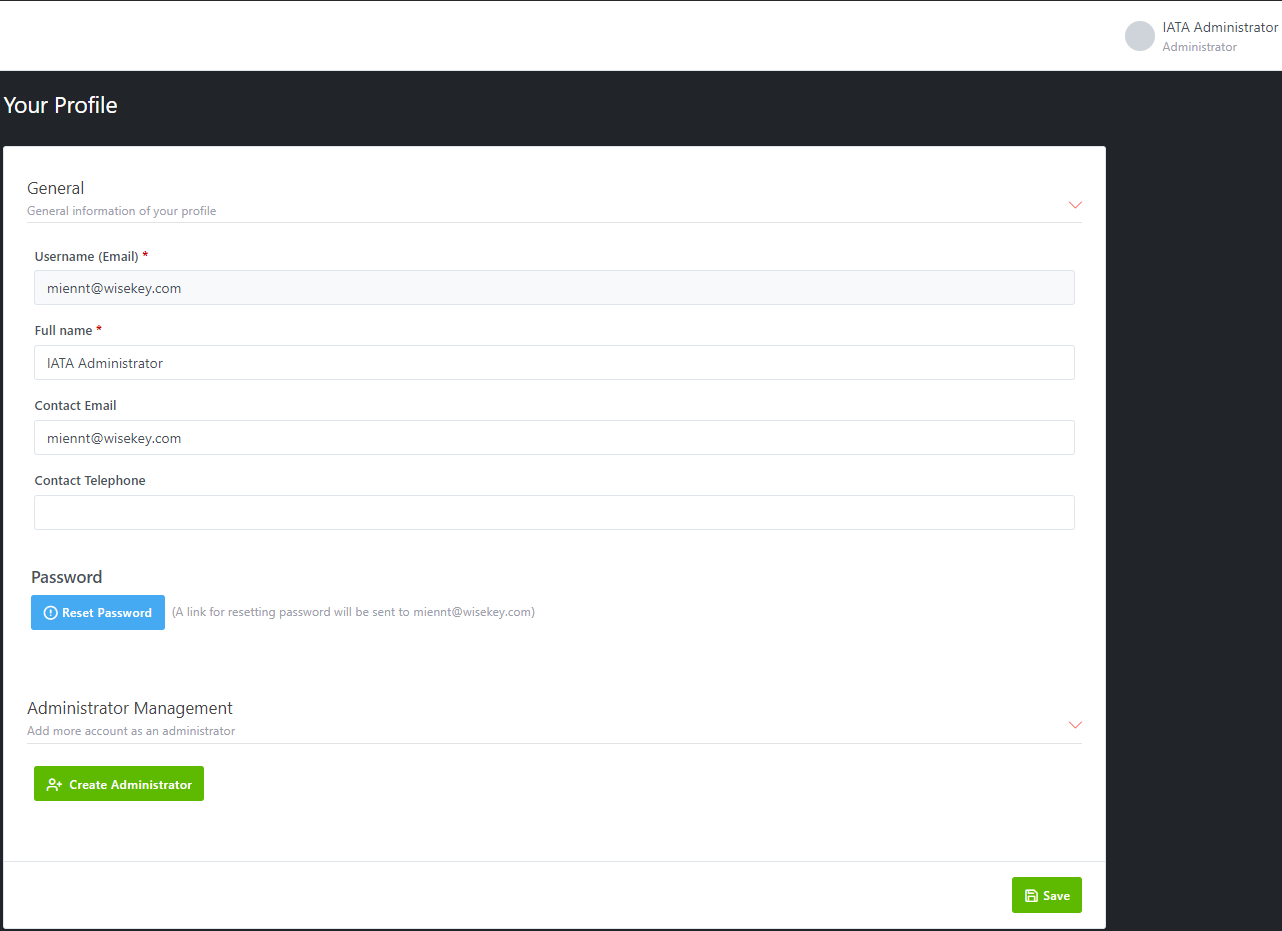
# Administrator Management

## Admin Profile

Administrator can update his profile by clicking on the admin avatar then select “Admin Profile”:



Admin Profile detail:

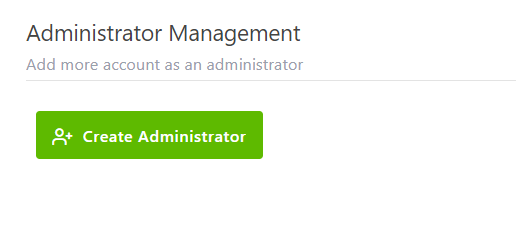


In Admin profile screen, admin can:

* Edit all information EXCEPT username (Email) field then click on SAVE to update the changes.
* Reset Password: a link for resetting password will be sent to the user Email
* Create Administrator accounts

## Admin creation

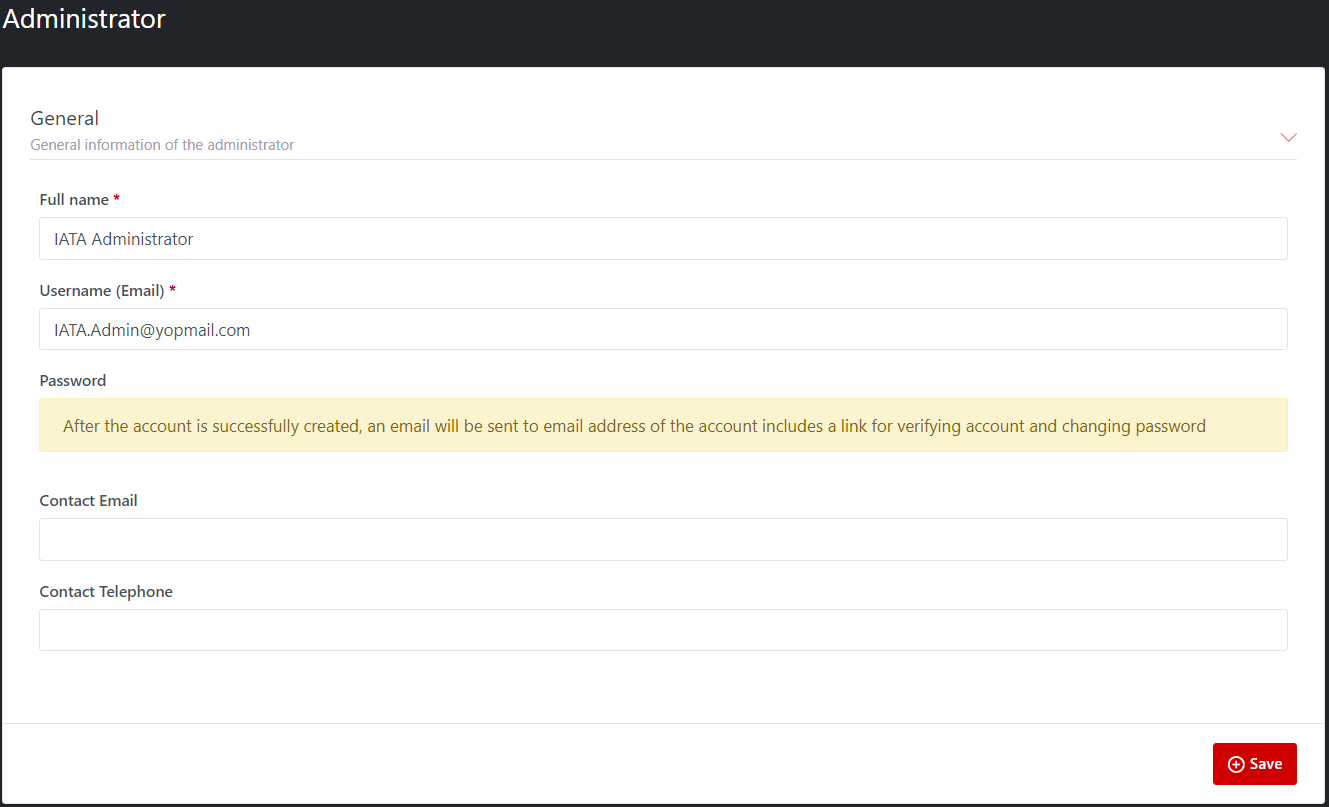
In Admin Profile, you can add more account as Administrator by clicking on **Create Administrator** button. It will bring you to Administrator creation page



Steps to create Administrator:

**Step 1:** Fill all the required fields:

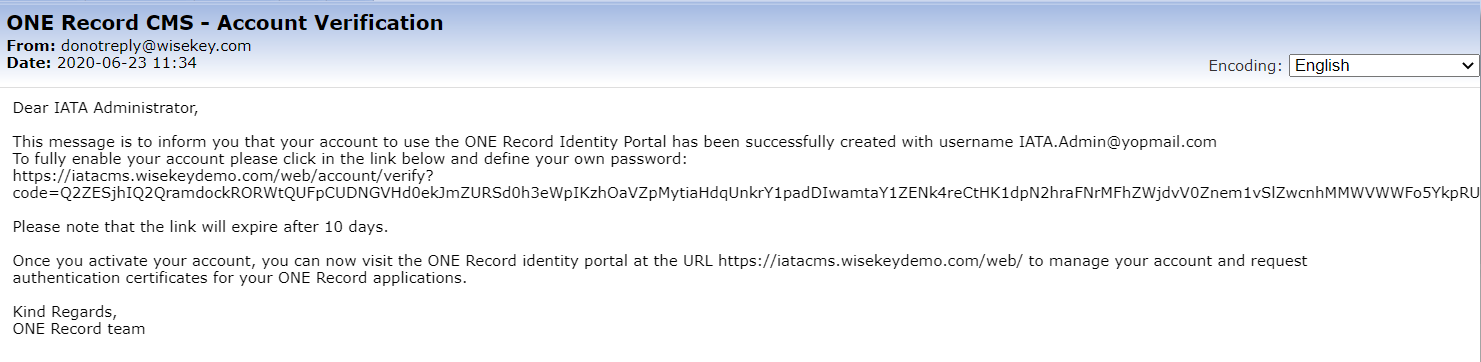
* Full name \*: it is a required field
* Username (Email) \*: it is a required field and it is unique, does not allow duplicate emails
* Password: After the account is successfully created, an email will be sent to username email address of the account includes a link for verifying account and changing password
* Contact Email: Optional
* Contact Telephone: Optional



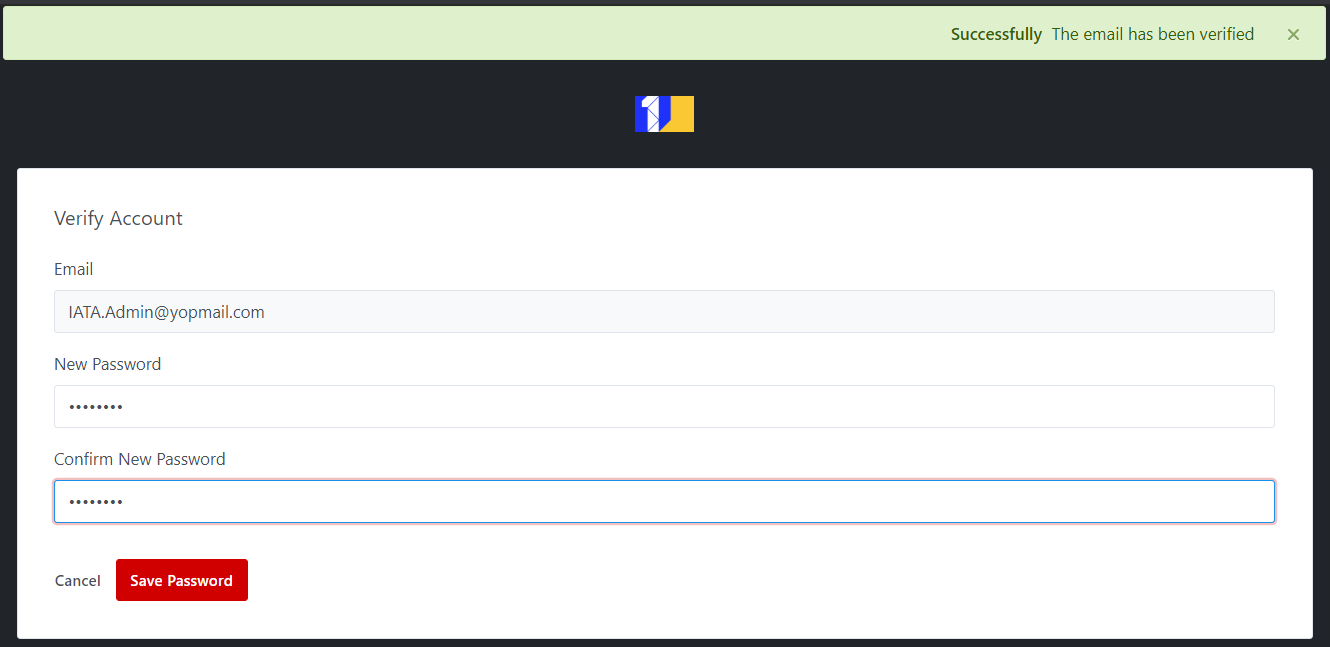
**Step 2:** Click on SAVE button to complete administrator account creation

**Step 3:** After account is created successfully, a notification email about verify account and change password will be sent to username (Email) address.





**Step 4:** New Administrator creation verify email and click on link to change password.



After the password is changed successfully, the new administrator can login with his admin account, view Admin Profile and update Admin profile as well as Reset Password if needed.

# Subscribers Management

Access rules:

* **Admin:** can create and manage Subscribers.

***Please note:***

* *When a user is created successfully, an e-mail informing of his* ***username/password*** *will be sent to* ***username email*** *details.* ***This password must be changed at 1st time login****.*
* *Anytime the* ***Reset Password*** *button is clicked, an email containing the instructions to reset the password, including a temporary password will be sent to* ***username email****.* ***This password also must be changed after logged-in successfully****.*

## Subscriber creation

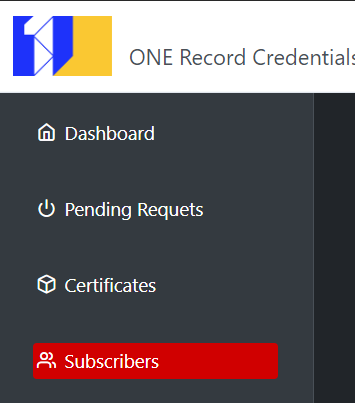
Subscribers can be created only by an IATA admin, by providing the following information:

* Entity Name
* Username (email address)
* Subscriber Role (Carrier, Customs, Forwarder, Ground Handler, RFS, Shipper, IT Provider)
* Supported Certificate Type: Server, Client, Server & Client
* Contact details: Name, Email, Telephone

When the administrator submits the subscriber details, an account is created and the subscriber is notified to the main email, receiving an invitation to activate the account and define the password.

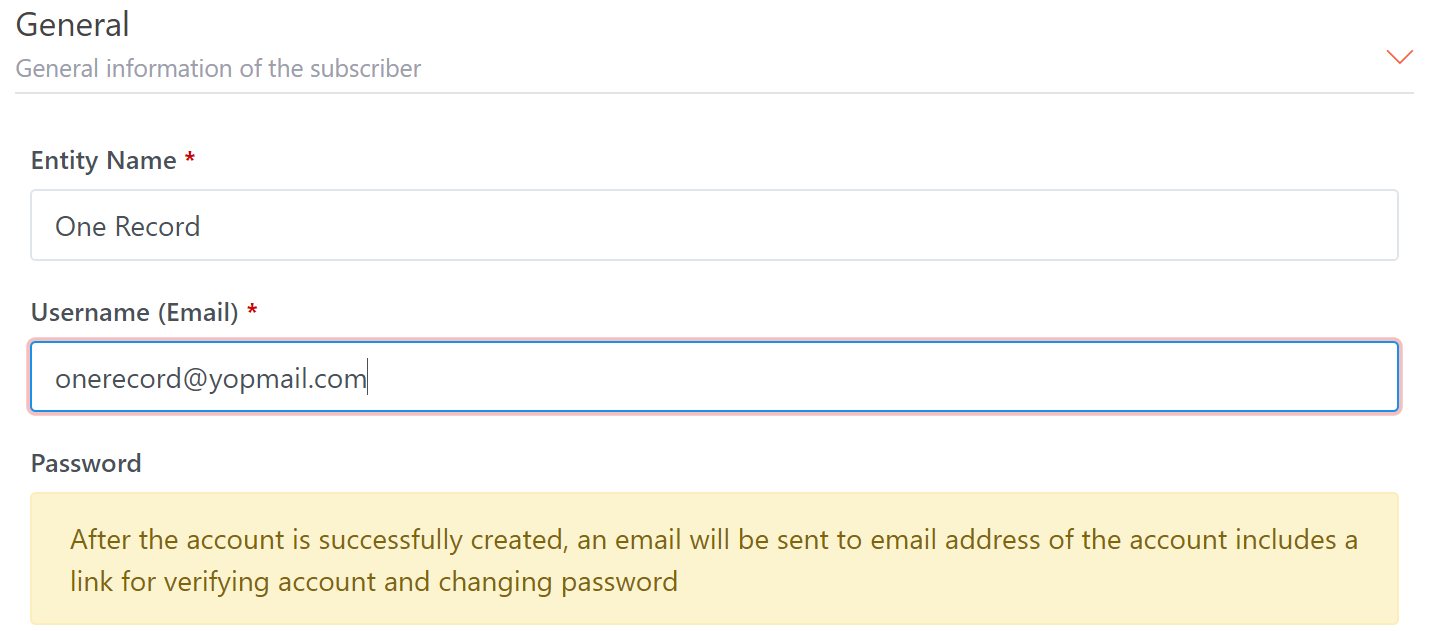
Here are steps to create a subscriber:

**Step 1:** Login as IATA Admin and open Subscribers from left menu

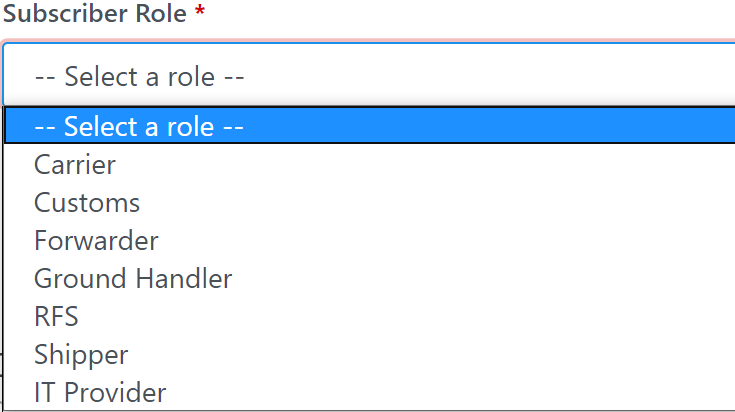


**Step 2:** Click on “New” button, and fill the all **required fields**, marked with the “\*” sign:

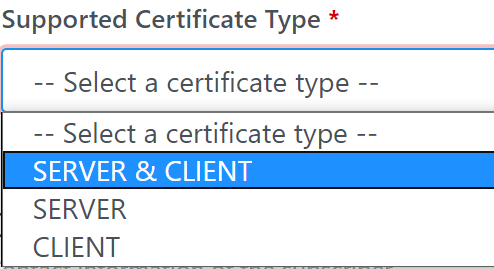
* **General**:
  + **Entity Name**
  + **Username** (must be a valid email address)



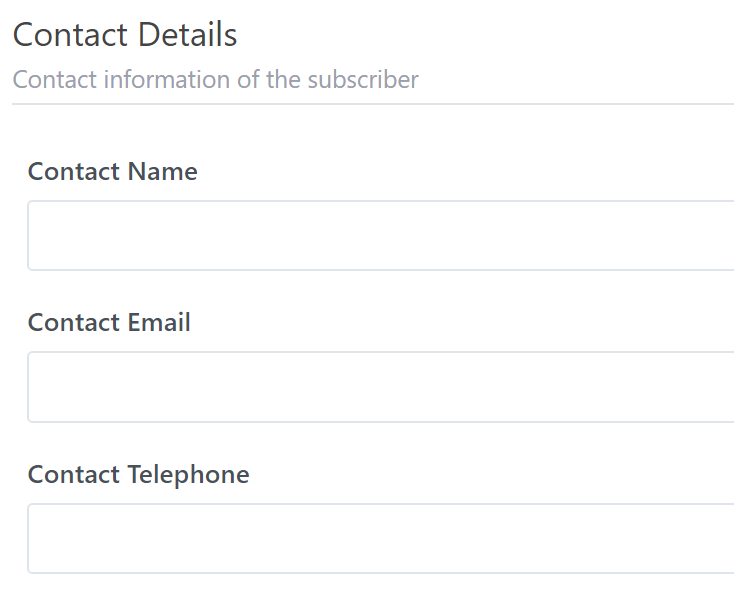
* + **Subscriber Role**: Select one from list (the options can vary subscriber type)



* + **Supported Certificate Type**: support 3 types: Client, Server, Server & Client.



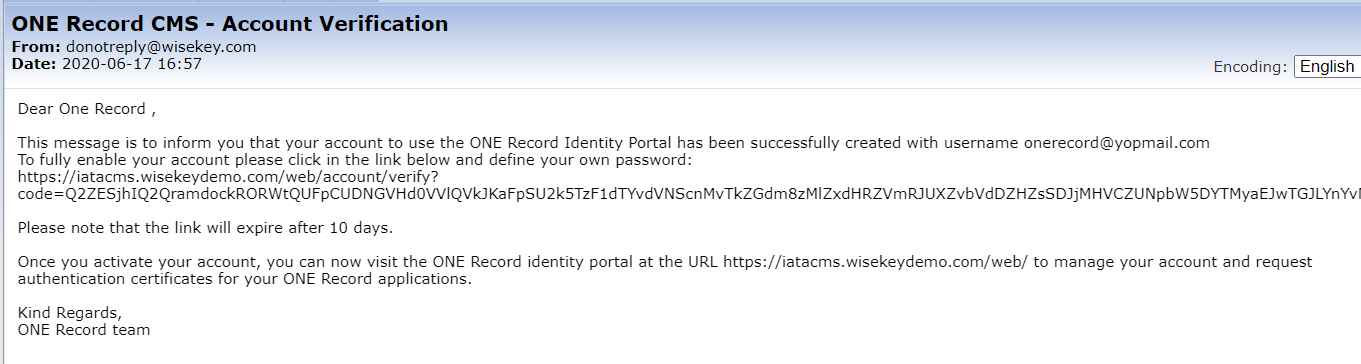
* **Contact details**: Contact Name, Contact Email, Contact Telephone (Optional). Please note that the contact email will be the preferred contact address to deliver notifications to the user. If not used, the login username, which is also an email address, will be used



When all required fields are filled with valid data (name, email…), then click on the “Save” button. A message to inform the account verification email has been sent to your email address like this:

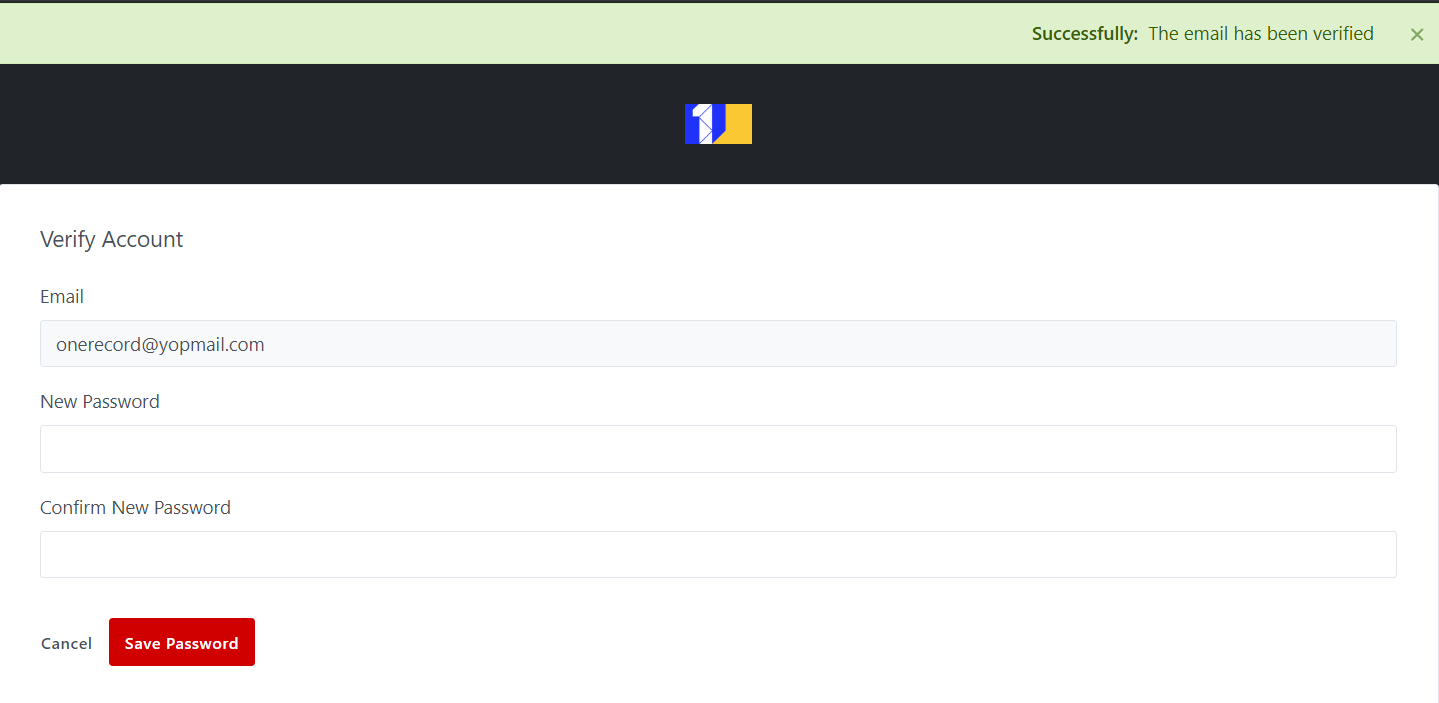


An account verification email message will be sent to the user containing his username and initial password, similar to this one:



***Important Note: please ensure your email server doesn’t filter out as “spam” the messages sent by the platform.***

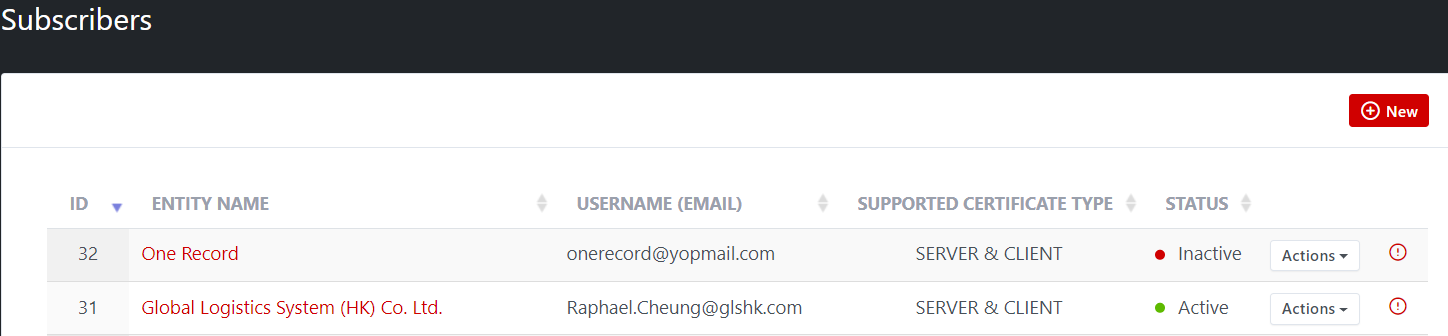
When subscriber click on the account verification link, the account will be verified, and user must change the password at 1st time:



## Subscriber list

All **subscribers** will be listed on the List page.

