EVERTRUST

OCSPd (legacy)

Version 3.1.3, 2025-06-20

Table of Contents

1. Installation

1.1. Introduction

Description

OCSPd (OCSP daemon) is an OCSP responder compliant with the following RFCs:

- RFC 6960
- RFC 5019

This project is powered up by:

- Akka
- BouncyCastle
- EHCache
- H2 Database
- IAIK PKCS#11 Wrapper
- Kamon
- Play! Framework
- Scala
- NGINX

This document is specific to OCSPd version **3.1.3**.

Scope

This document is an installation procedure detailing how to install and bootstrap OCSPd on a server running **CentOS/RHEL 6.x/7.x/8.x x64**.

Out of Scope

This document does not describe how to configure and operate an OCSPd instance. Please refer to the administration guide for administration related tasks.

1.2. Pre-requisites

This section describes the system and software pre-requisites to install OCSPd.

Hardware pre-requisites

The minimum requirements for running OCSPd are:

- 2 CPU cores;
- 8 GB of RAM;
- 500 GB of free disk space.

System pre-requisites

The following elements are considered as system pre-requisites:

- A server running CentOS / RHEL [6-7-8].x x64 with the network configured;
- Access with administrative privileges (root) to the server mentioned above;
- The IP address / DNS Name of one or several NTP server(s);
- The IP address / DNS Name of an SMTP relay;
- The email address of the OCSPd server administrator.

Software pre-requisites

The following elements are considered as software pre-requisites:

- The OCSPd installation package: `ocspd-3.1.3.noarch.rpm`;
- The NGINX installation package: `nginx-latest.el8.ngx.x86_64.rpm` (latest version of the nginx web server);
- Java 11: The latest Java 11 OpenJDK package (will be installed as a dependency of OCSPd but may required when working offline);

1.3. Installation Procedure

1.3.1. Installing NGINX

1. Upload the file `nginx-latest.el8.ngx.x86_64.rpm` through SCP under `/root`;
2. Access the server through SSH with an account with administrative privileges;
3. Install the NGINX web server using the following command:

```
yum localinstall /root/nginx-latest.el8.ngx.x86_64.rpm
```

4. Enable NGINX to start at boot using the following command:

```
systemctl enable nginx
```

5. Stop the NGINX service with the following command:

```
/etc/init.d/nginx stop
```

1.3.2. Installing the rngd service

1. Access the server through SSH with an account with administrative privileges;
2. Install the `rng-tools` package with the following command:

```
yum install rng-tools
```

3. Configure the `rngd` service with the following command:

```
echo 'EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 10 -W 2048"' >
/etc/sysconfig/rngd
```

4. Enable and start the `rngd` service:

```
systemctl enable rngd
systemctl start rngd
```

1.3.3. Installing OCSPd

1. Upload the file `ocspd-3.1.3-1.noarch.rpm` through SCP under `/root`;
2. Access the server through SSH with an account with administrative privileges;
3. Install the OCSPd package with the following command:

```
yum localinstall /root/ocspd-3.1.3-1.noarch.rpm
```

Installing the OCSPd package will install the following dependencies:

- `dialog`
- `java-11-openjdk-headless`

1.4. Configuration procedure

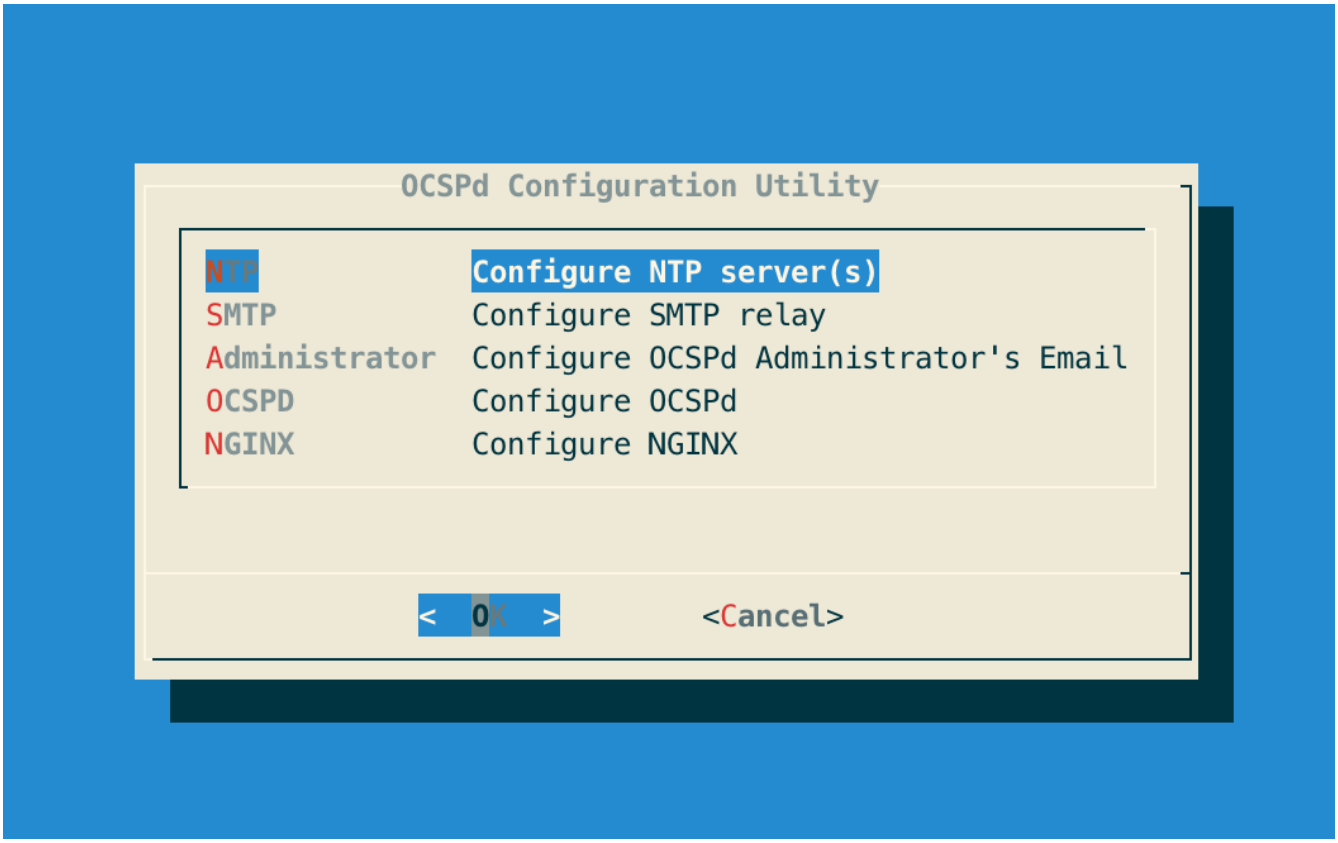
Configuring the NTP server(s)

Step 1: Access the server through SSH with an account with administrative privileges;