The “Action” option allows to: **Edit** users on list page. The “View” icon opens the subscriber Details page.



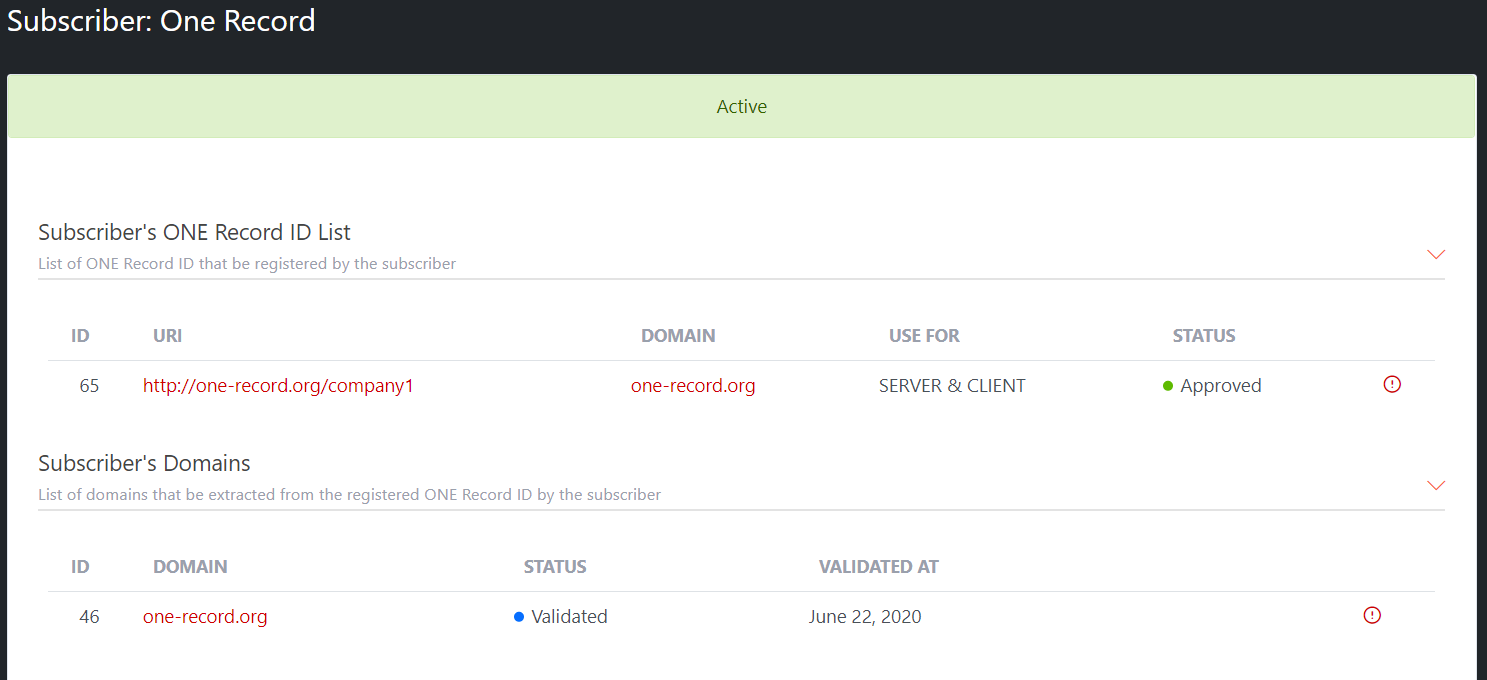
## Subscriber details

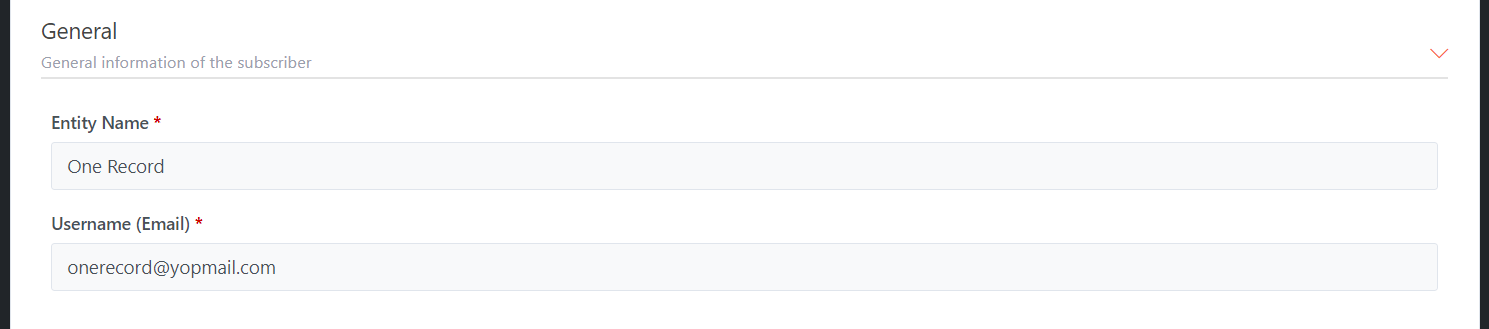
Show the current user STATUS (default is INACTIVE after subscriber account is created).

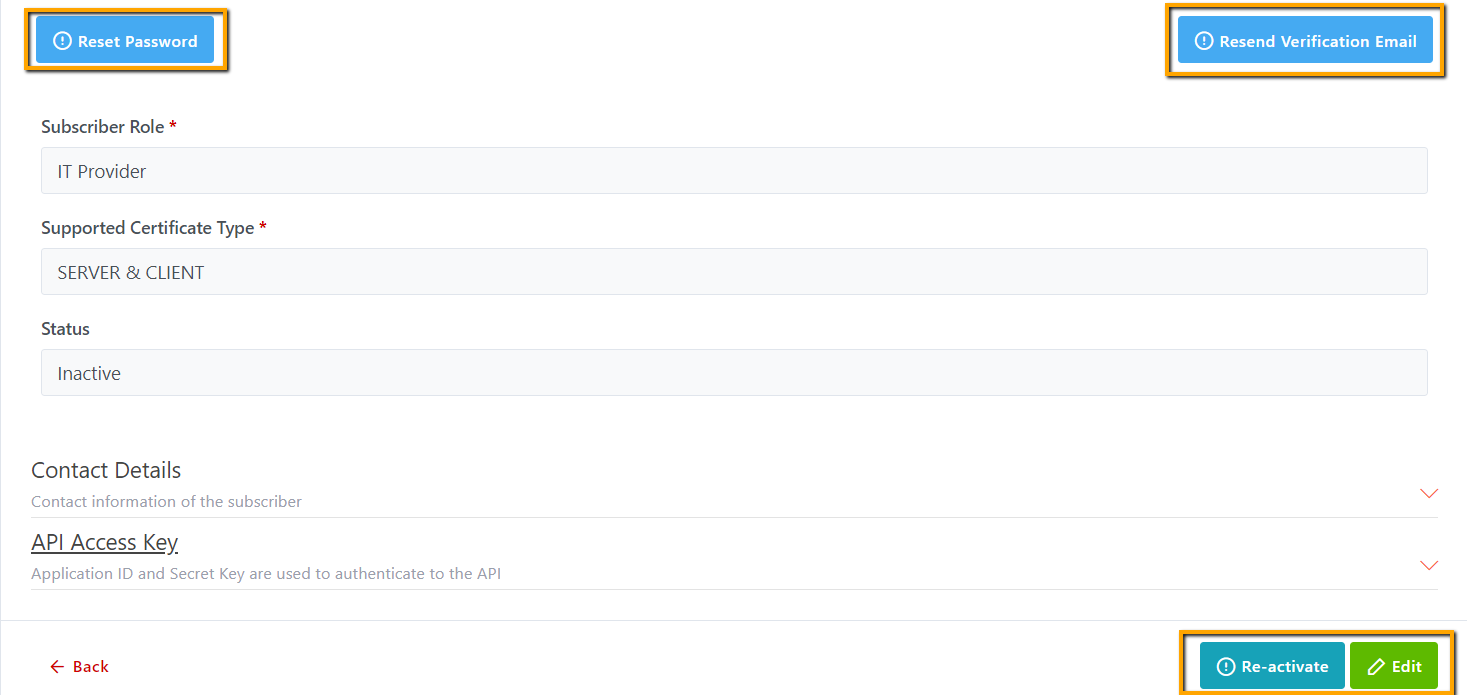
Show all Subscriber’s ONE Record ID list (pending/approved/rejected).

Show all Subscriber’s Domains with status and validated at information.

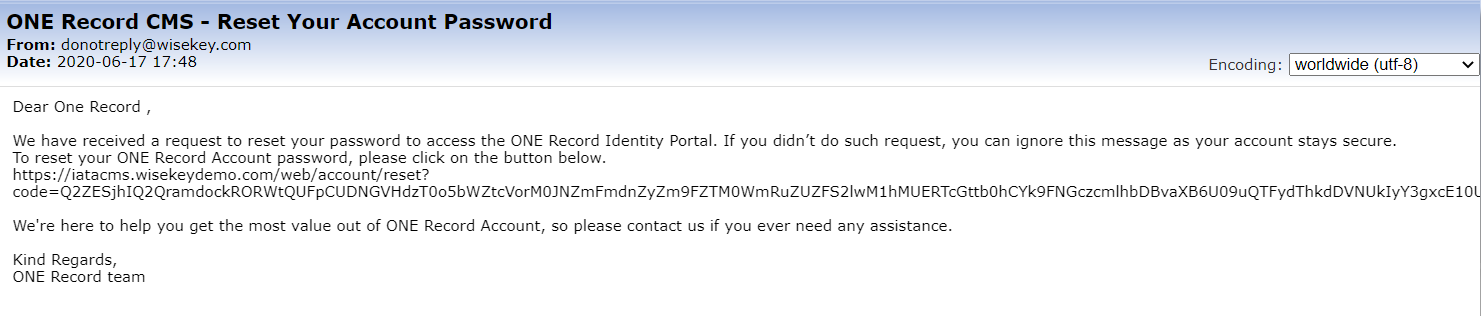
It’s possible to deactivate, re-activate, edit, reset password, and resend verification email using the related buttons available in this page.



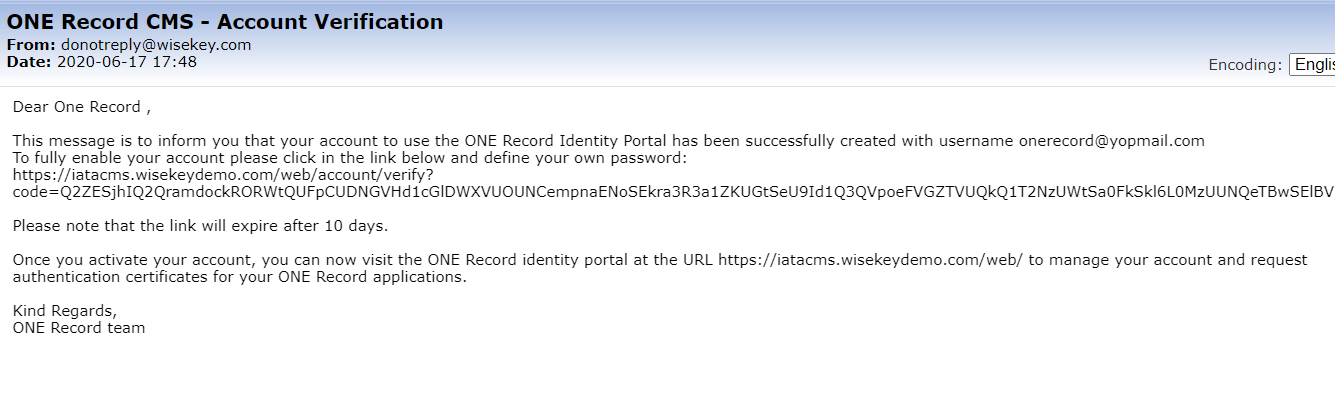




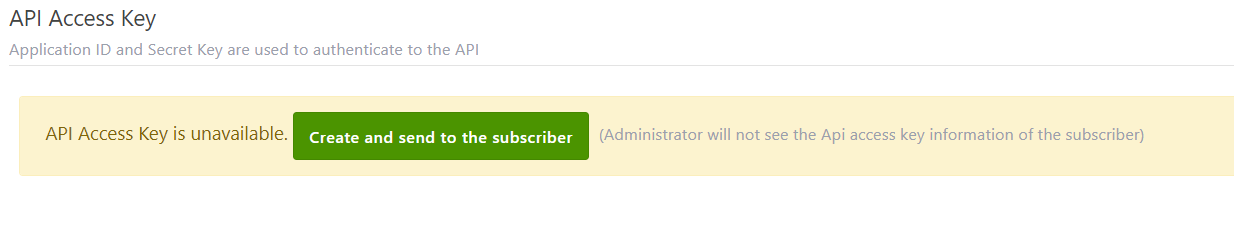
When using the “Reset Password” feature, the user will receive an email similar to this:



When using the “Resend Verification Email” feature, the user will receive an email similar to this:



In Subscriber detail page, can create and send API access key to subscriber so they can use 1R API



## Subscriber Edit page

Allows to edit all available fields EXCEPT ID, and the Username (Email).

## Subscriber Homepage

The user interface for the subscriber looks like the image below:

A screenshot of a cell phone

Description automatically generated

The subscriber can edit its profile information, create ONE Record ID and request certificates. An account can register multiple domains and ONE Record IDs.

# ONE Record IDs Management

## Register ONE Record ID

The **subscriber** must register one or more ONE Record IDs. Examples:

* https://servername.domain1.com/companyid1
* https://servername.domain1.com/companyid2
* https://servername2.domain1.com/companyid3
* https://servername.domain2.com/companyid4

### Create a new ONE Record ID

Steps detail to create a new ONE Record ID:

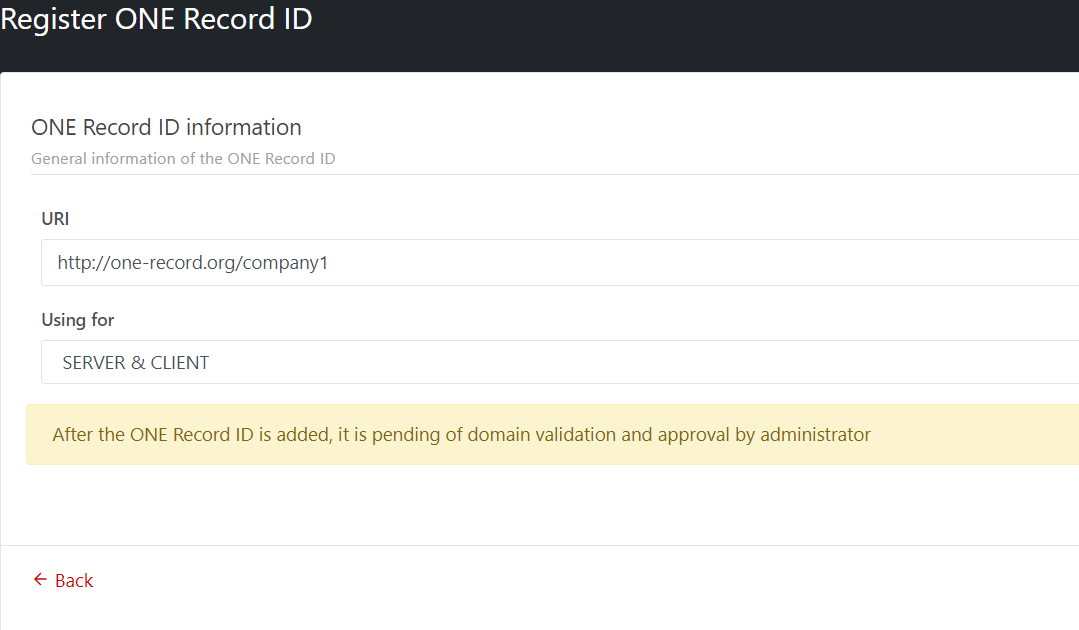
**Step 1**: Login as **Subscriber** then open ONE Record IDs from left menu.Then click on **Register ONE Record ID** button.

**Step 2:** Fill URI for General information of the ONE Record ID

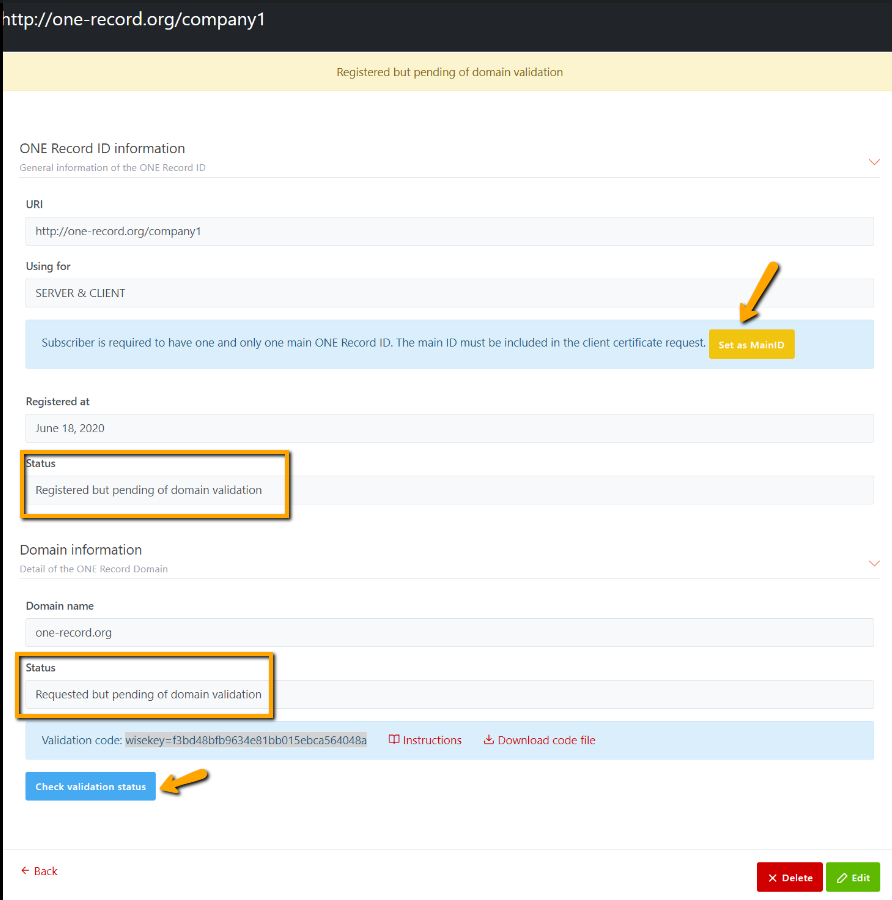
URI format is: <https://servername.domain1.com/companyid1>

For each URI the subscriber must specify if it will be used for client and/or server.

**Illustrative example:**



**Step 3**: After fill the URI and select client and/or server, click on SAVE to create a new ONE Record ID. A message will be shown to notify that “Successfully: ONE Record ID has been inserted successfully”

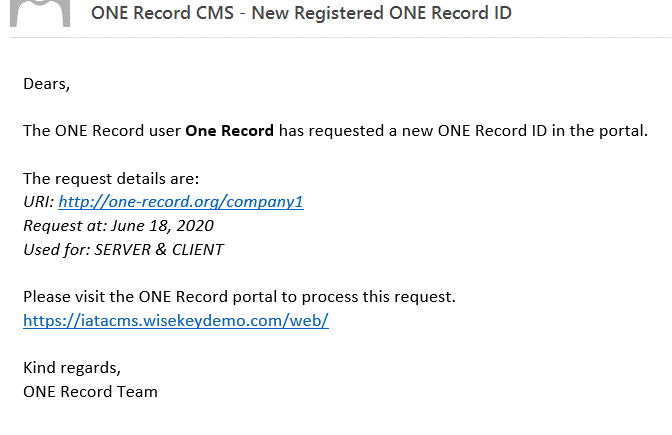


***Please note:***

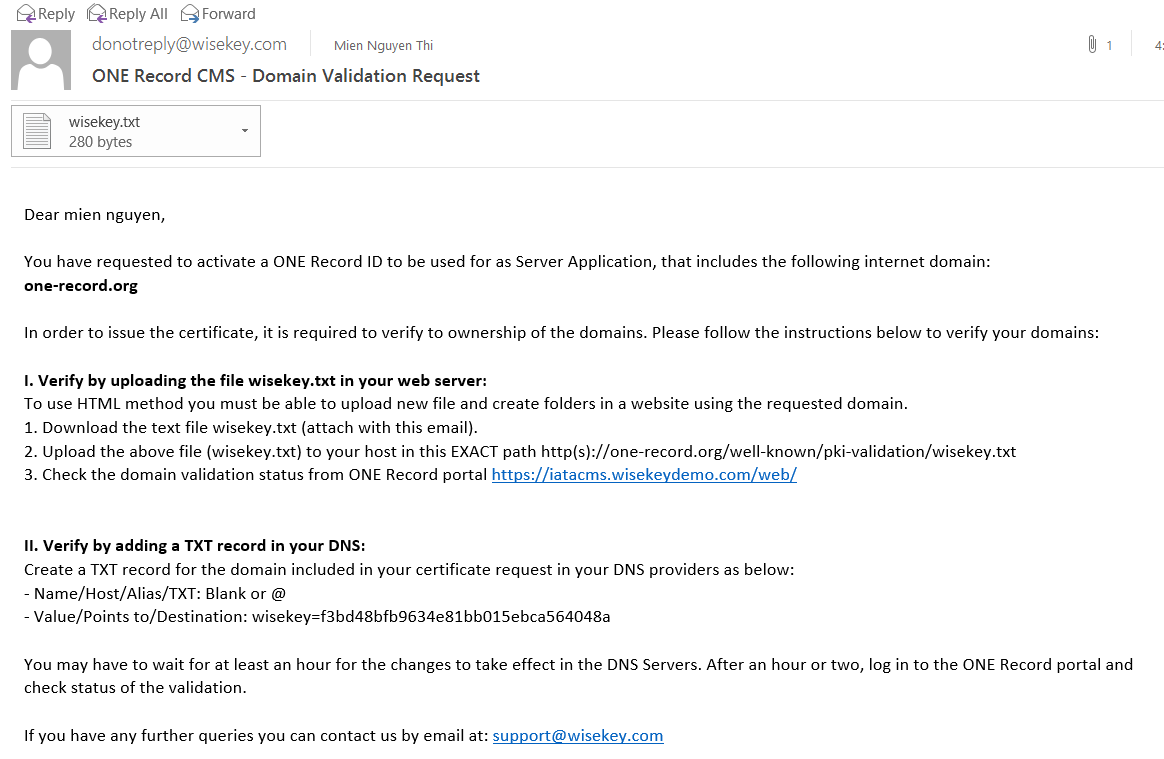
* ***Any new ONE Record ID need to be approved by IATA Admin (It is required before requesting a Client/Server certificate using the ID).***
* ***Domain is extracted from URI need to be validated to use for Server Certificate request***
* ***Each Subscriber has one and only one main ONE Record ID. The main ID must be included in the Client Certificate Request. Subscriber can select any ONE Record ID as main ID by clicking button [Set as Main ID]***

**Step 4**: A new ONE Record ID will be listed and shown in the ONE Record IDs List page of Subscriber, and it is also shown in Pending Request section in Dashboard of IATA admin, so that IATA admin can see all pending approval registered ONE Record ID.