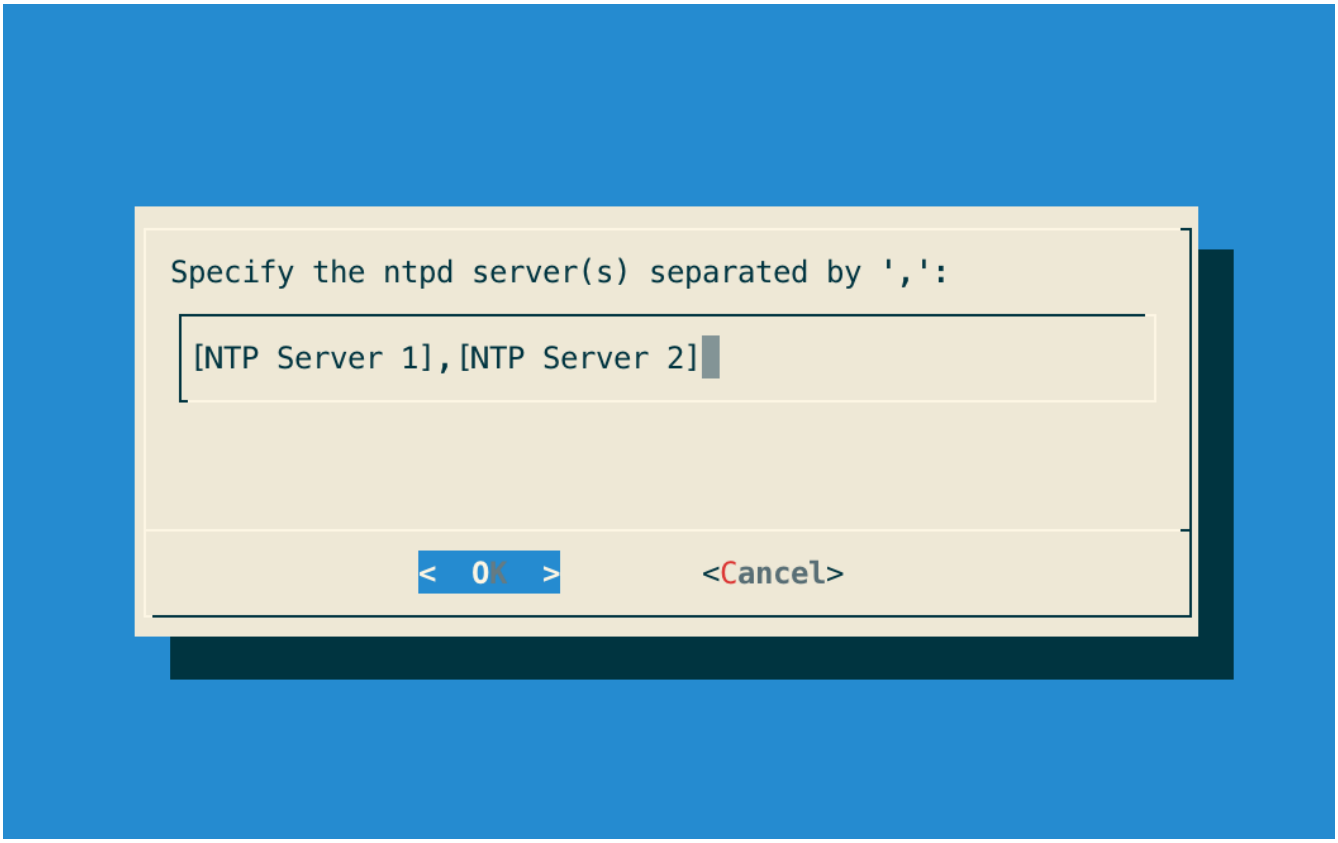
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

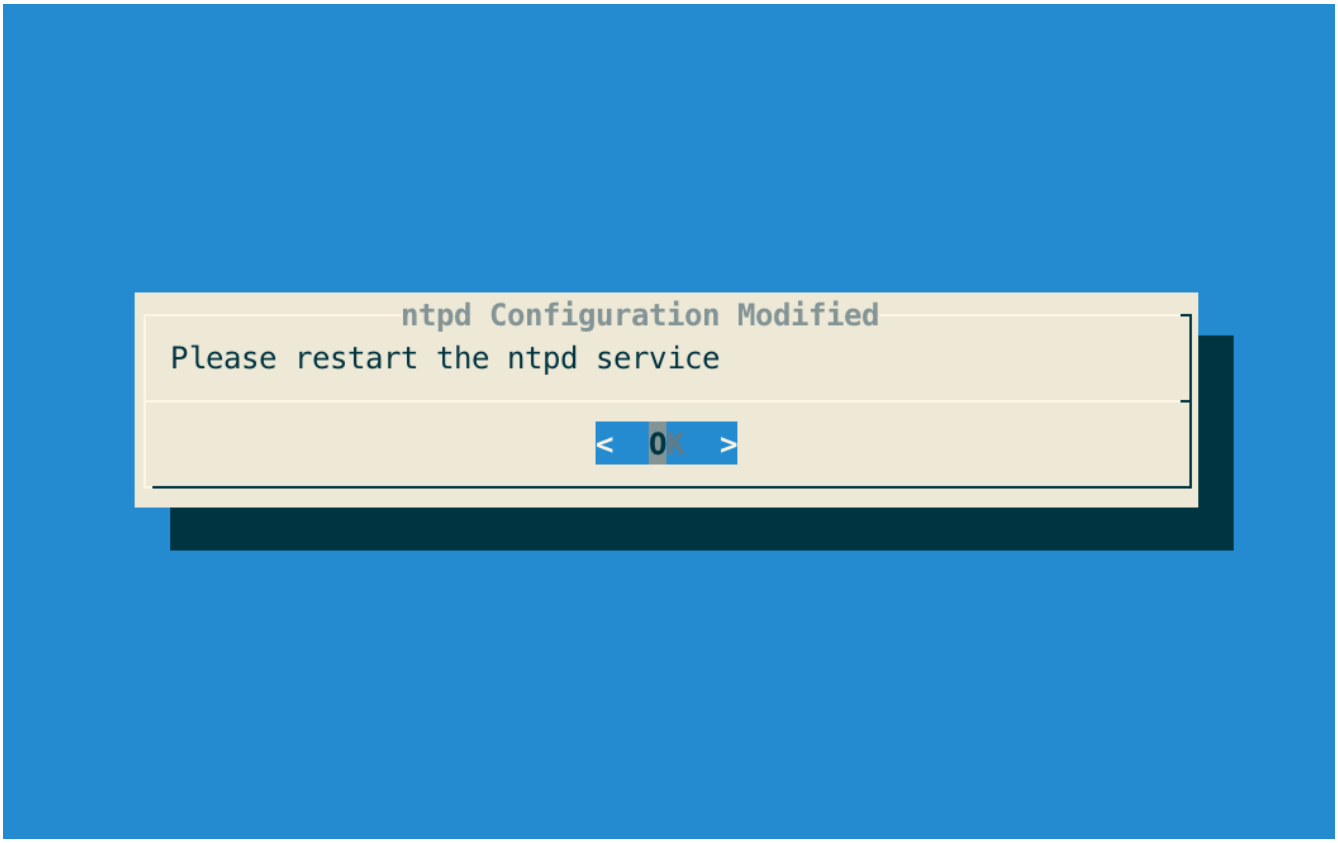
Step 3: In the main menu, select '**NTP**':