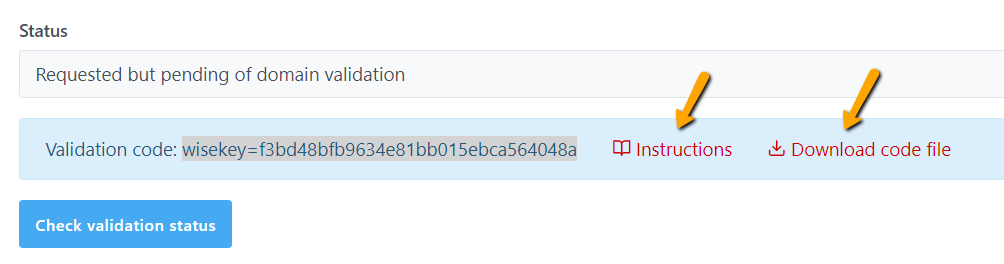
**Step 5:** Notification email about new registered ONE Record ID will be sent to IATA Admin to approve the request.



**Step 6:** If the new URI will be used for a server access and it includes a new internet domain, a notification email about Domain Validation request will be sent to Subscriber email so that he/she follows the instruction to make domain (extracted from URI) validated.



If Subscriber miss the instruction email, he/she can view instruction in ONE Record ID detail page and download code file for validating domain.

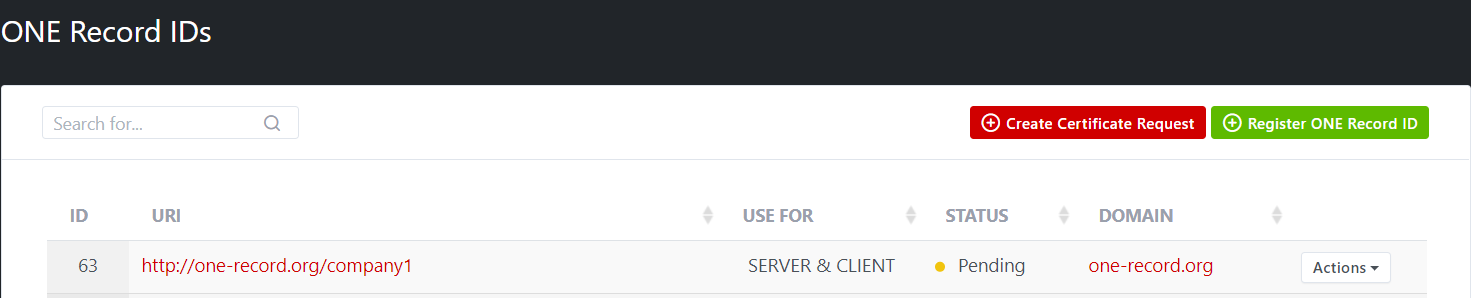


**IMPORTANT:** If a domain has been validated and the validation date is not expired then any subscriber created ONE Record IDs with that domain, the domain will be marked as Validated automatically.

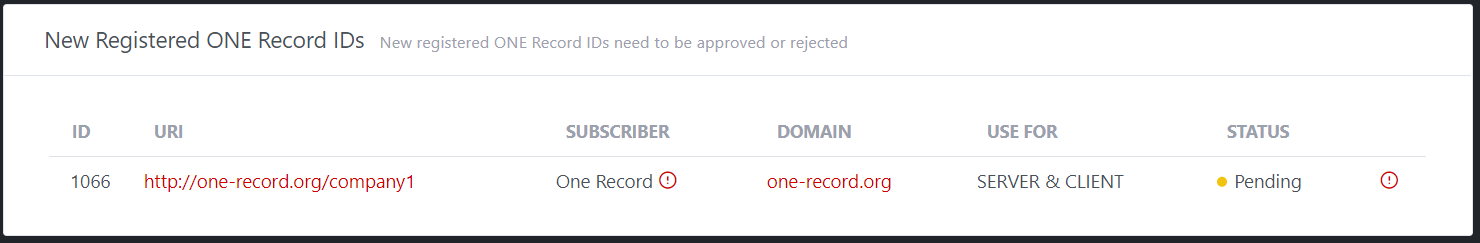
### ONE Record ID List page

**Subscriber**: All **ONE Record IDs** will be listed on the List page.

The “Action” option allows to: **Edit** ONE Record ID on list page. The “View” icon opens the ONE Record ID Details page:



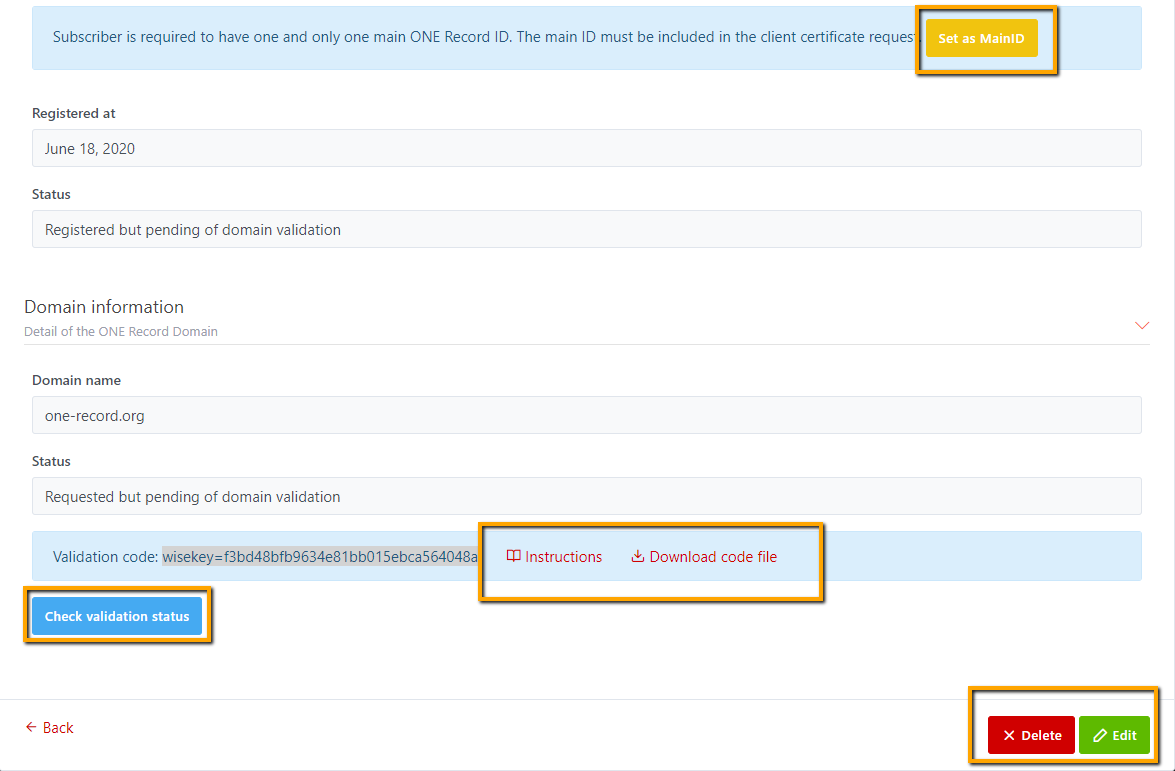
**IATA Admin**: pending approval registered ONE Record ID is listed in Dashboard page



### ONE Record ID details page

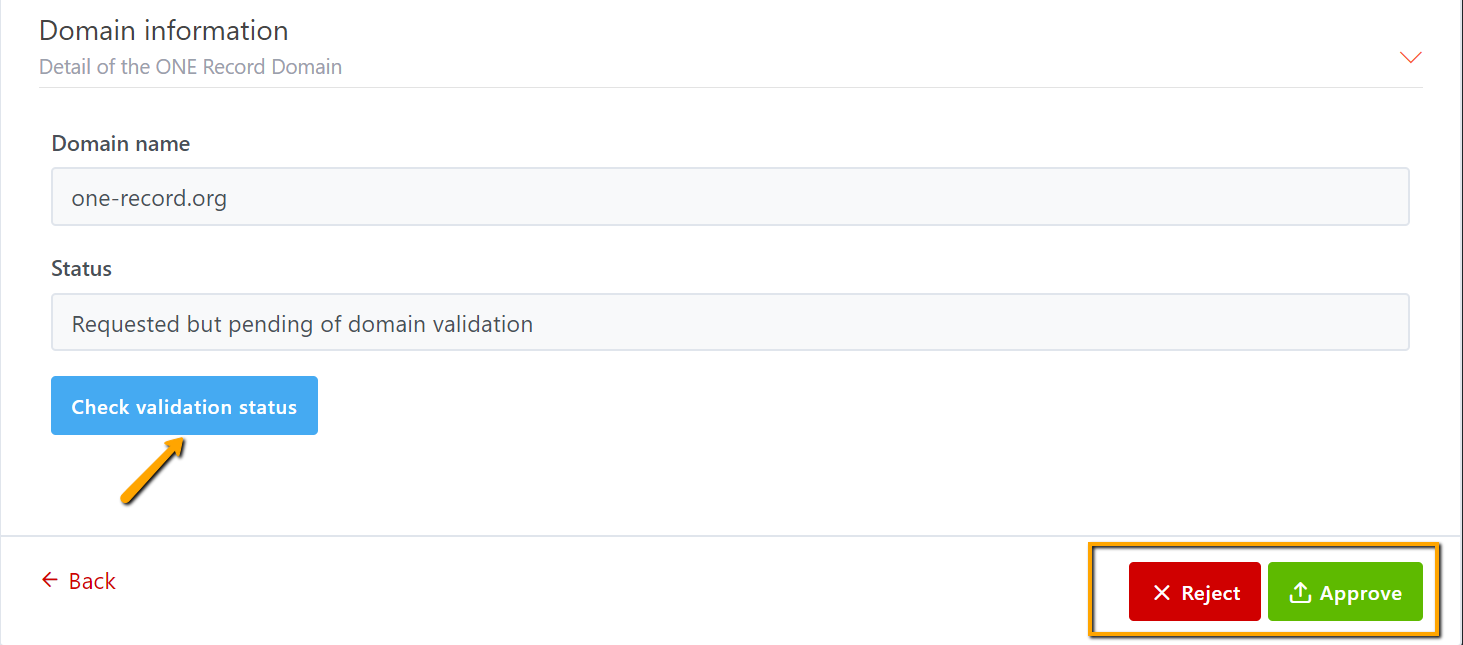
View page by **Subscriber**. The possible operations are:

* Set MainID
* Check Validation Status
* View Instructions and Download validation code file for validating domain.
* Delete
* Edit



For **IATA Admin**, view a pending ONE Record ID will have possible operations are:

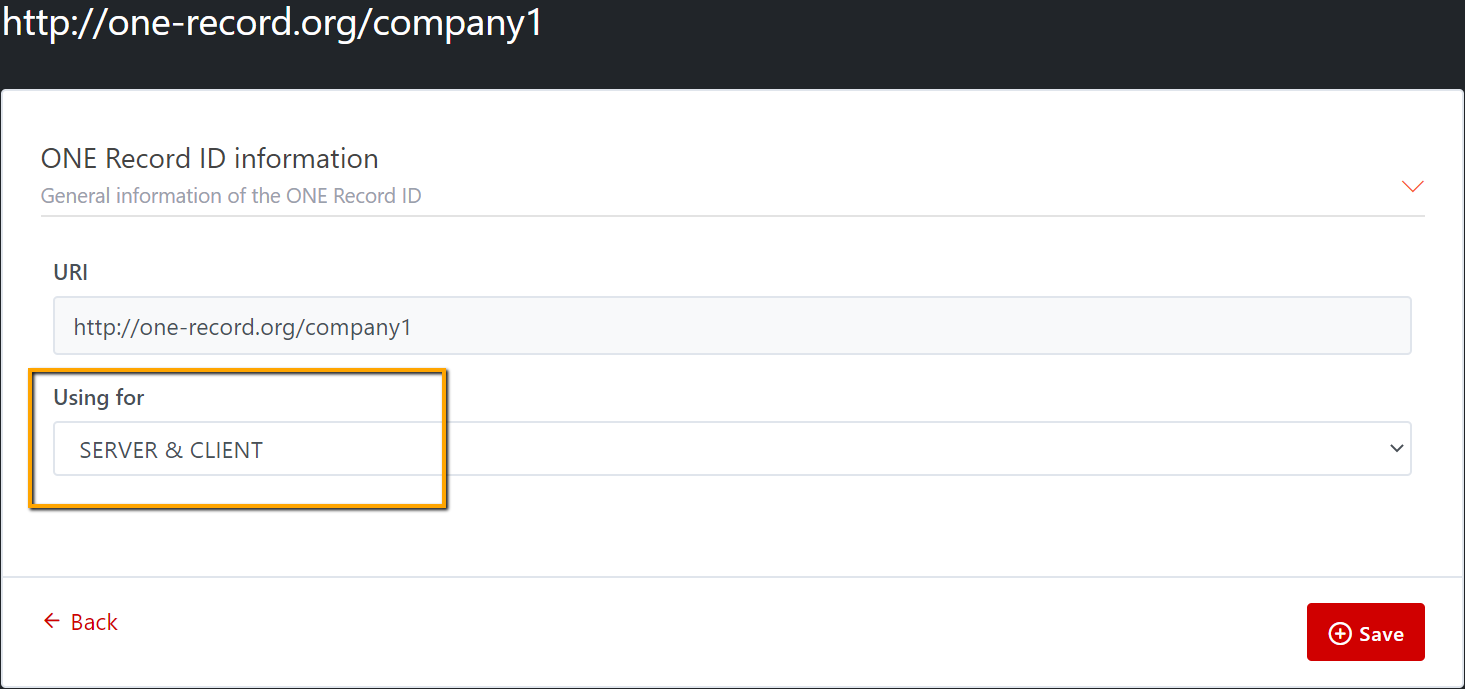
* Check Validation status
* Approve
* Reject



### ONE Record ID edit page

Edit ONE Record ID feature is only available for **Subscriber**. You can edit **pending/approved/rejected** ONE Record ID.

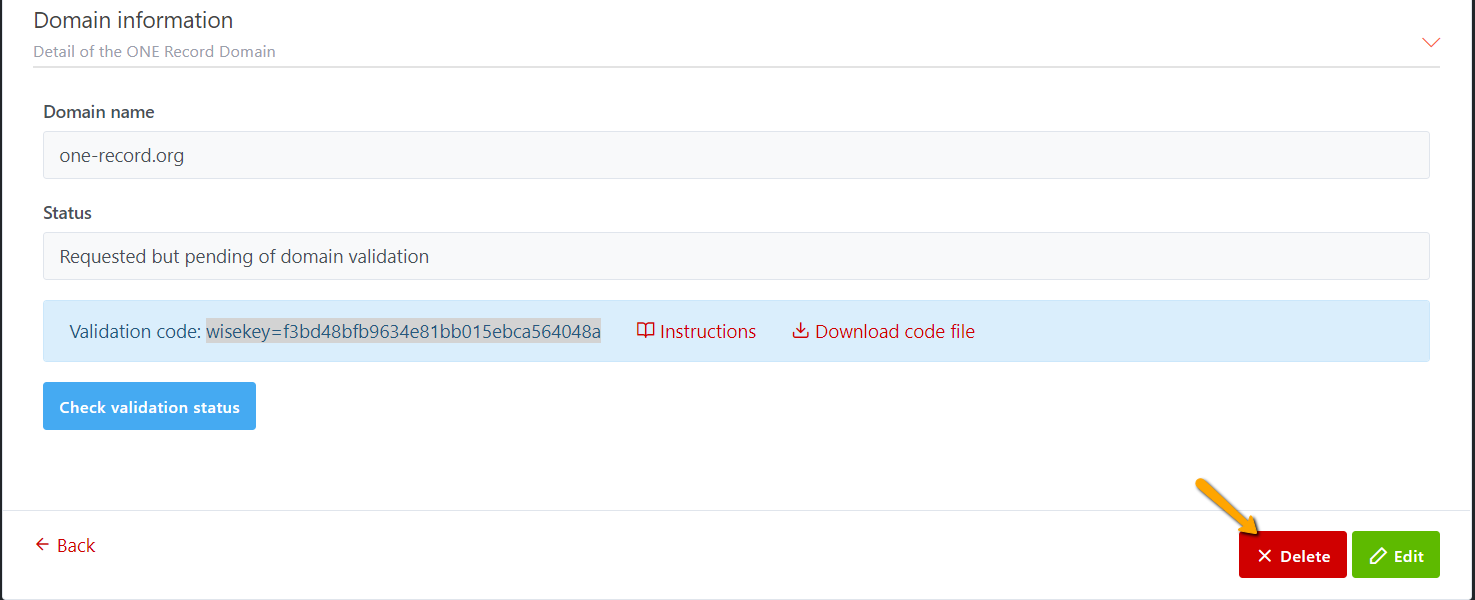
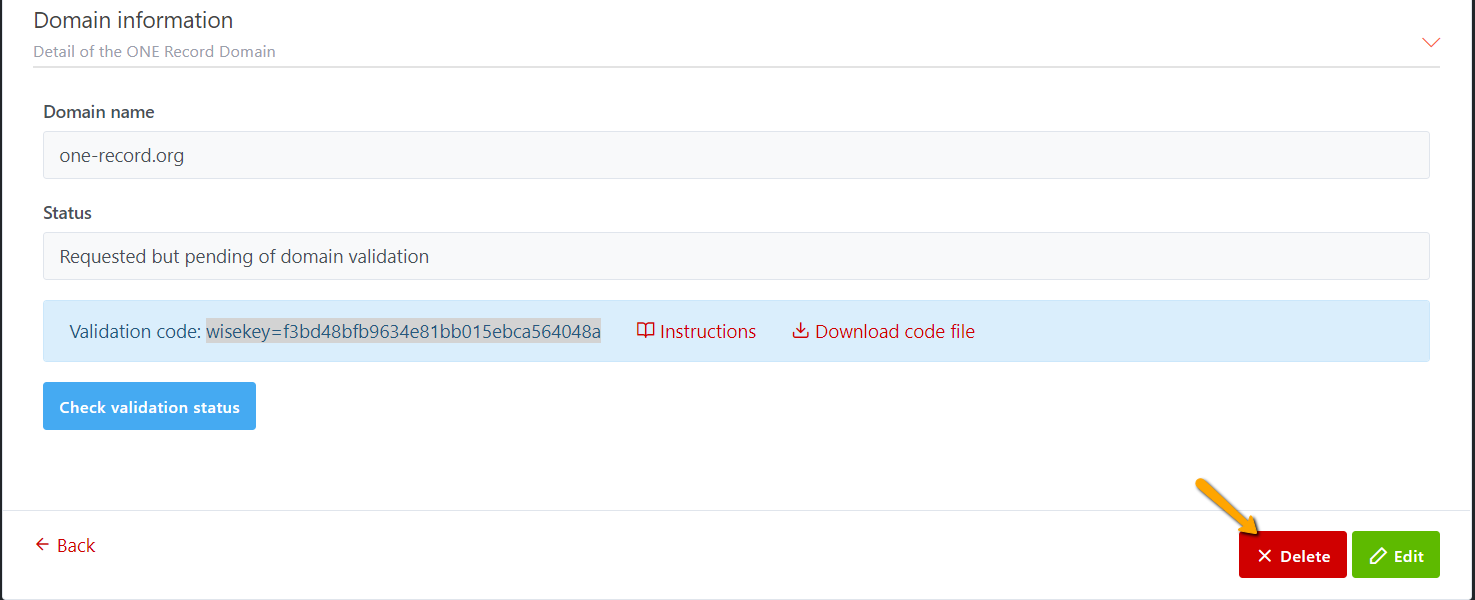
Only **Subscriber** can change the **Using for** client and/or server, cannot change URI on edit page:



### ONE Record ID delete page

**Only Subscriber** is able to **delete** the **pending approval ONE Record ID** or delete the **rejected ONE Record ID.**

Delete button is not allowed for approved 1R ID.



## Approve/Reject a registered ONE Record ID

Only **IATA admin** can approve/reject a registered ONE Record ID.

When the subscriber registers a new ONE Record ID:

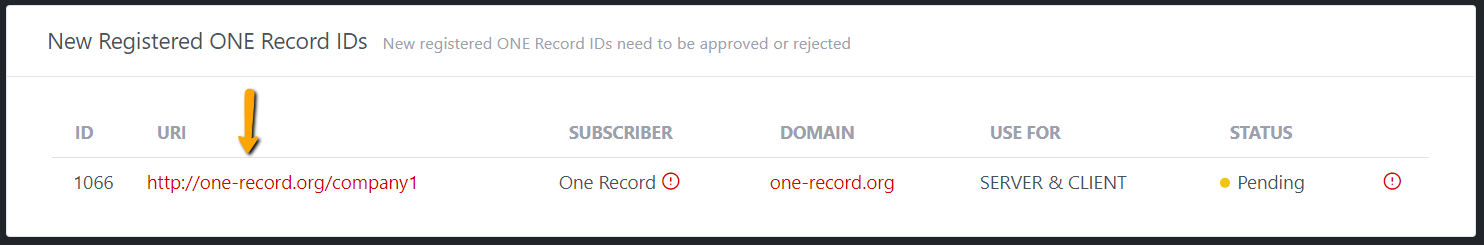
* The admin receives a notification about the new request, that needs to be approved or denied in the portal
* If the new URI will be used for a server access and it includes a new internet domain, the portal will notify to the subscriber the process to validate the domain

ONE Record ID possible status:

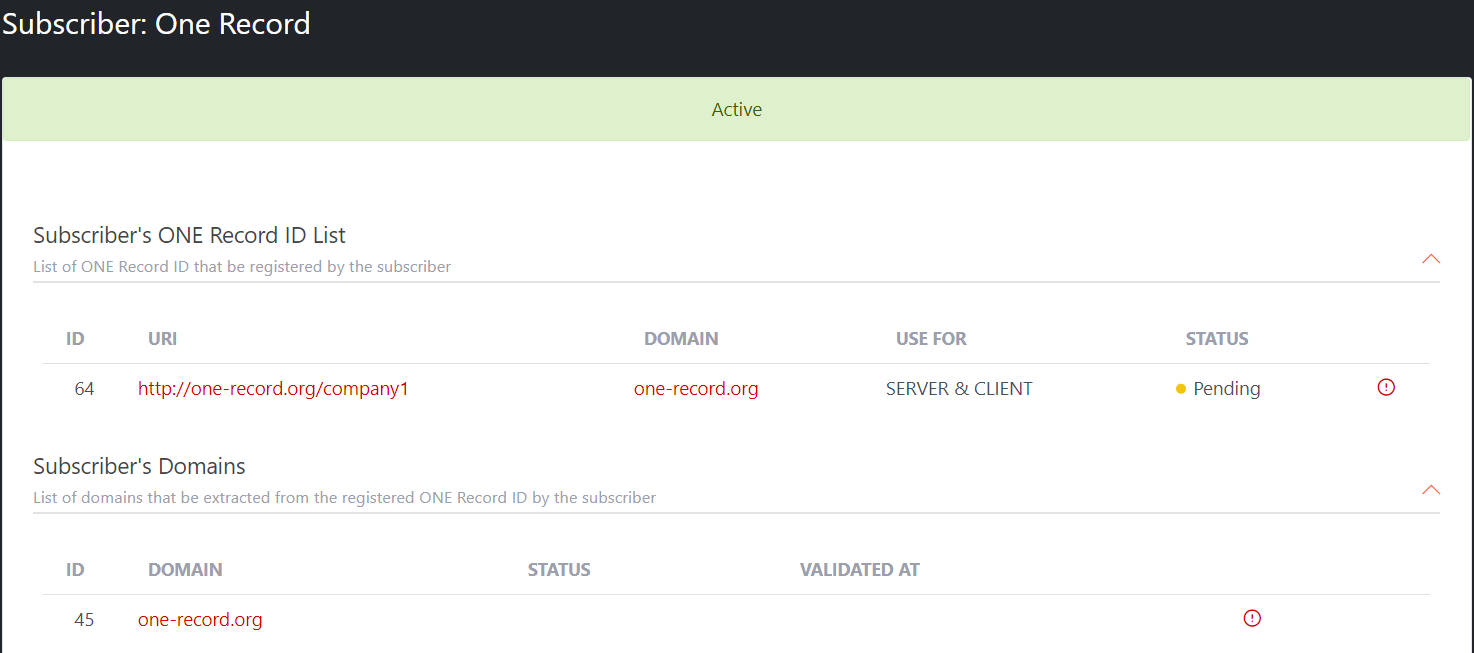
* Requested: not yet processed by the admin
* Approved but pending of domain validation
* Approved
* Denied
* Suspended (next version)