Step 4: Specify the list of NTP server(s) separated by ',' and validate:



Step 5: The NTPs configuration is updated:



Step 6: Exit the configuration utility and restart the NTPd service with the following command:

```
# /etc/init.d/ntpd restart
```

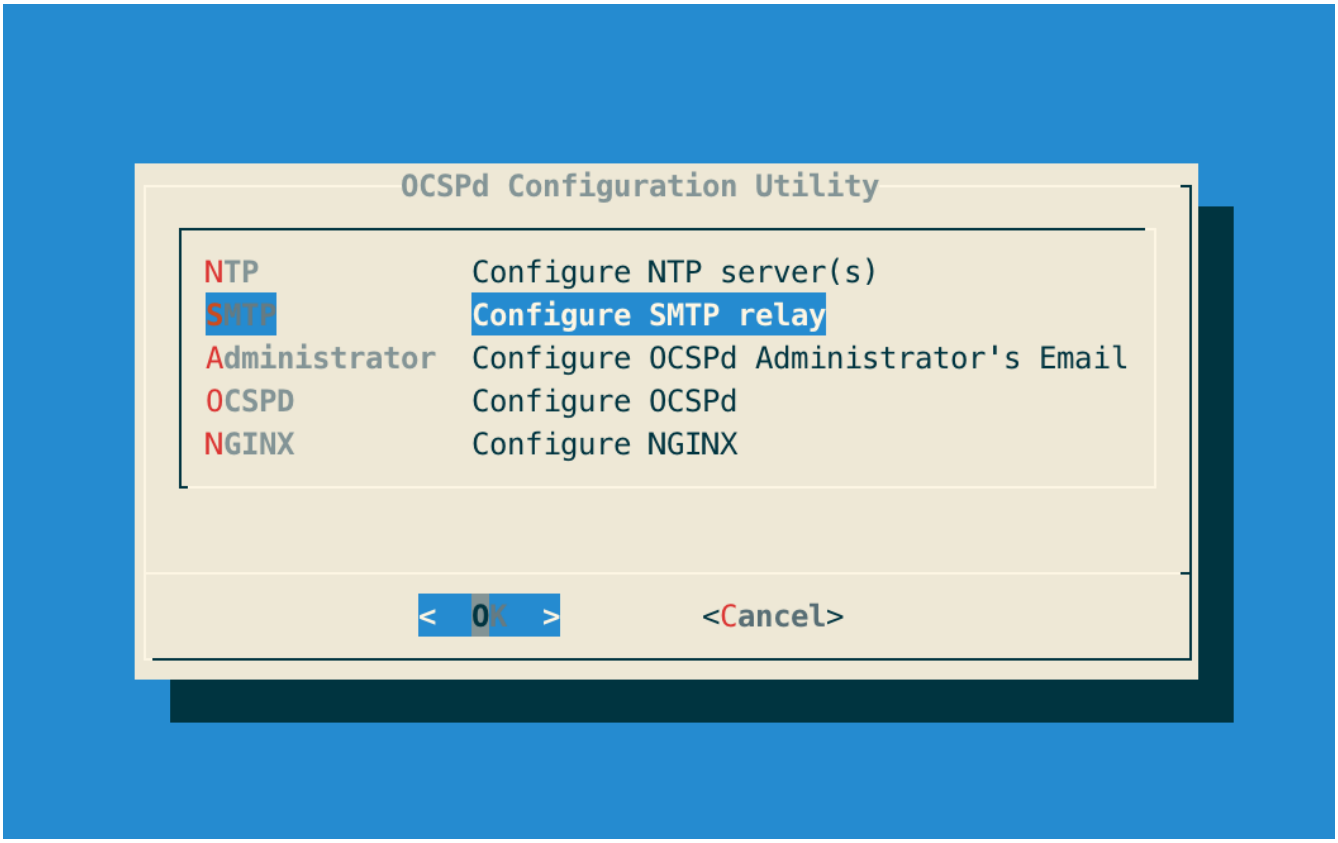
Configuring the SMTP Relay

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