### Approve a registered ONE Record ID

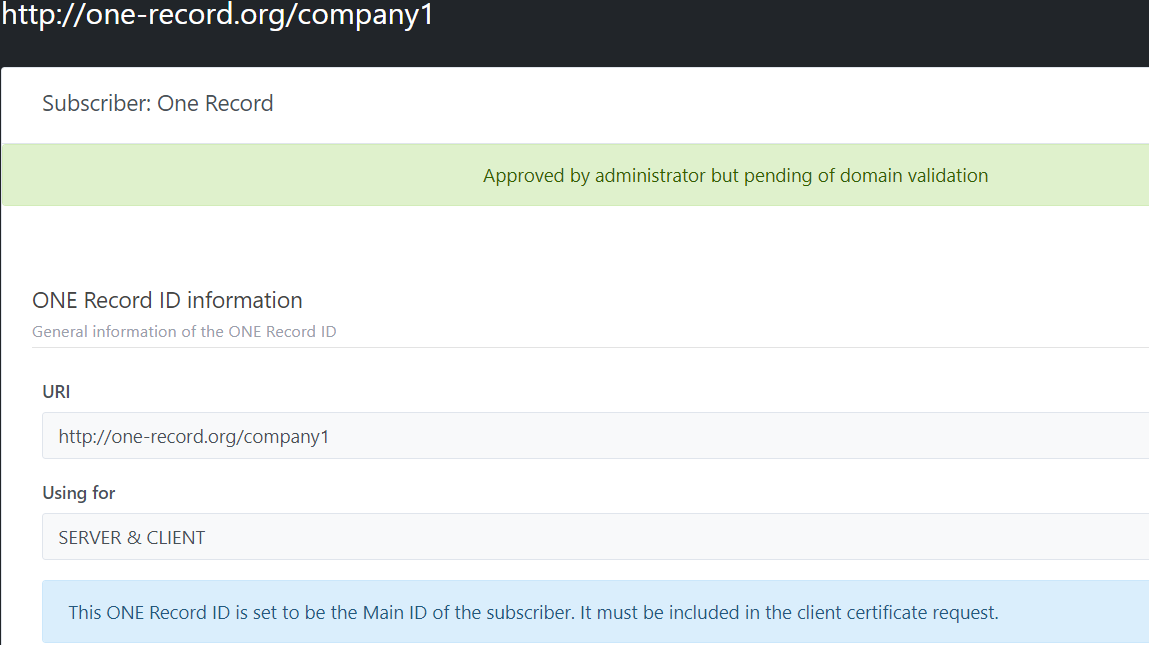
IATA Admin can open a **pending ONE Record ID** from **main dashboard** by clicking on URI link (note: to open Domain, click on domain under Domain column):



Or by opening a subscriber detail page then click on any **pending URI** in **Subscriber’s ONE Record ID list** section to approve

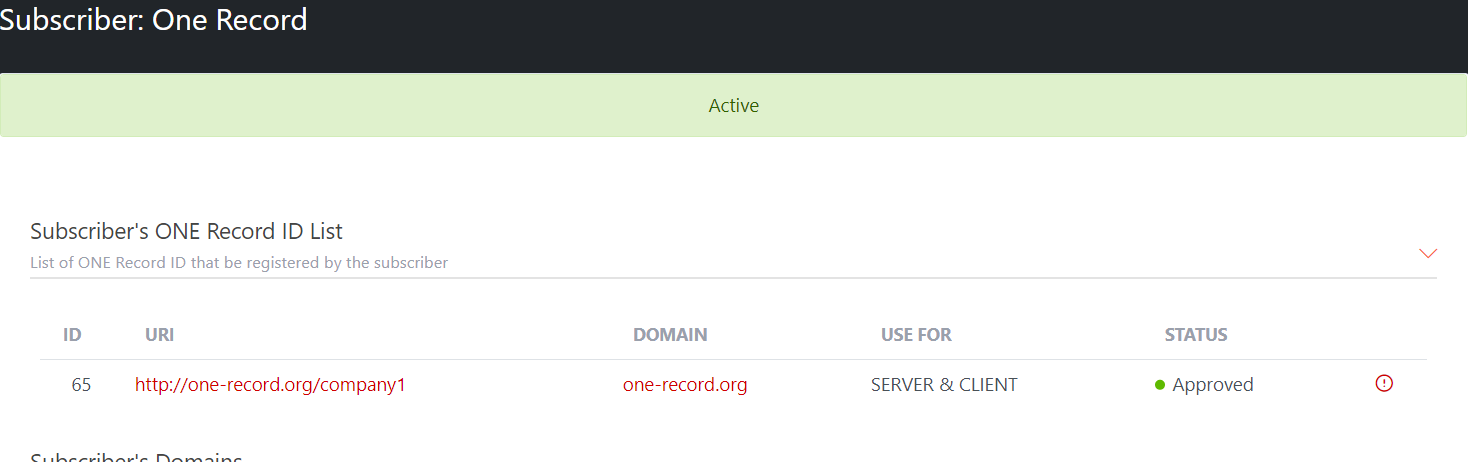


IATA Admin can approve a pending/rejected ONE Record ID by clicking on Approve button at the end of ONE Record ID detail page.

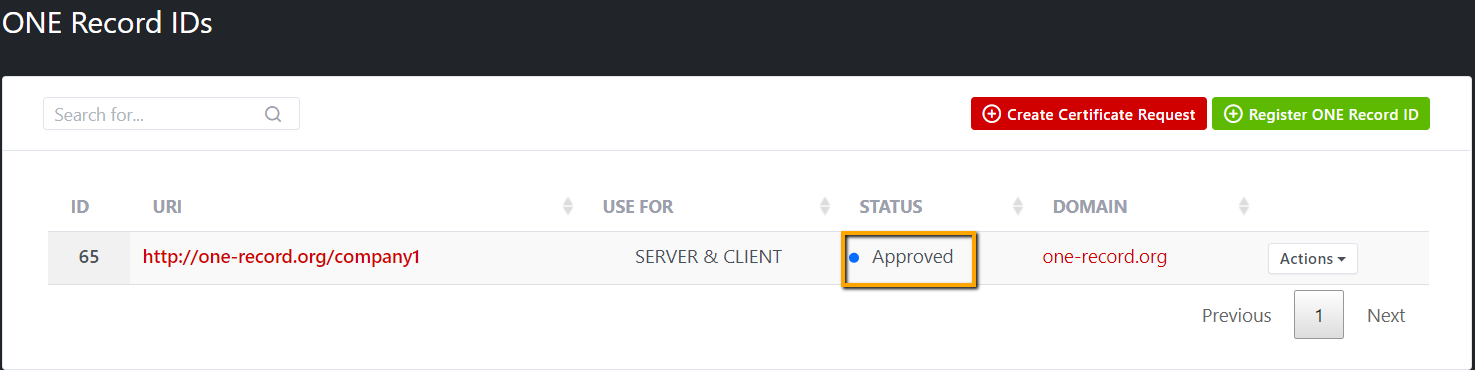


When ONE Record ID is approved, the Approve button will be disappeared, only Reject button is available. Therefore, IATA admin can reject any approved ONE Record ID later.

On **IATA Admin** dashboard, open Subscriber detail from Subscriber list page, the status of 1R ID is updated as **Approved**.

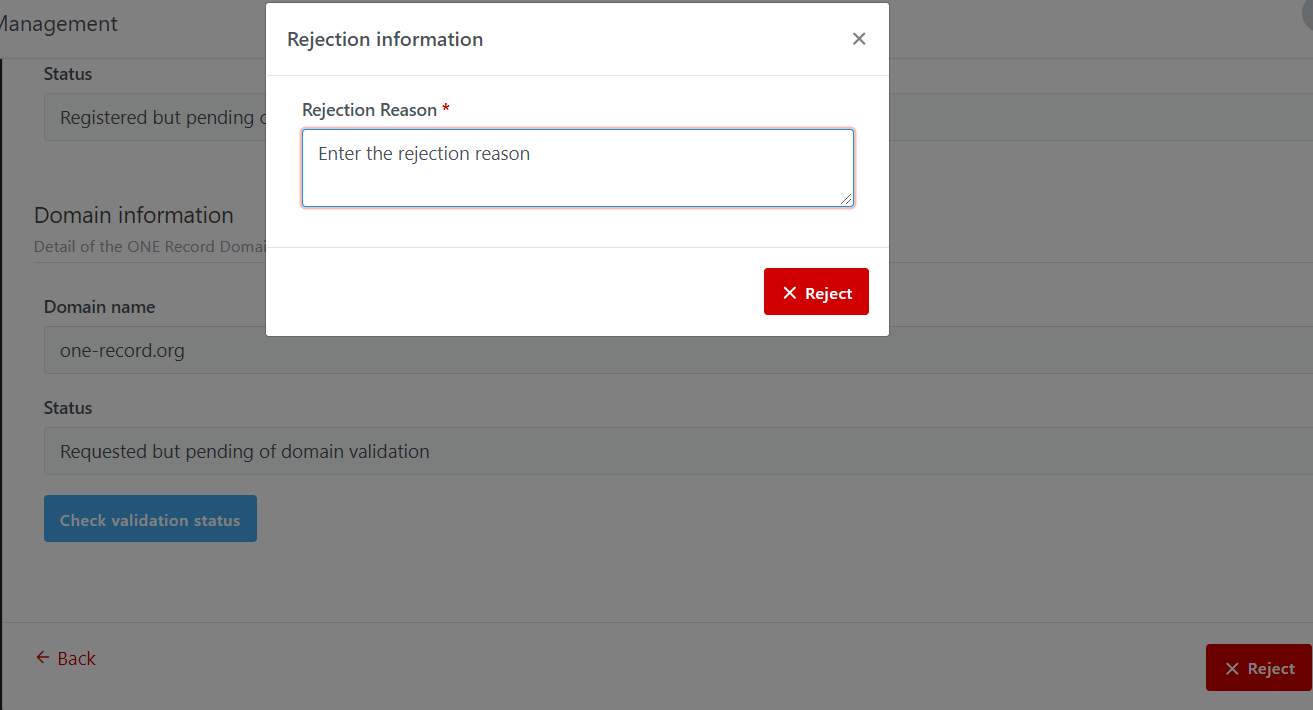


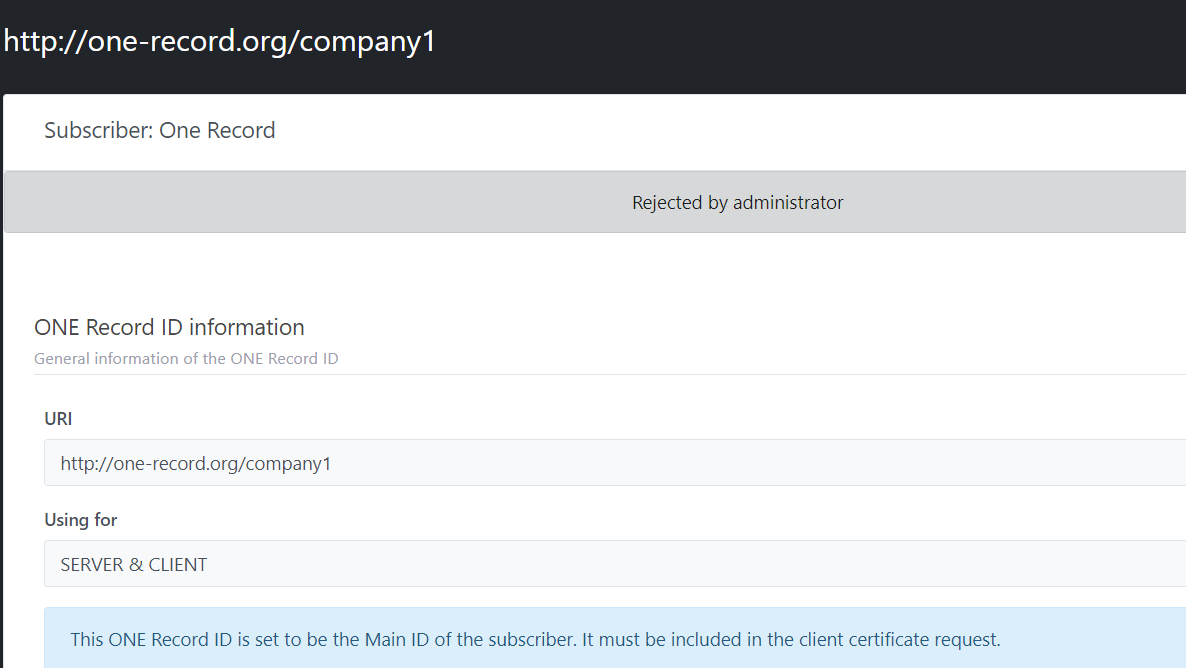
On **Subscriber** home page, you can see 1R ID has been updated status as **Approved**.



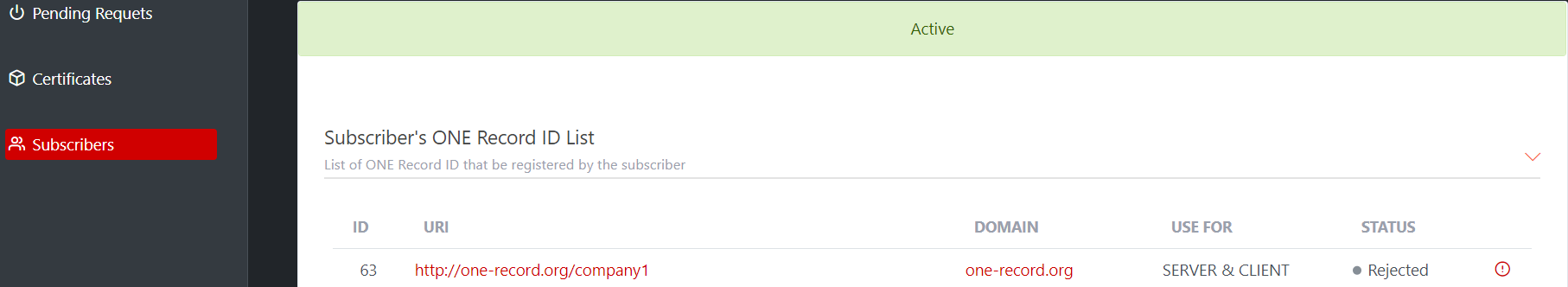
### Reject a registered ONE Record ID

**IATA admin** can reject any **pending ONE Record ID** by clicking on Reject button.

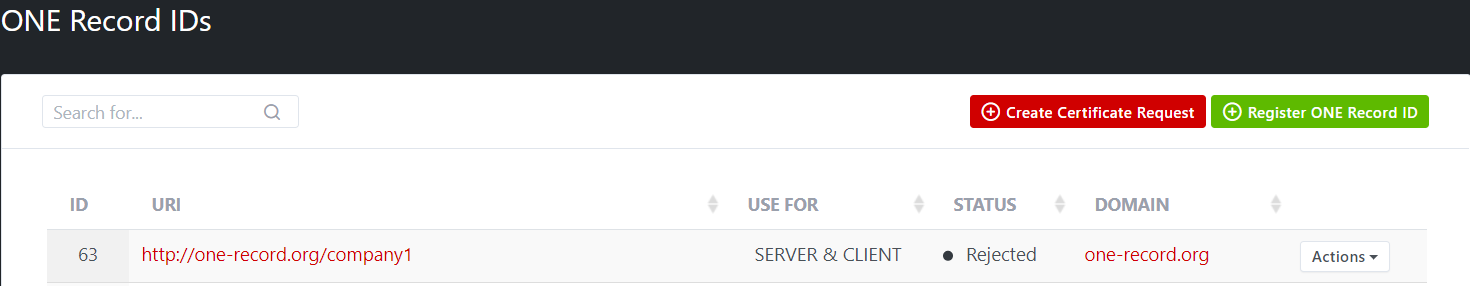




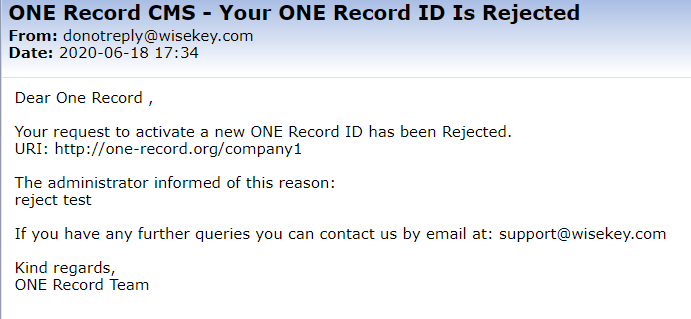
On **IATA Admin** dashboard, open Subscriber detail from Subscriber list page, the status of 1R ID is updated as **Rejected**.



On **Subscriber** home page, you can see 1R ID has been updated status as **Rejected**.



After successfully rejected, the Reject button will be disappeared, only Approve button is available, so IATA admin can approve a rejected 1R ID, and a notification email will be sent to Subscriber as following:



# Certificate Management

## Client Certificate

Access rules:

* **Admin:** can Approve/Reject Client Certificate request, Download/Revoke a Client Certificate.
* **Subscriber:** can Create/Delete Client Certificate request, Download/Revoke a Client Certificate

**To request a Client Certificate, Domain Validation is NOT REQUIRED.**

### Creating a Client Certificate request

Pre-requisite:

* ONE Record ID setting to use for CLIENT or CLIENT & SERVER.
* ONE Record ID is approved by IATA admin, no need domain validation
* Only Subscriber can create a Client Certificate Request

The subscriber can request client certificates for any ONE Record ID that has been approved by IATA admin. Client certificates are generated as PFX.

**Client Certificate profile:**

* Key usage: DIGITAL SIGNATURE
* EXTENDED KEY USAGE: clientAuthentication
* SUBJECT NAME: CN=<COMPANY\_ID>
* SUBJECT ALTERNATIVE NAME:
* URI1=<ONE\_RECORD\_ID1>
* URI2=<ONE\_RECORD \_ID2>
* …
* URIn=<ONE\_RECORD \_IDn>

In the client certificate there is one SAN of type URI for each ONE Record ID selected.

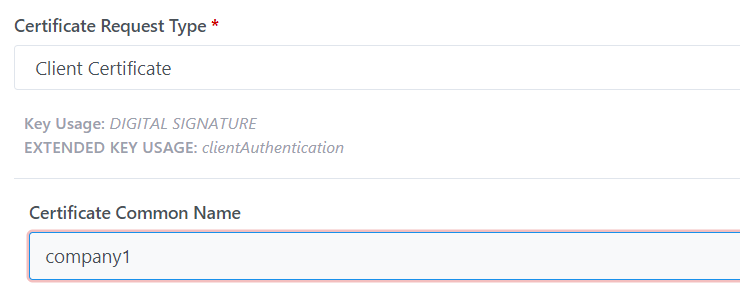
Here are steps detail to create a Client Certificate request:

**Step 1**: Open “**ONE Record IDs**” from left menuthen click on the **Create Certificate Request** button OR open “**Certificates**” from left menu and click on **NEW** button.

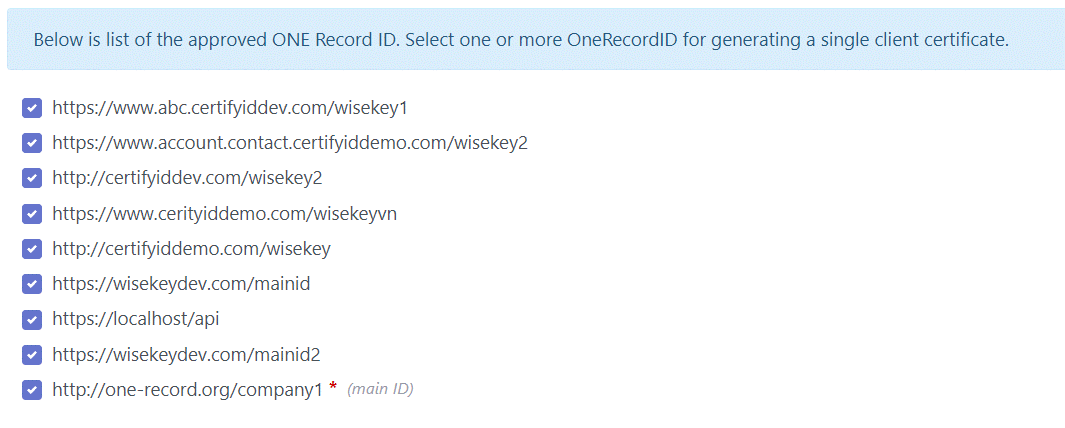
**Step 2:** Select **Certificate Request Type** as **Client Certificate**

Then all needed information to create a Client Certificate is displayed.

* Key Usage: DIGITAL SIGNATURE
* EXTENDED KEY USAGE: clientAuthentication
* Certificate Common Name = COMPANYID (which is set as MainID)



**Step 3:** Select one or more OneRecordID for generating a single client certificate. By default, all ONE Record IDs are checked.



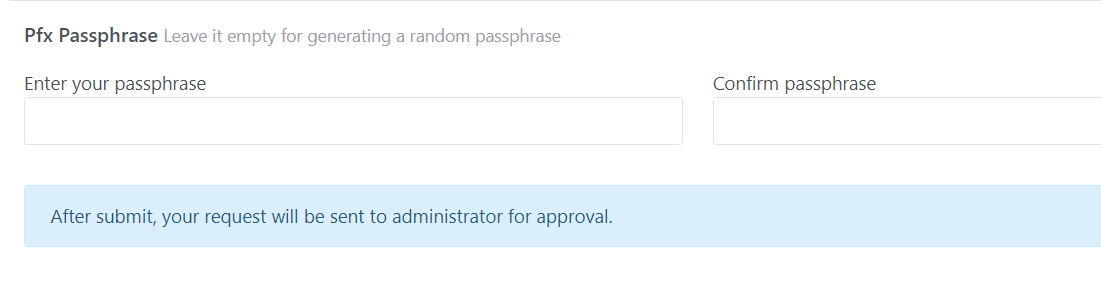
There are two options for client certificate generation:

▪ Option 1: The subscriber must select a single ONE Record ID, and this will generate a certificate for that ONE Record ID in particular.

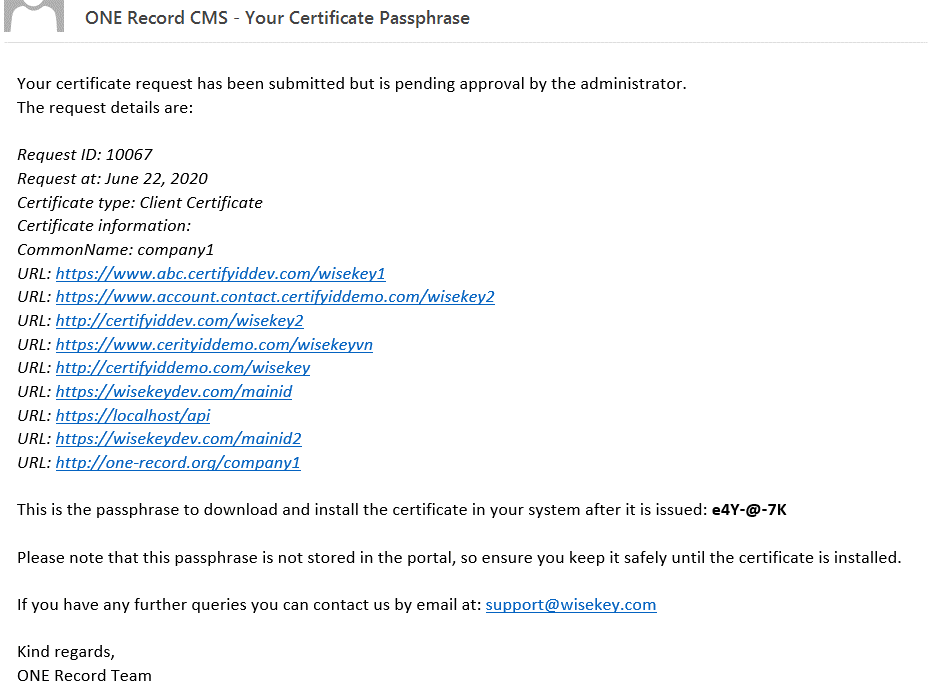
▪ Option 2: The subscriber can select one or more ONE Record IDs, and this will generate a single certificate that contains multiple SAN containing an URI for each ONE Record ID.

The portal will generate always a PFX containing the keys and certificate, protected with a password defined by the subscriber when doing the request. If the password field is left empty, the portal will automatically generate a random passphrase for the certificate.

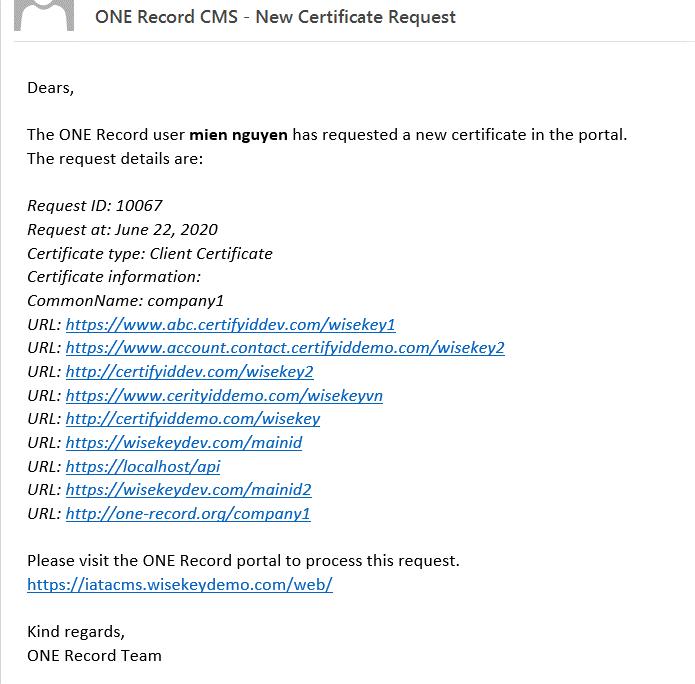
**Step 4:** Enter pfx passphrase for Client Certificate, this is optional. If the passphrase is entered, you should keep it in a safe place to use for installing certificate. If the passphrase is NOT filled, a notification email containing a randomly generated passphrase will be sent to Subscriber



Email notification to send the passphrase to Subscriber when requesting a Client Certificate but passphrase field is empty:



**Step 5:** After submit, your request will be sent to administrator for approval with a notification email like this:



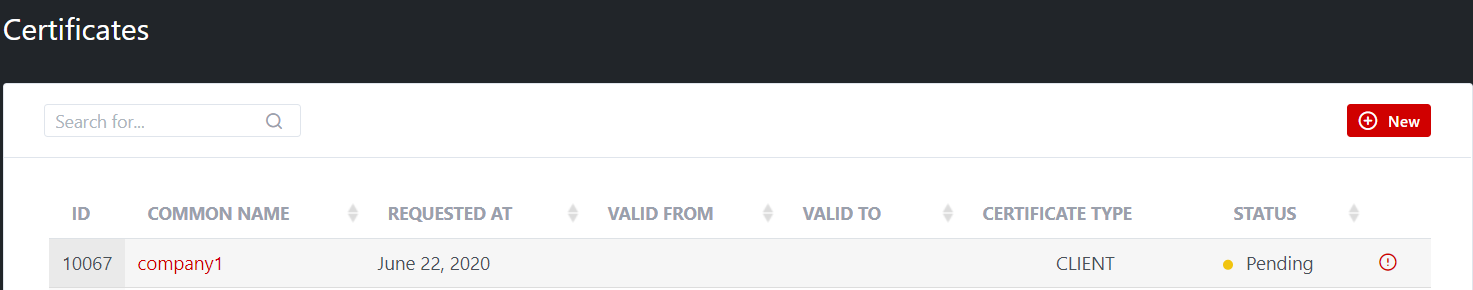
**Step 6**: A new Client Certificate request will be listed and shown in the Certificate List page of Subscriber and shown in Dashboard (New Certificate Requests - New certificate requests of subscribers need to be approved or rejected) and Pending Request of Administrator.

### Client Certificate Request List Page

**Subscribers**:

All **Certificate requests** will be listed on the List page.

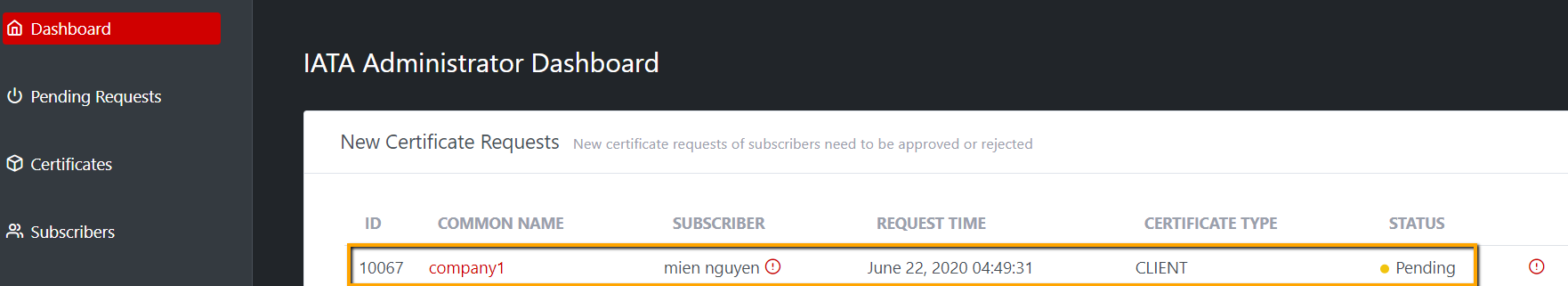
The “View” icon opens the Certificate Details page.



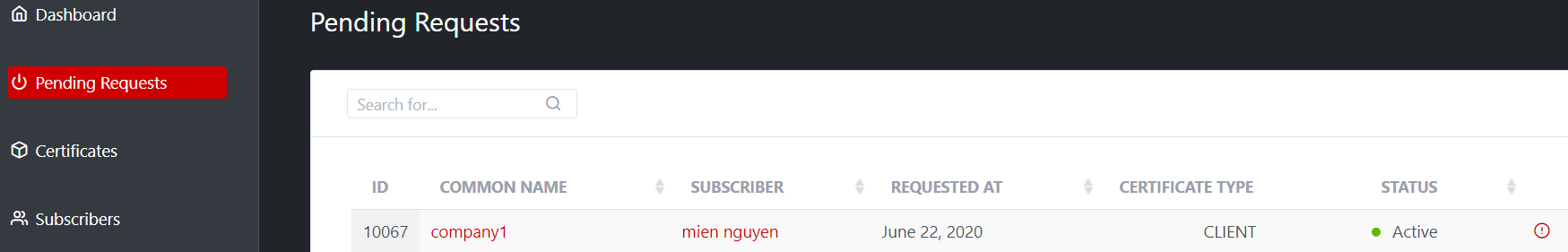
**Administrator:**

All pending certificate requested are listed in Dashboard and Pending Requests page:

Administrator Dashboard:



Pending Requests page:



**Subscriber** also can:

* View detail of a certificate request
* “Delete” a Certificate request.
* Download a CSR from certificate request detail

**Administrator** also can:

* Approve a certificate request
* Reject a certificate request
* Download a CSR from certificate request detail

### Client Certificate Request Detail page

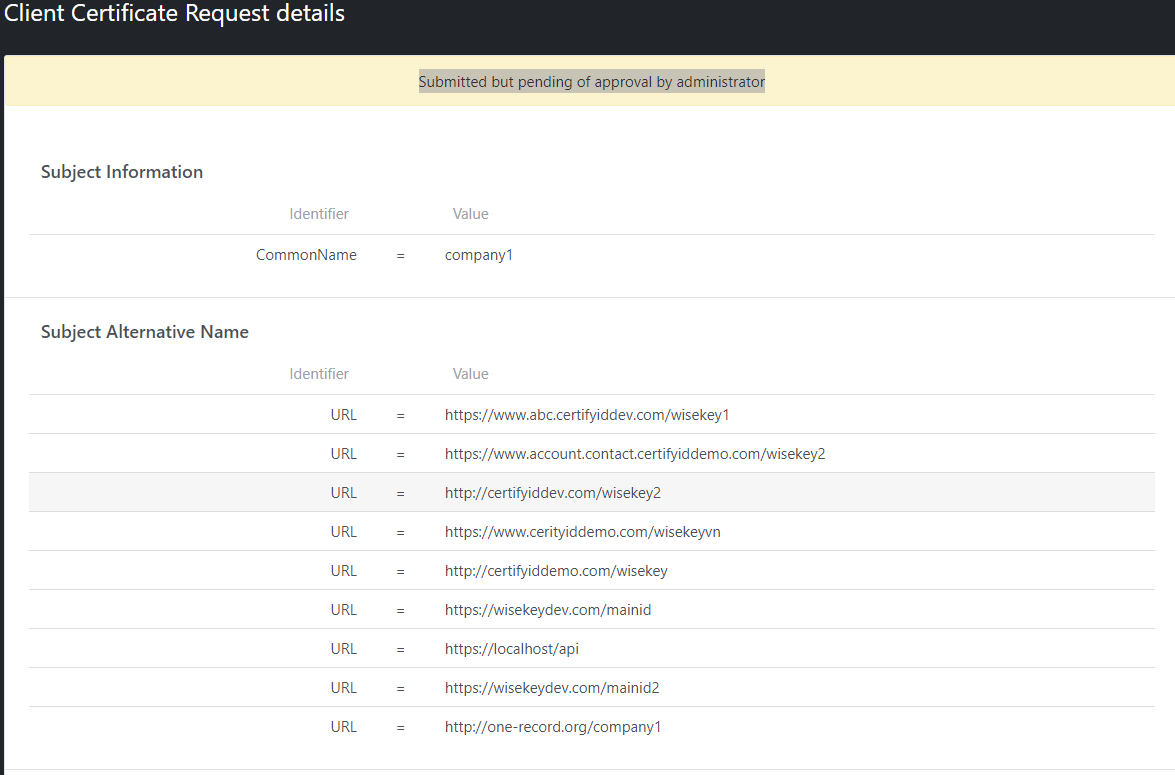
Any new request will show status in detail page: Submitted but pending of approval by administrator

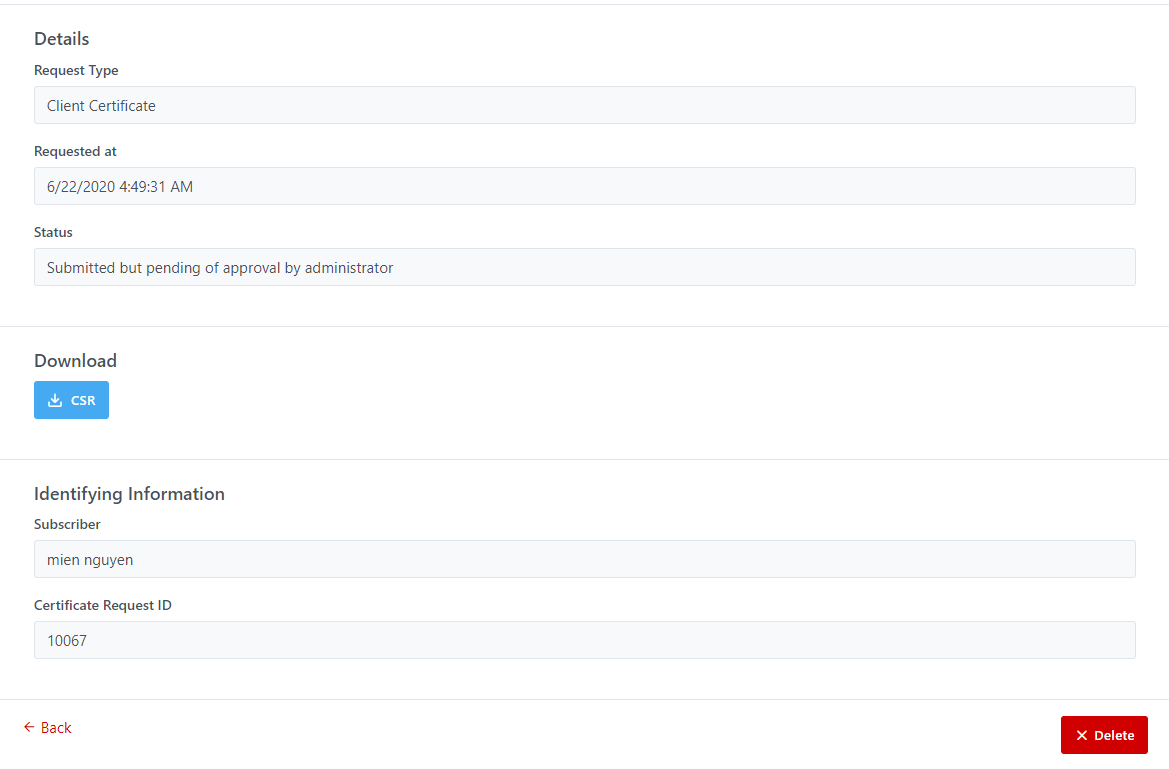
**Subscriber:**

View detail page. The possible operations are:

* “Delete” a Certificate request.
* Download a CSR from certificate request detail

**Illustrative screen:**

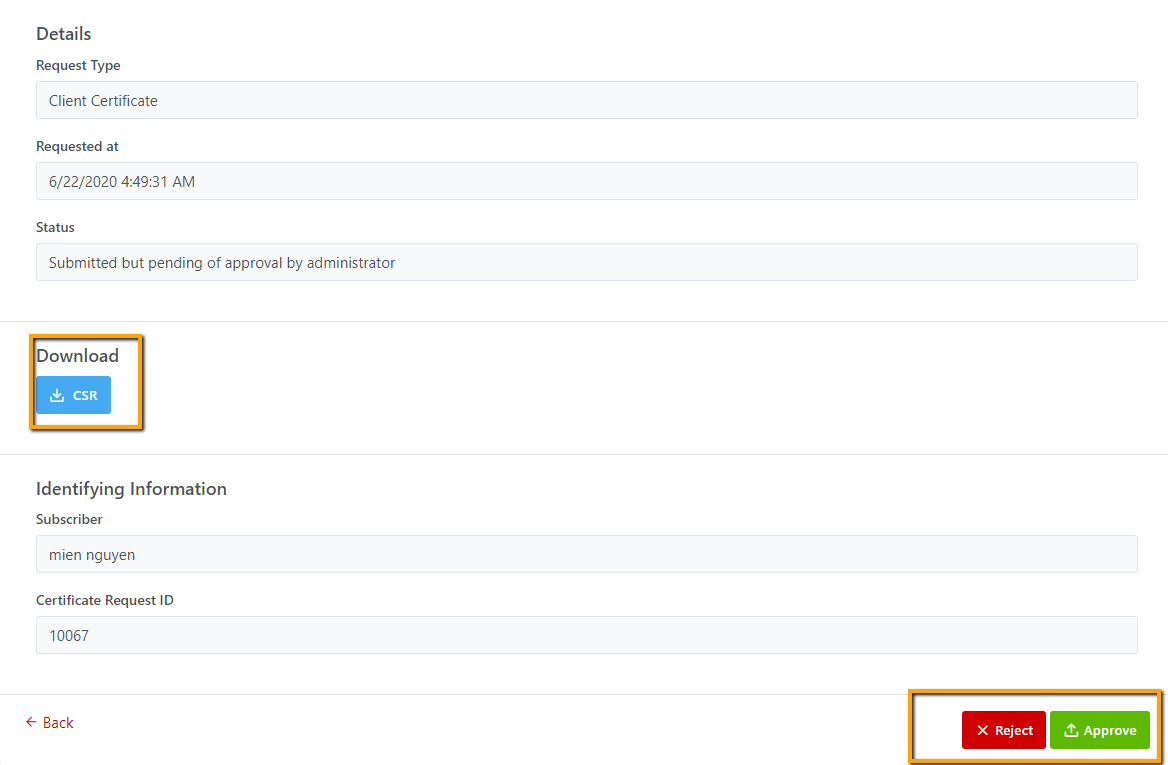




**Administrator:**

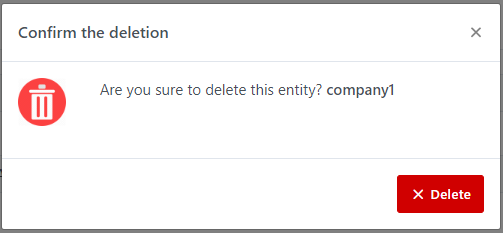
View detail page. The possible operations are:

* Approve request
* Reject request
* Download a CSR of that request



### Delete a client certificate request

Only **Subscriber** can delete a **pending/rejected** certificate request by clicking **Delete** button in Certificate request detail page. A confirmation popup window will be displayed before deleting.



When a request is deleted, it will not be shown in Certificate list page of Subscrbier, as well as Dashboard, and Pending Requests page of IATA Administrator.

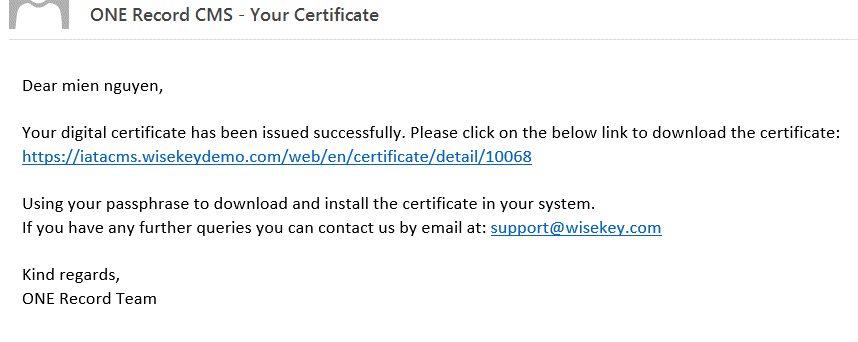
### Approve a Client Certificate Request

Only **IATA Administrator** can approve the certificate request by clicking **Approve** button in view request detail page

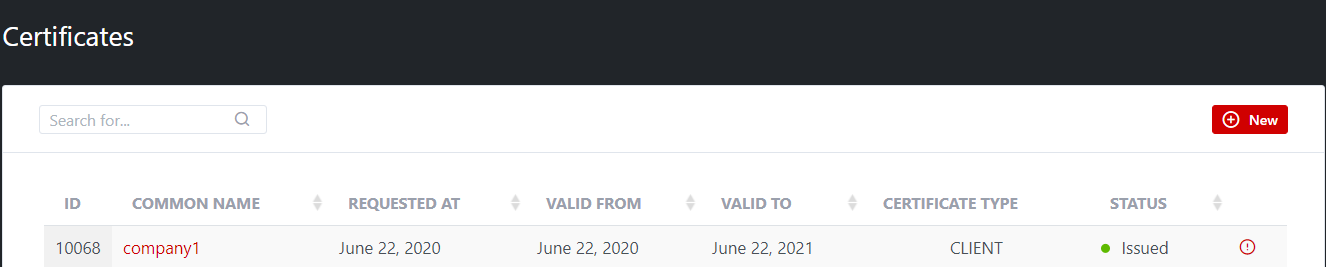
After the request is approved, the Certificate is issued and the status of request is changed from Pending to Issued on both Subscribers (Certificate list page) and Administrator (Pending request page). Also, a notification email about certificate is issued will be sent to Subscribers

**Illustrative screen:**

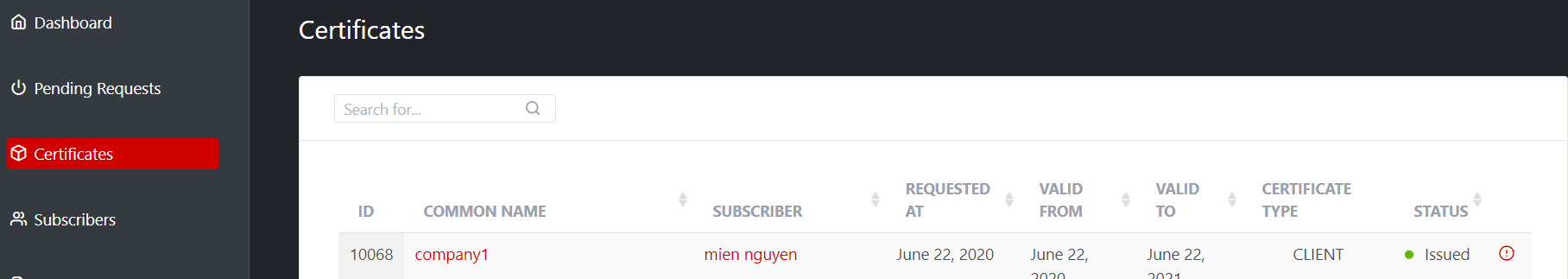
Email notification:



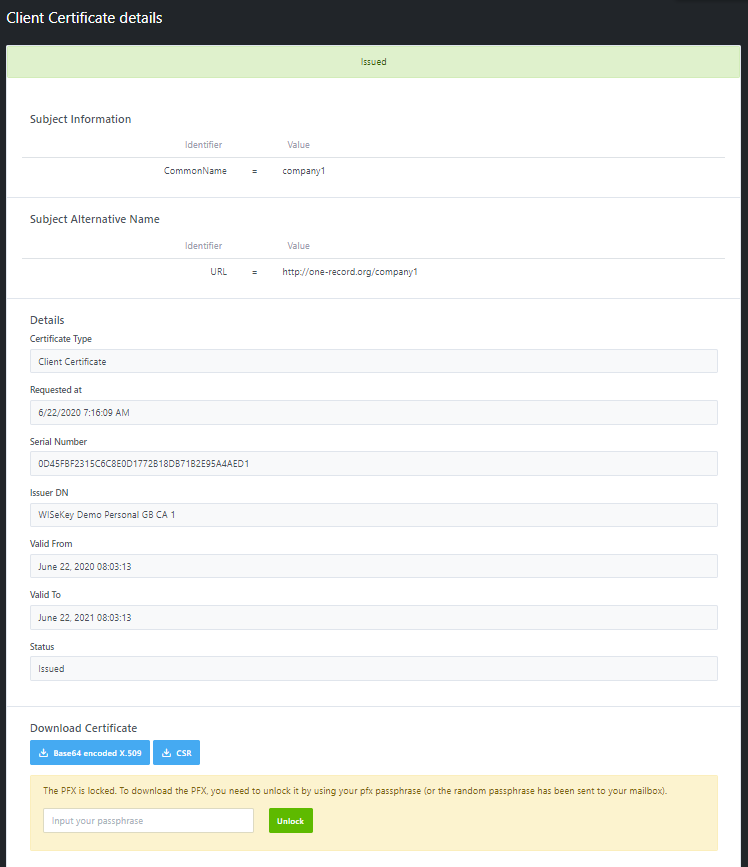
Subscriber (Certificate list page)



Administrator (Pending request page)



Certificate detail page:



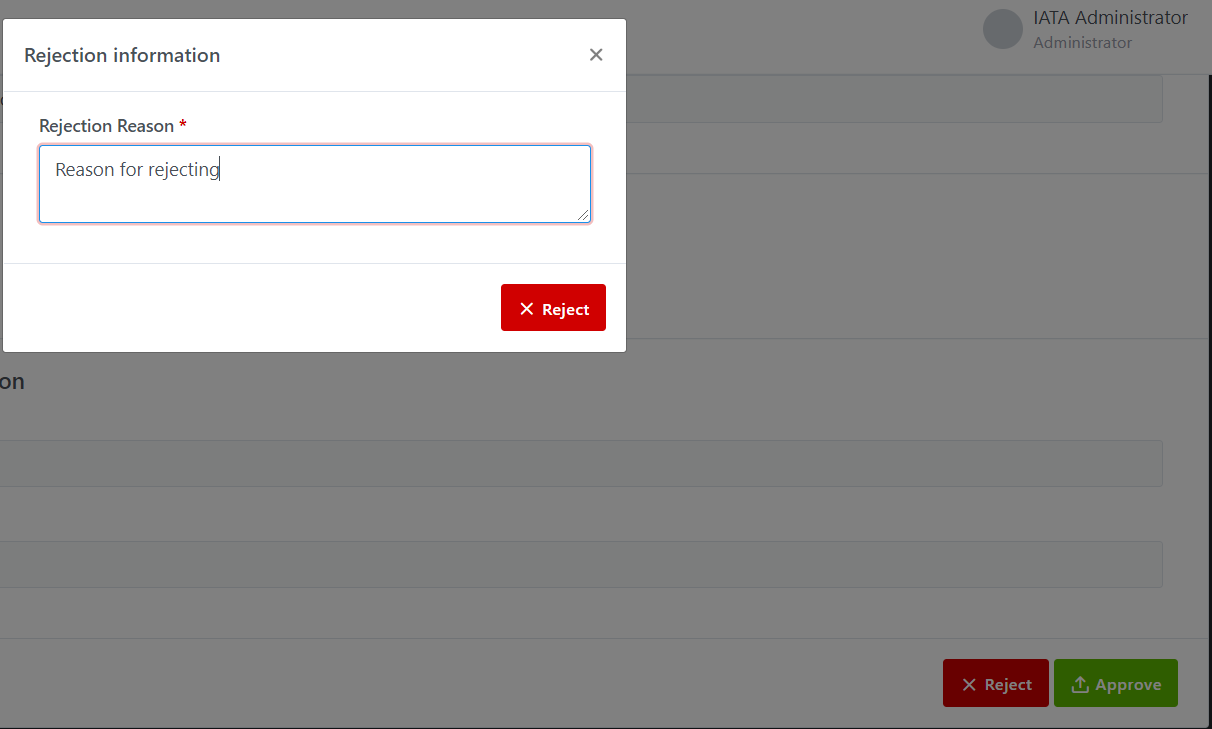
To download the PFX, you need to unlock it by using your pfx passphrase (or the random passphrase that was been sent to your mailbox).

NOTE:

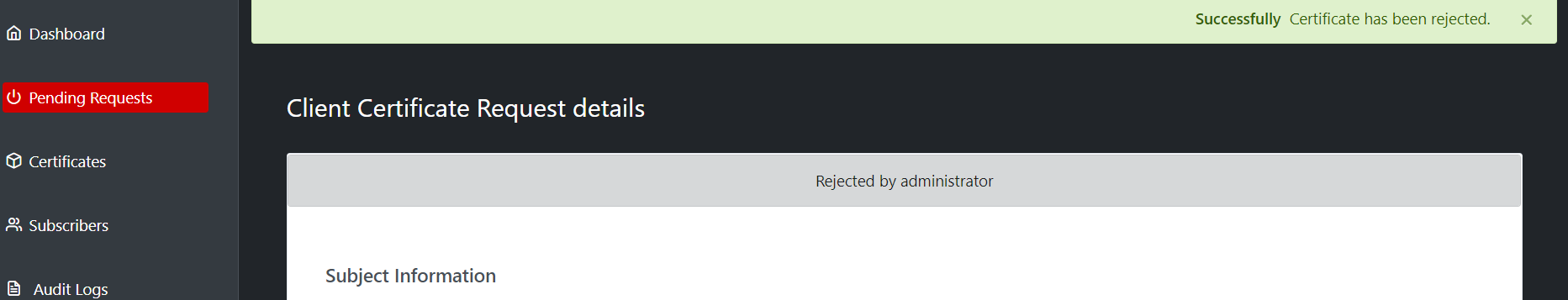
The Dashboard page only show pending requests, so approved requests will not be shown here. After requests are approved, it will be shown in Certificate page.

### Reject a Client Certificate Request

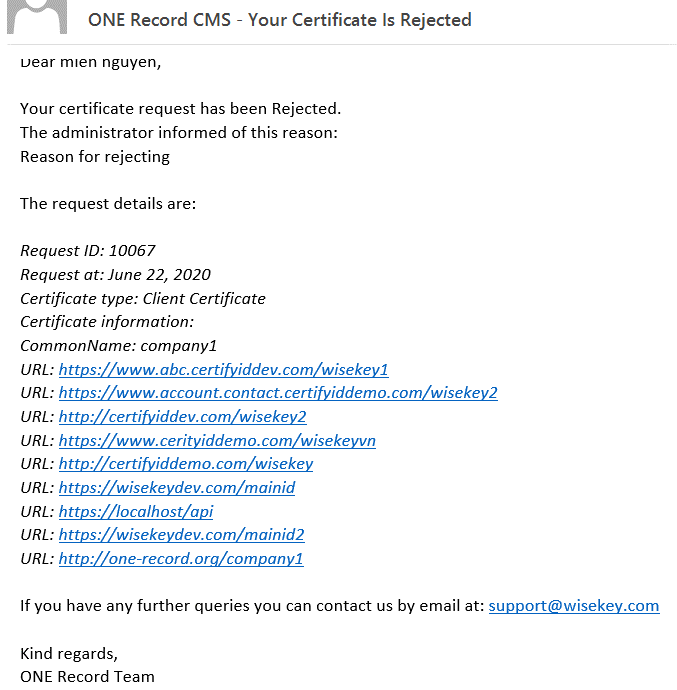
Only **IATA Administrator** can approve the certificate request by clicking **Reject** button in view request detail page and enter the reason for rejecting.



After request is rejected, a message will be shown:

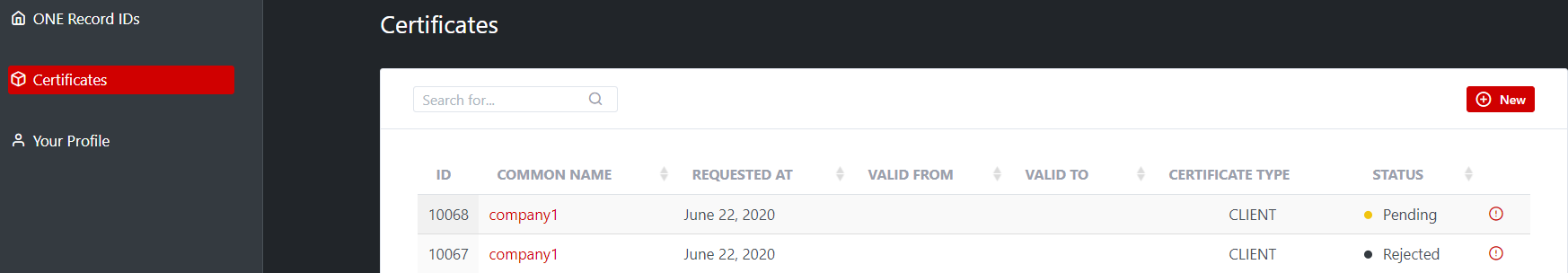


And a notification email about request is rejected will be sent to Subscriber

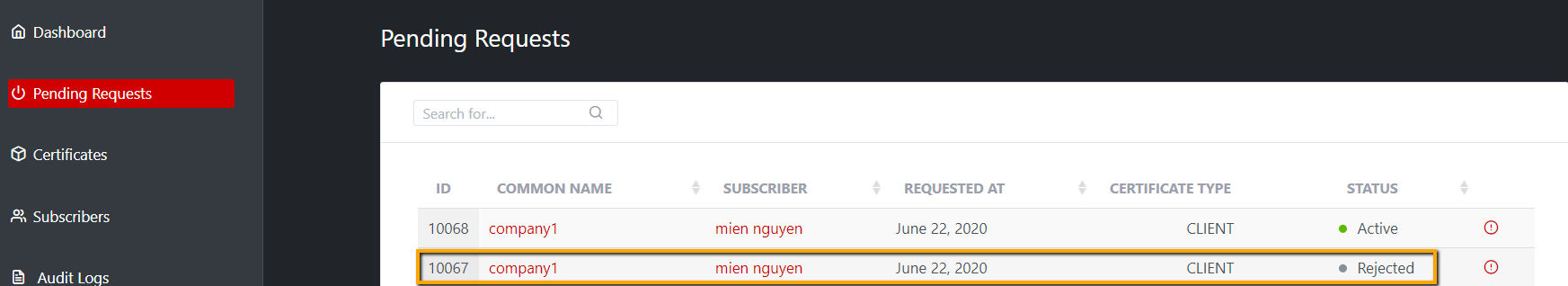


The status of request is updated to Rejected in both Subscribers (Certificate list page) and Administrator (Pending Request page).

Subscriber (Certificate list page)



Administrator (Pending request page)



NOTE: Dashboard page only show pending requests, so rejected request will not be shown here.

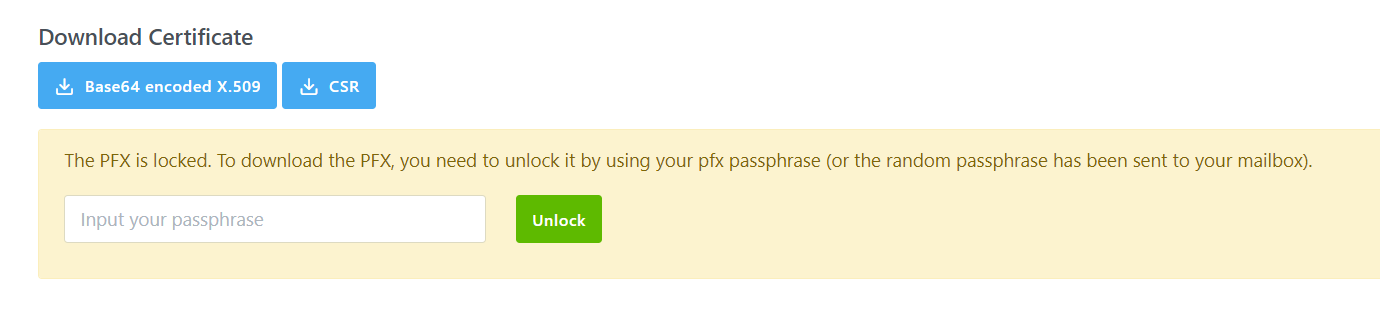
### Download an Issued Client Certificate

Both Subscriber and IATA administrator can download certificate, there are 3 options to be downloaded:

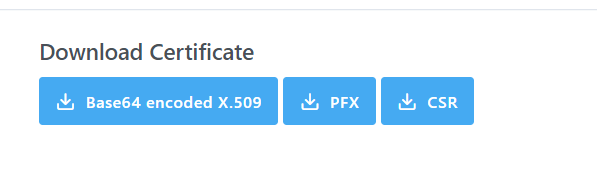
* Base64 encoded X.509
* PFX: must enter the passphrase first time to unlock pfx and download
* CSR

You can click Base64 encoded X.509 (.crt) and CSR to download without asking to enter any passphrase

To download PFX, you are required first time to enter the passphrase to unlock pfx, when pfx is unlocked successfully, you can download at any time.

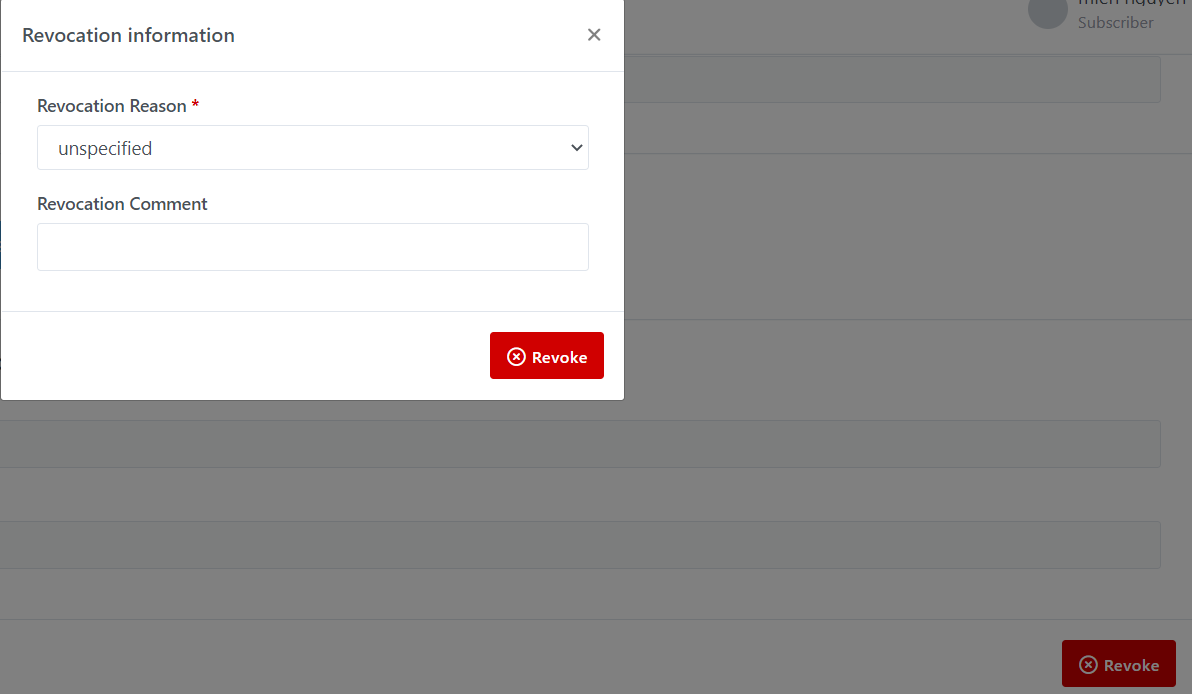


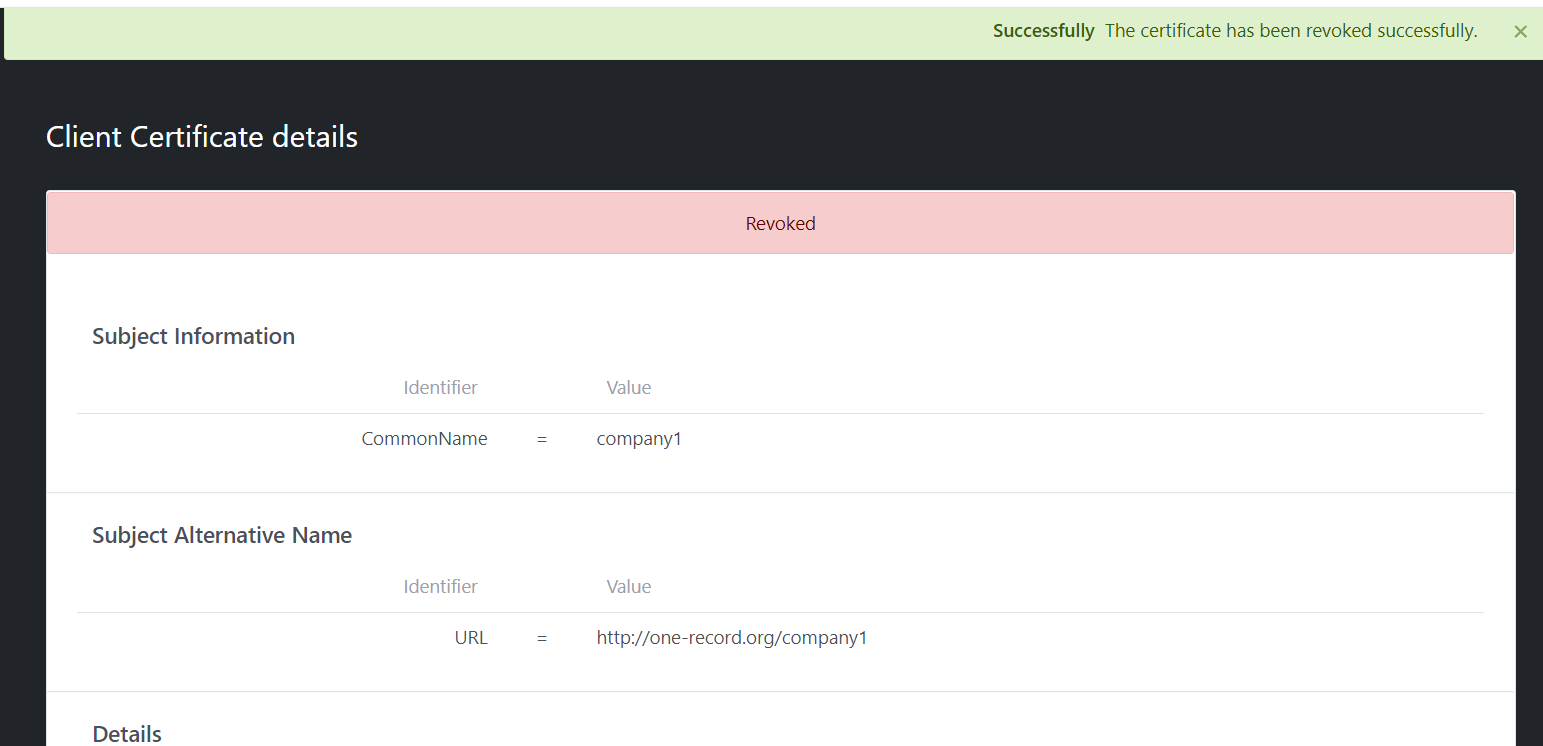
After unlocking the PFX successfully, it’s available for downloading.



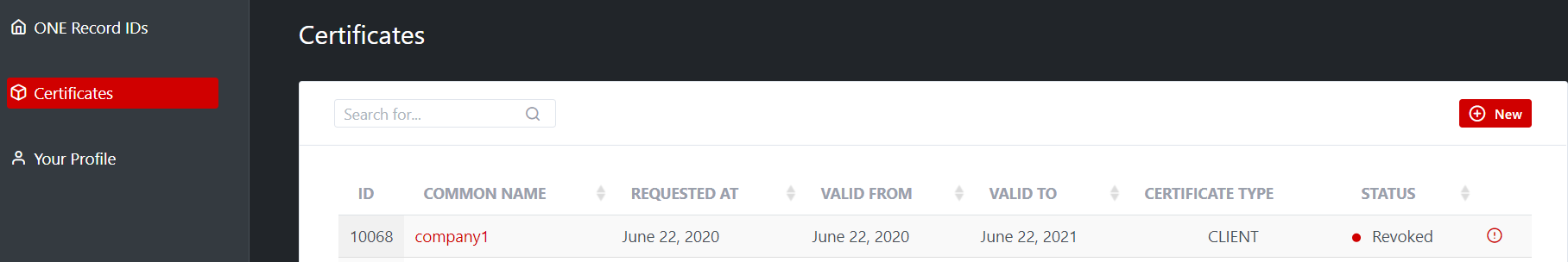
### Revoke a Client Certificate

Both Subscriber and IATA administrator can REVOKE a certificate. You need to select revocation and click on Revoke button in Revocation information window:

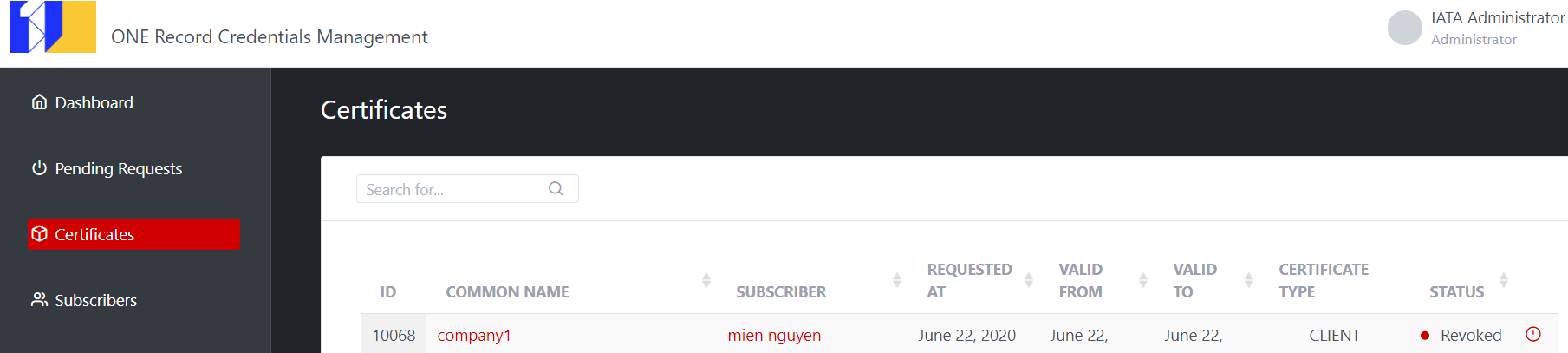
When a certificate is revoked, its status will be updated from Issued to Revoked.



Revoked Certificate in Subscriber (Certificate list page)



Revoked Certificate in Administrator (Certificate list page)



When a Certificate is revoked, subscriber and administrator still can Download PFX, CSR, Base64 encoded X.509

## Server Certificate

The subscriber can request Server certificates for any ONE Record ID that has been approved by IATA admin. It is required to have a validated domain to request a Server Certificate.

**Server Certificate profile**

* Key usage: DIGITAL SIGNATURE, KEY ENCYPHERMENT
* EXTENDED KEY USAGE: serverAuthentication, clientAuthentication
* SUBJECT NAME: CN=<FQDN1>
* SUBJECT ALTERNATIVE NAME:
* DNS1=<FQDN1>
* DNS2=<FQDN2>
* …
* DNSn=<FQDNn>

In the server certificate there is one SAN of type FQDN for the different FQDN extracted in the list of selected ONE Record ID (the same FQDN could be repeated for several ONE Record ID, but we only add it once in the certificate).

### Domain Validation

**Overview**

When a new ONE Record ID is approved to be used for a server access, before issuing a server certificate it is required that the subscriber demonstrates control on the included domain in the URI.

The domain validation is valid for 2 years (will be reduced soon on 1 year) and in the period unlimited certificates with FQDN in that domain can be used.

When a server URI is approved by the admin, the portal will check if the domain was already validated, if not, it will notify to the subscriber a random value that needs to be added as a TXT record in the DNS server.

Only after the portal verifies that the domain is validated will allow to request server certificates.

**Procedure for domain validation**

In order to issue the certificate, it is required to verify to ownership of the domains. There are two ways for verifying the domains:

1. **By uploading the email attached file in the web server**

To use HTML method, the subscriber must be able to upload new file and create folders in a website using the requested domain.

a) Download the text file attached with the email (usually of format wisekey.txt);

b) Upload the above file to the host in this EXACT path http(s)://domain/well-known/pki-validation/wisekey.txt;

c) Check the domain validation status from ONE Record portal.

2. **By adding a TXT record in the DNS**

Create a TXT record for the domain included in the certificate request in the DNS providers as below:

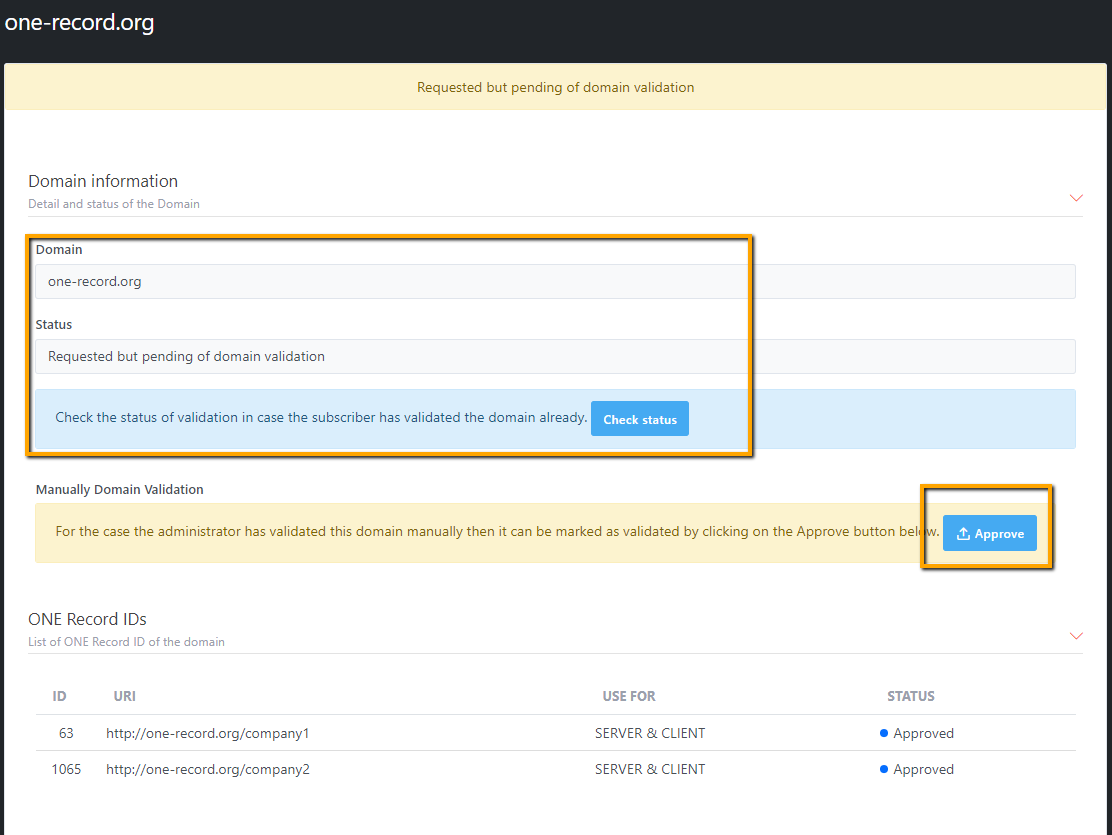
a) Name/Host/Alias/TXT: Blank or @

b) Value/Points to/Destination: wisekey=SOMEVALUESENTINTHEEMAIL

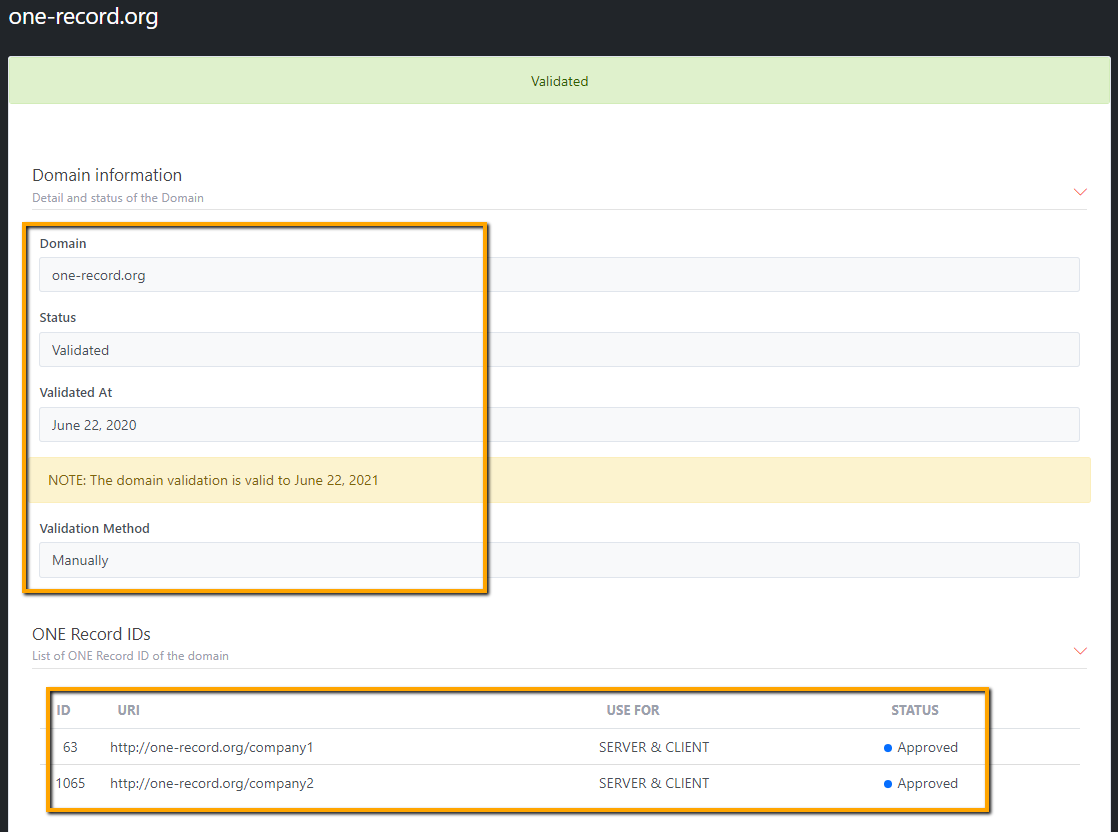
The subscriber may have to wait for at least an hour for the changes to take effect in the DNS Servers. After an hour or two, the subscriber should log in to the ONE Record portal and check status of the validation.

**Manually Domain Validation**

Currently the portal support manual domain validation (based on checking domain manually, checking subscriber is really the ownership of the domain…) then click button **Approve** to make that domain validated. Administrator can click on **Check Status** button to check the current status of domain validation.



When Approve button is clicked, the domain will be validated in 1 year, the status, validated date, expired date of validation domain, validation method is updated and shown as below:



### Create a Server Certificate Request

**Only Subscriber can create Server Certificate Request**

**Administrator will approve/reject the Server Certificate Request.**

**Pre-requisite:**

* One Record ID settings to be used for SERVER or CLIENT & SERVER
* One Record ID has been approved by IATA Admin
* Domain is validated and the validation date is not expired.

Server certificates require to upload a CSR (Certificate Signing Request) and domain validation.

The subscriber can request server certificates for any ONE Record ID that has been approved by IATA Admin and that contains a domain that is validated.

The subscriber can select one or more ONE Record IDs, and this will generate a single certificate that contains multiple SAN containing an FQDN for each ONE Record ID.

Example:

The subscriber selects multiple ONE Record IDs:

▪ https://servername.domain1.com/companyid1

▪ https://servername.domain1.com/companyid2

▪ https://servername2.domain1.com/companyid3

▪ https://servername.domain2.com/companyid4

The portal will generate a TLS server certificate that contains three SAN:

▪ SAN1: DNS = servername.domain1.com

▪ SAN2: DNS = servername2.domain1.com

▪ SAN3: DNS = servername.domain2.com

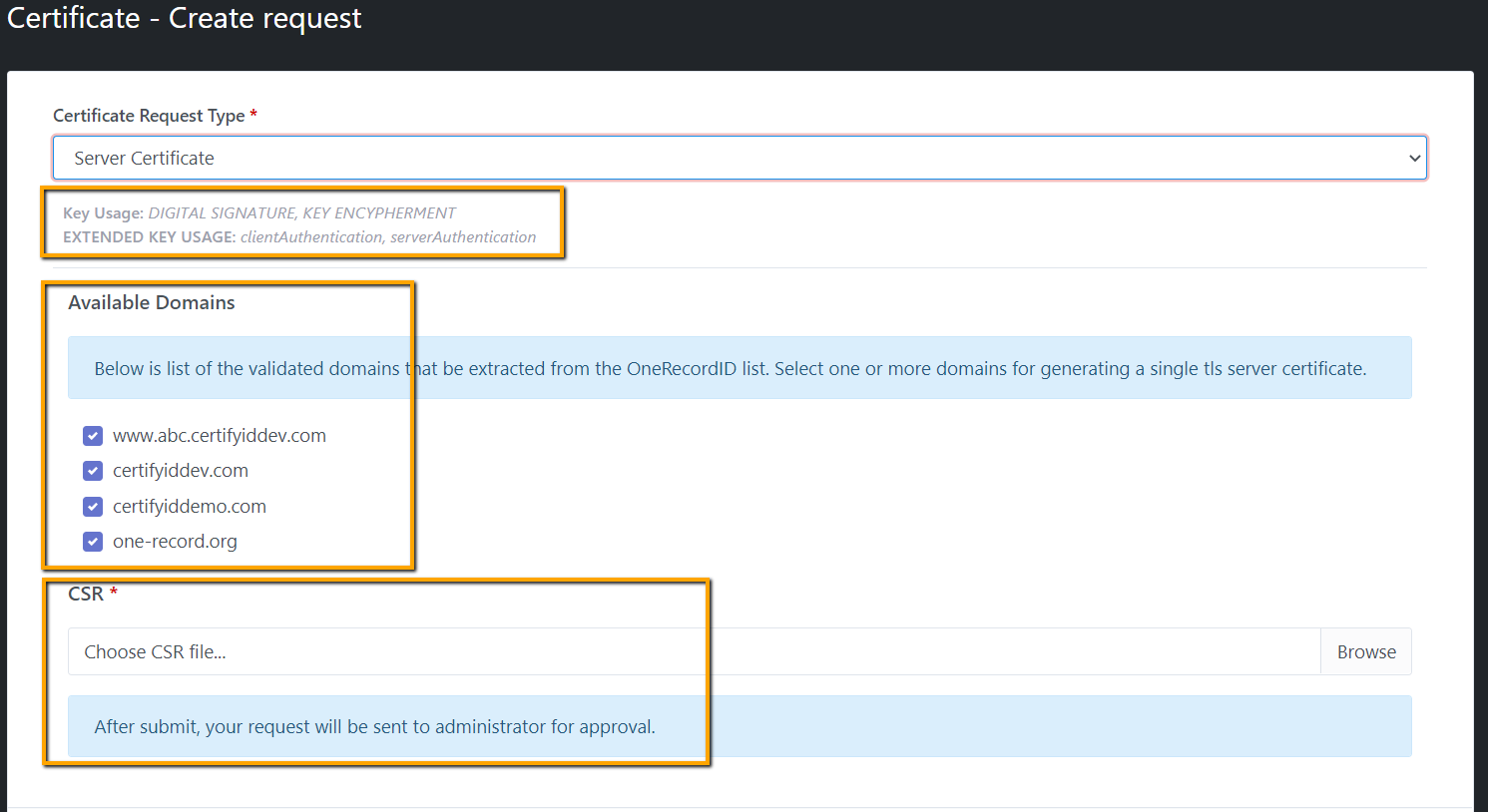
Steps to create a Server Certificate request

**Step 1**: Open “**ONE Record IDs**” from left menuthen click on the **Create Certificate Request** button OR open “**Certificates**” from left menu and click on **NEW** button.

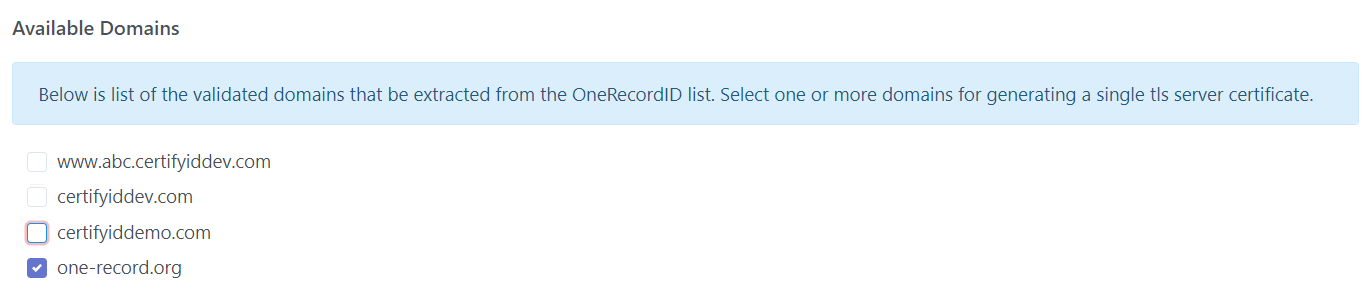
**Step 2:** Select **Certificate Request Type** as **Server Certificate**

Then all needed information to create a Server Certificate is displayed.

* Key Usage: DIGITAL SIGNATURE, KEY ENCYPHERMENT
* EXTENDED KEY USAGE: clientAuthentication, serverAuthentication
* Available Domains

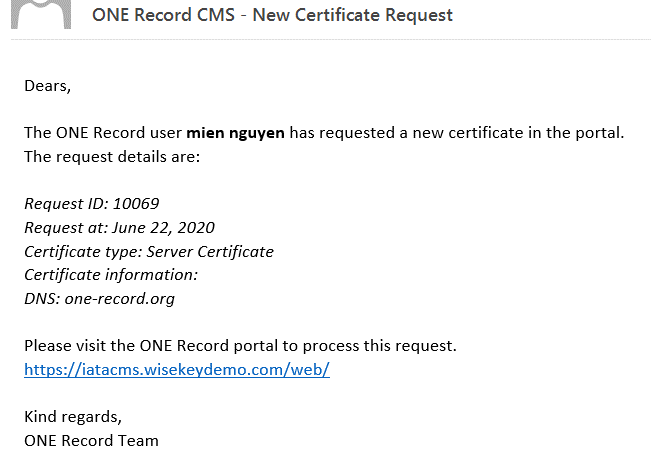


**Step 3:** Select one or more domains for generating a single tls server certificate. By default all available domains are checked.



NOTE: Common Name of Server Certificate is empty

**Step 4:** Upload a CSR file (it is required) then click on Submit button. When a request is created successfully, it will be listed in **Certificate list page of Subscribe** as well as **Dashboard page (New Certificate Request section) and Pending request page of Administrator**. The status is **Pending.** Also **a notification email** will be sent to **Administrator** to approve this request

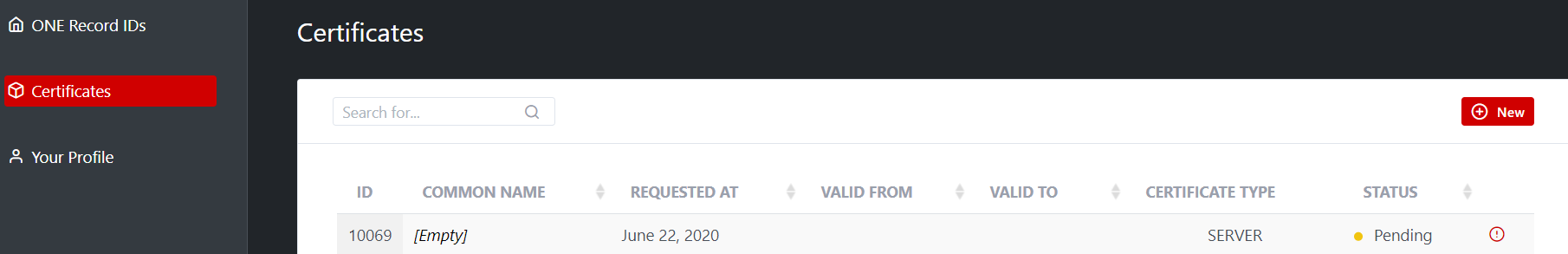


### Server Certificate request list page

**Subscribers**:

All **Certificate requests** will be listed on the List page.

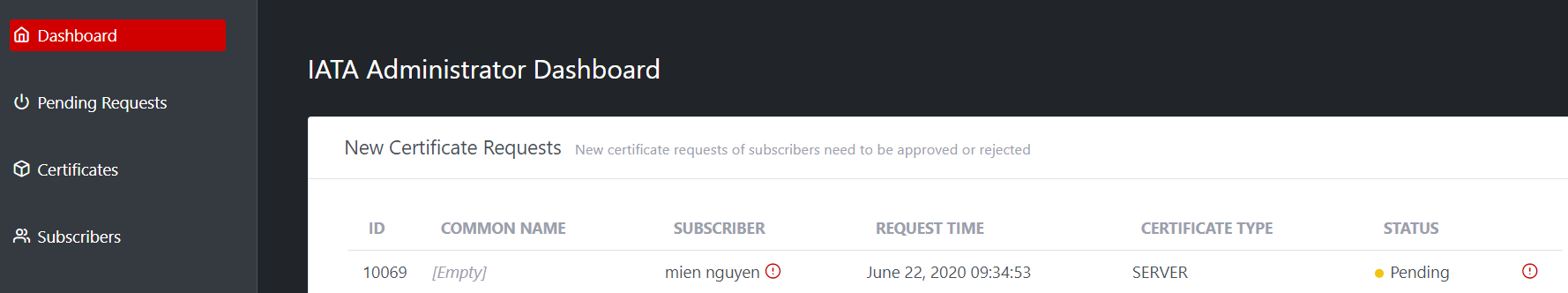
The “View” icon opens the Certificate Details page.



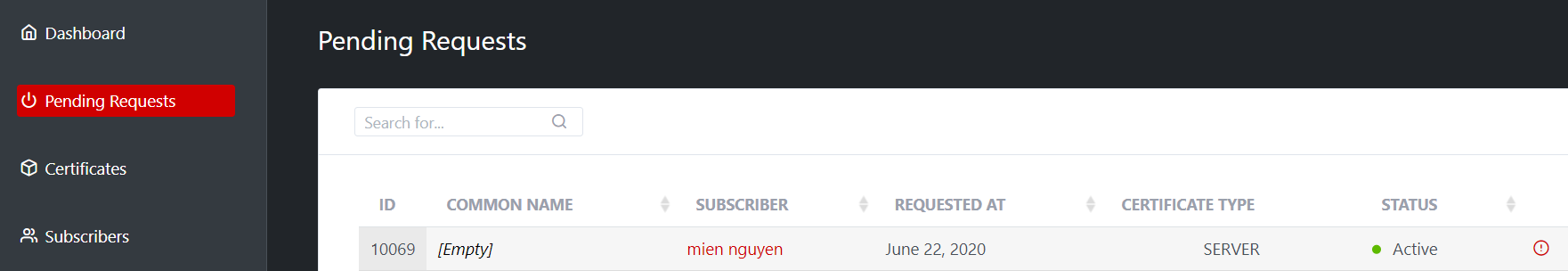
**Administrator:**

All pending certificate requested are listed in Dashboard and Pending Requests page:

Administrator Dashboard:



Pending Requests page:



**Subscriber** also can:

* View detail of a certificate request
* “Delete” a Certificate request.
* Download a CSR from certificate request detail

**Administrator** also can:

* Approve a certificate request
* Reject a certificate request
* Download a CSR from certificate request detail

### Server Certificate Request Detail page

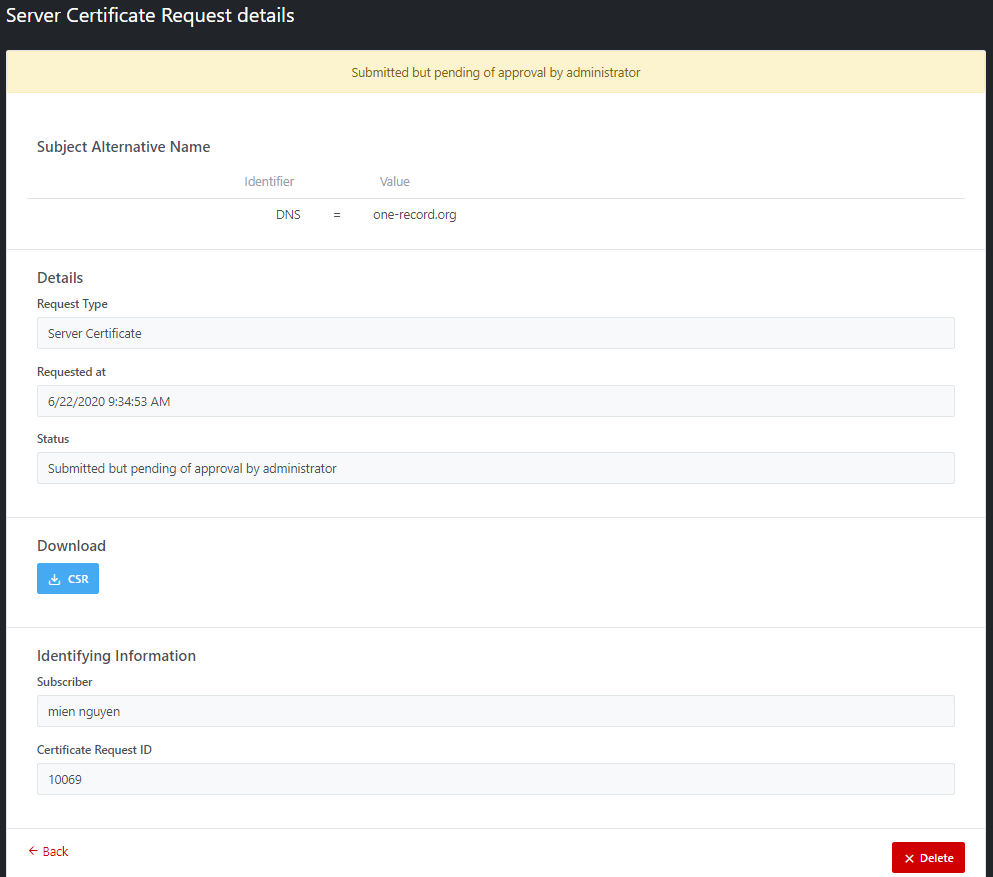
Any new request will show status in detail page: Submitted but pending of approval by administrator

**Subscriber:**

View detail page. The possible operations are:

* “Delete” a Certificate request.
* Download a CSR from certificate request detail

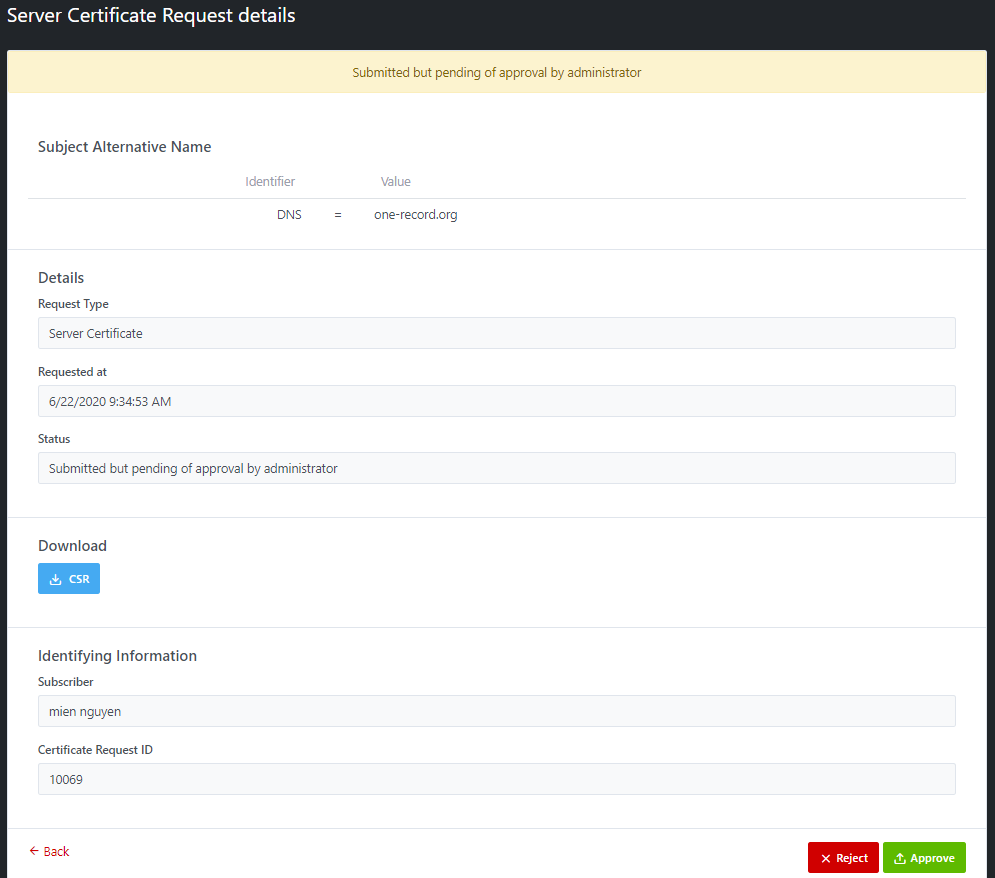
**Illustrative screen:**



**Administrator:**

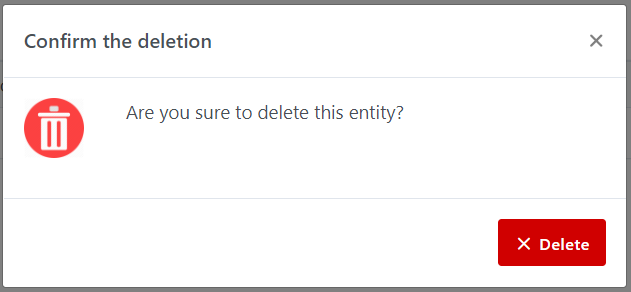
View detail page. The possible operations are:

* Approve request
* Reject request
* Download a CSR of that request



### Delete a Server certificate request

Only **Subscriber** can delete a **pending/rejected** certificate request by clicking **Delete** button in Certificate request detail page. A confirmation popup window will be displayed before deleting.



When a request is deleted, it will not be shown in Certificate list page of Subscriber, as well as Dashboard, and Pending Requests page of IATA Administrator.

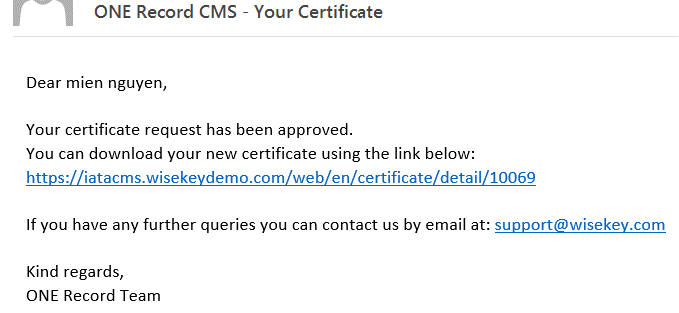
### Approve a Server Certificate Request

Only **IATA Administrator** can approve the certificate request by clicking **Approve** button in view request detail page

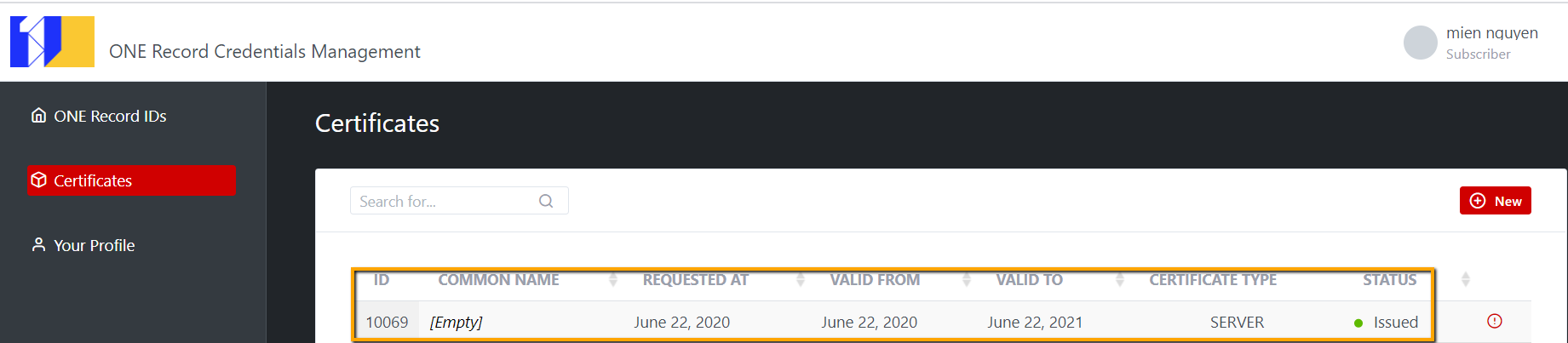
After request is approved, Certificate is issued, a notification email about certificate is issued will be sent to Subscribers. Status of request is changed from Pending to Issued on both Subscribers (Certificate list page) and Administrator (Pending request page)

**Illustrative screen:**

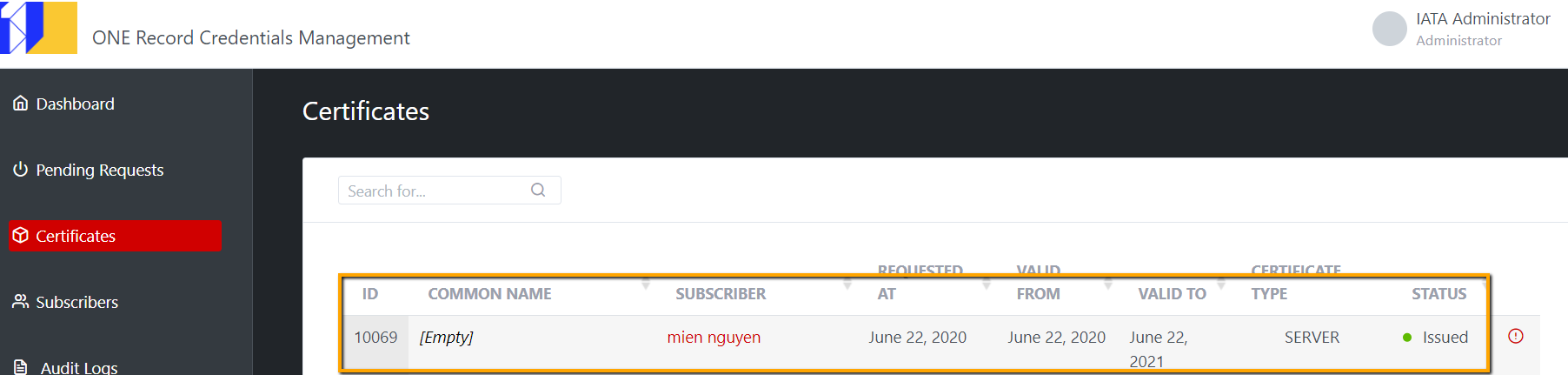
Email notification:



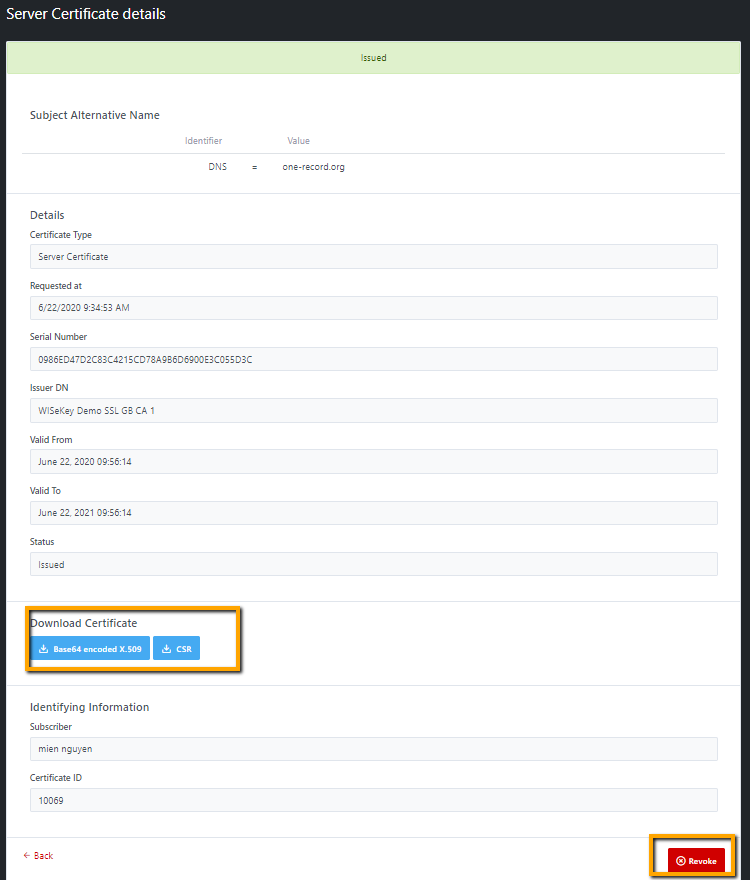
Subscriber (Certificate list page)



Administrator (Pending request page)



Certificate detail page:



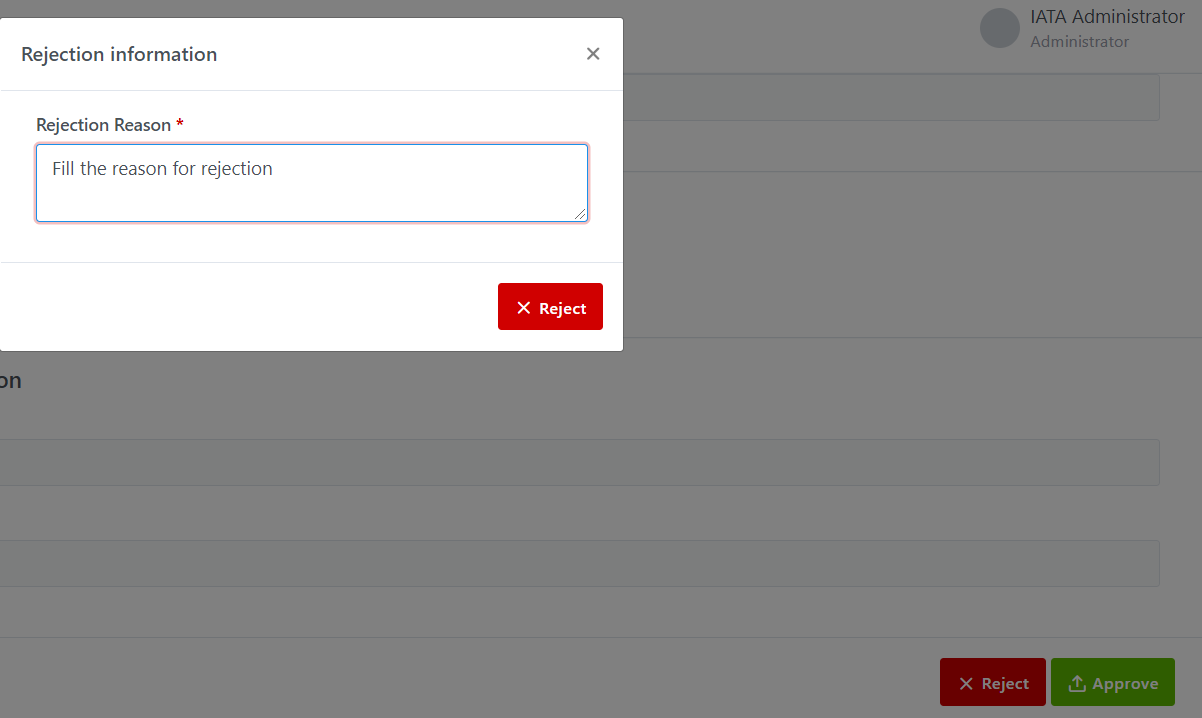
There is no PFX for Server Certificate, only Base64 encoded X.509 is available for downloading server certificate

NOTE:

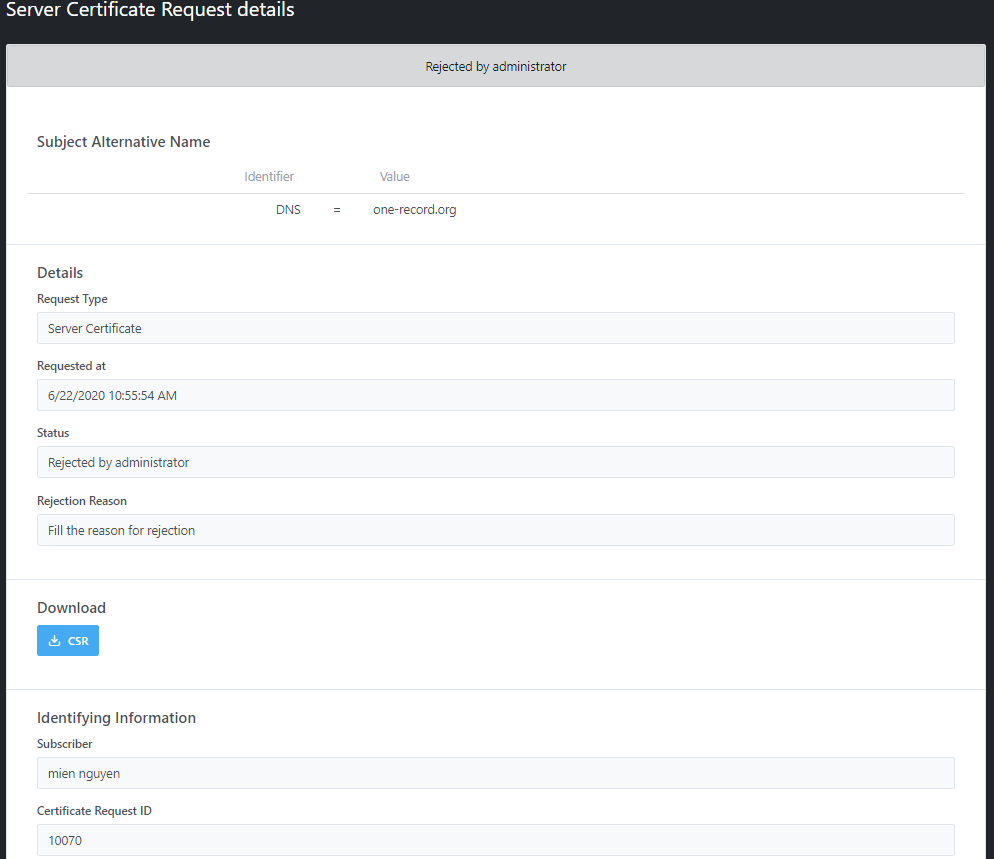
Dashboard page only show pending requests, so approved request will not be shown here. After request is approved, it will be shown in Certificate page.

### Reject a Server Certificate Request

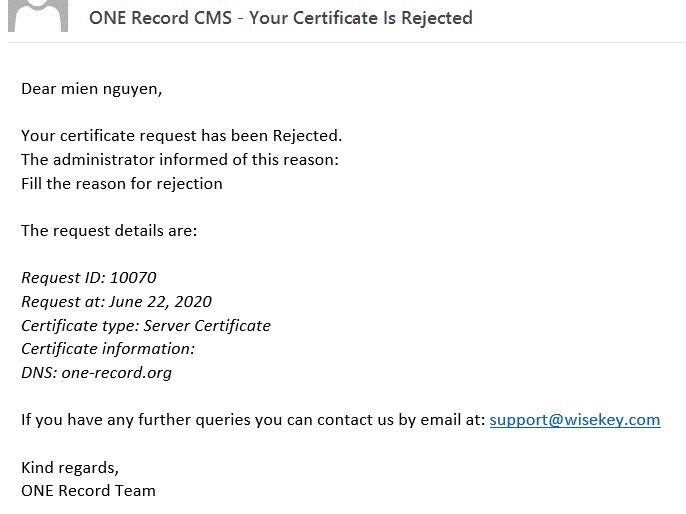
Only **IATA Administrator** can approve the certificate request by clicking **Reject** button in view request detail page, and enter the reason for rejecting.



After request is rejected, a message will be shown:

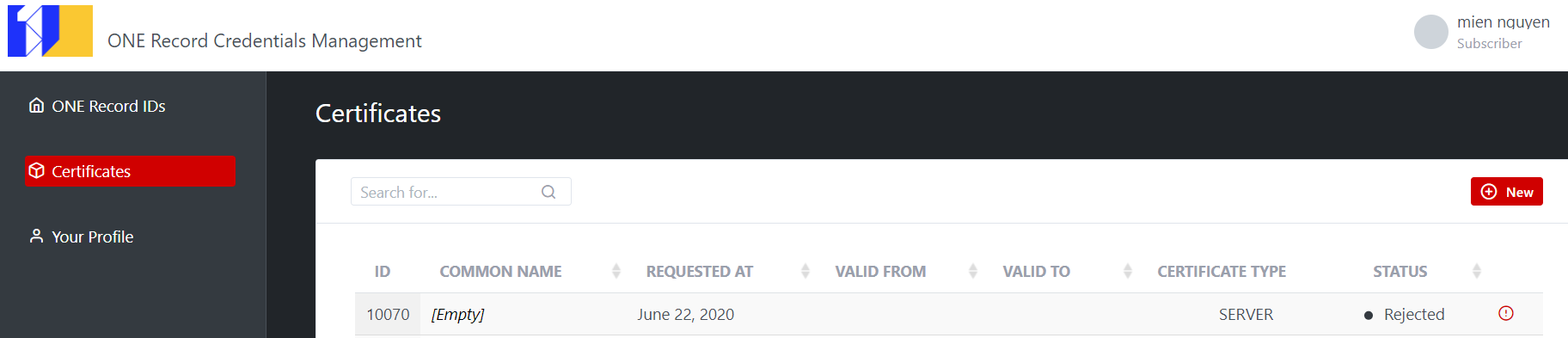


And a notification email about request is rejected will be sent to Subscriber

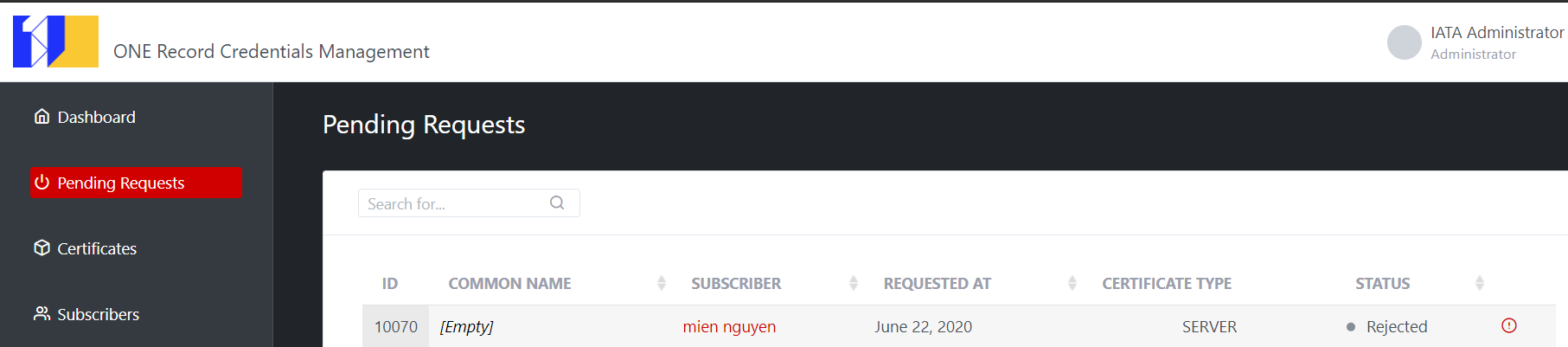


The status of the request is updated to Rejected in both Subscribers (Certificate list page) and Administrator (Pending Request page).

Subscriber (Certificate list page)



Administrator (Pending request page)



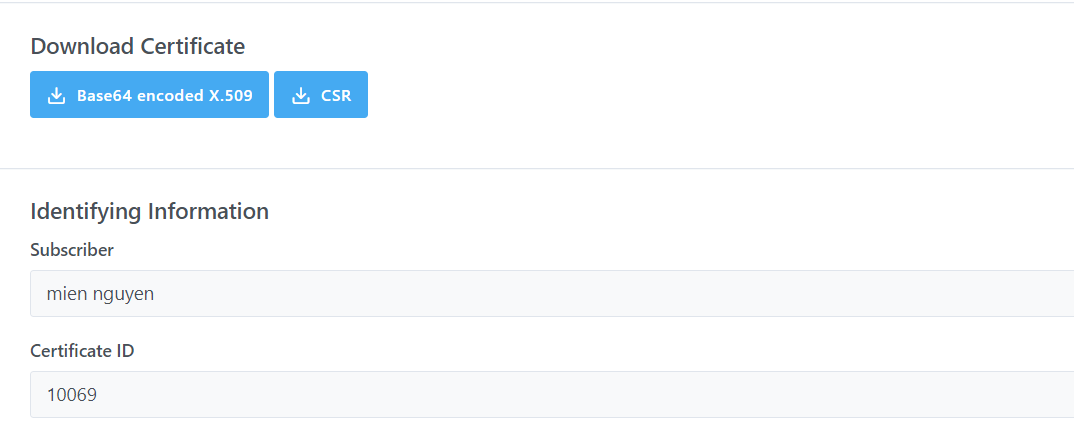
NOTE: Dashboard page only show pending requests, so rejected request will not be shown here.

### Download an Issued Server Certificate

Both Subscriber and IATA administrator can download certificate, there are 3 options to be downloaded:

* Base64 encoded X.509
* CSR

You can click Base64 encoded X.509 (.crt) and CSR to download Server Certificate

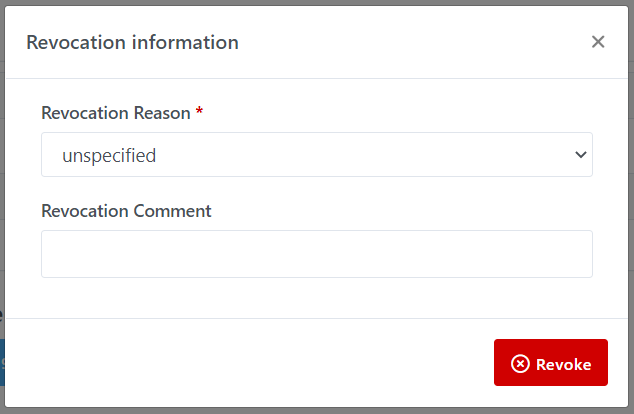


### Revoke a Server Certificate

Step to revoke a certificate:

**Step 1:** Open a certificate to view detail and scroll down to the end to find the **Revoke** button

**Step 2:** Click on **Revoke** button, you will see a popup window **Revocation information**

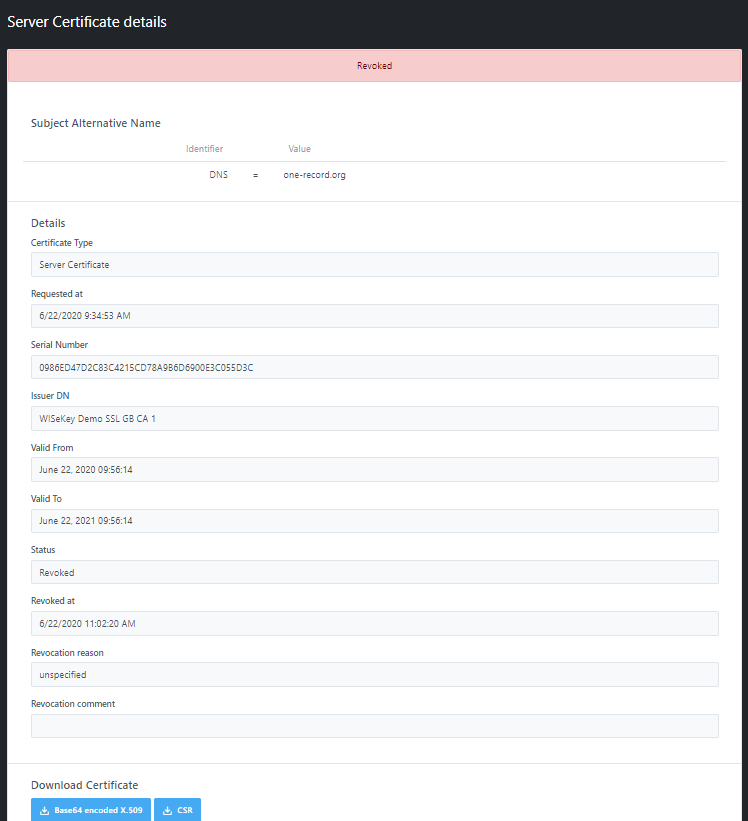


**Step 3:** Select any Revocation Reason and put, optionally, your Revocation Comment. Then Click on Revoke button to confirm

A screenshot of a cell phone

Description automatically generated

**Step 4:** Certificate is revoked successfully, and the status is shown as Revoked.



The status of Revoked Certificate is Revoked and updated on Certificate list page of Subscribers and IATA Administrator.

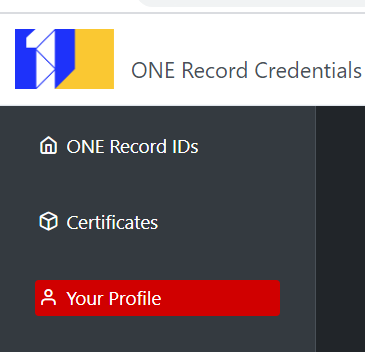
# User Profile Management

Pre-requisite:

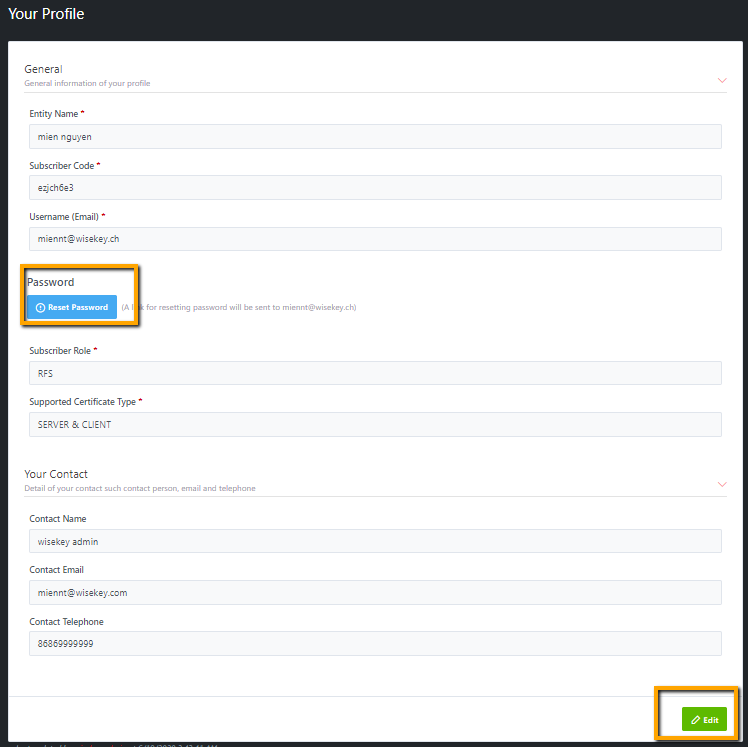
* User have to be logged-in with his/her own account.

## Update Profile

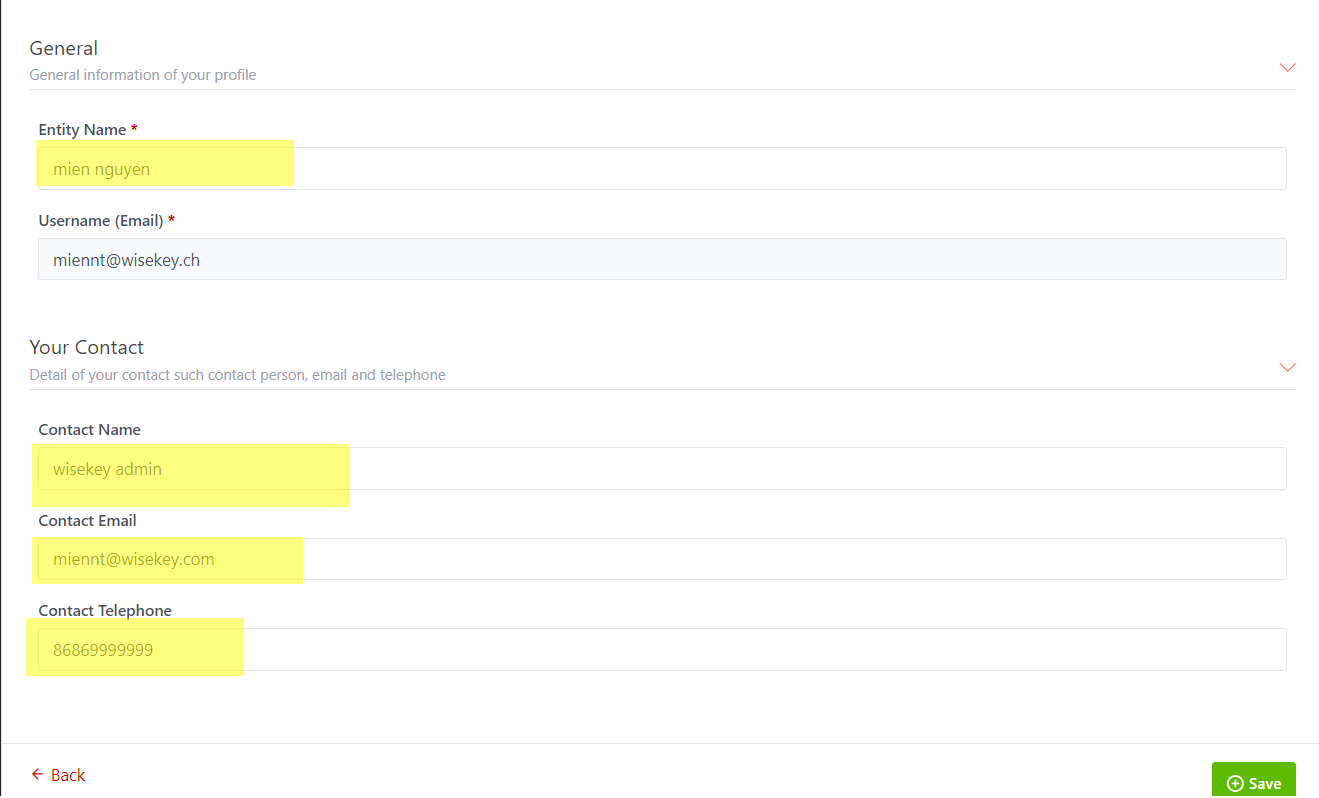
Any user can update his profile by clicking **Your Profile** on left-menu:



**Step 1:** In your profile screen, scroll down and find button “Edit”, click on this button to update/modify your profile



**Step 2:** It’s possible toedit all information EXCEPT username. Email field is for contact email address



**Step 3:** Click on SAVE button then all your changes will be updated. The updated infor of any user will be shown correctly in Subscribers detail screen when viewing using Admin account.

## Reset password

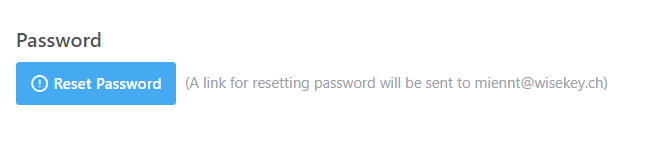
Reset password feature is available in Your Profile page. Any user can reset password of his/her own account.

Steps detail to reset password:

**Step 1:** Open Profiles

**Step 2:** Scroll down to find “Reset Password” in Your Profile page and click on this button. A for resetting password will be sent to **username email address.**

**For example:**



**Step 3:** Check your email and click on the link to reset your password.