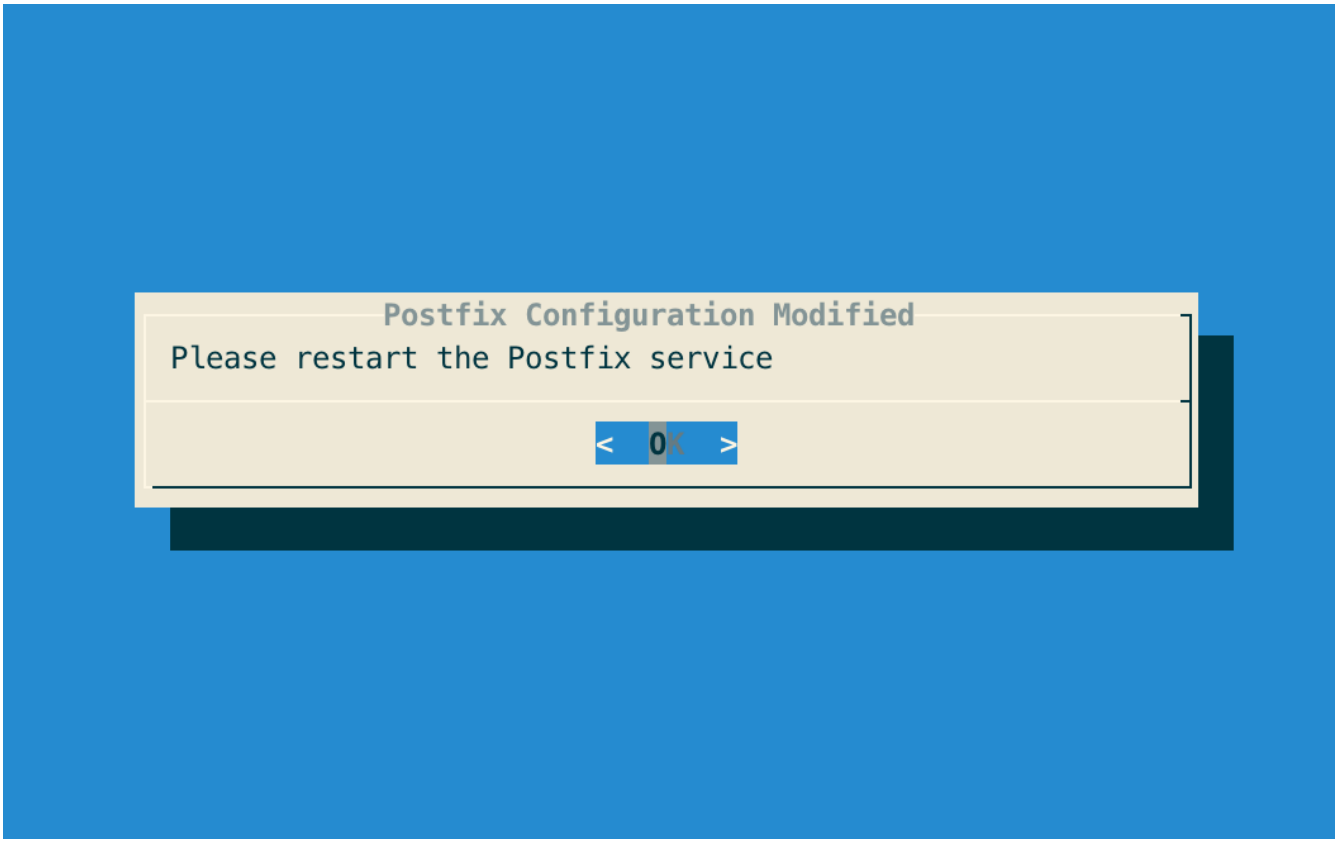
```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**SMTP**':



Step 4: Specify IP address or the DNS name of the SMTP relay and validate:

Step 5: The Postfix configuration is updated:



Step 6: Exit the configuration utility and restart the Postfix service with the following command:

```
# /etc/init.d/postfix restart
```

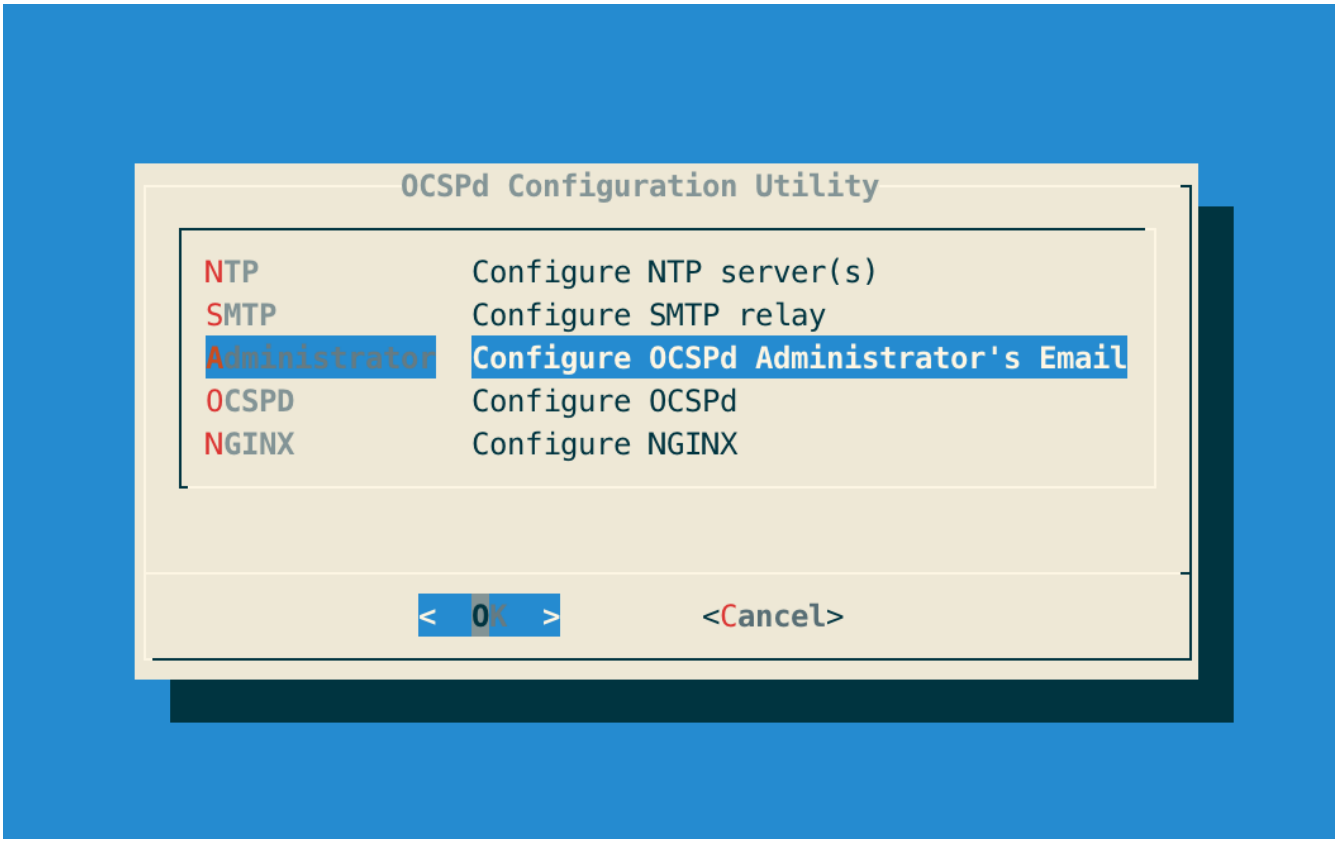
Configuring the OCSPd Administrator's Email Address

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**Administrator**':



Step 4: Specify the email address of the OCSPd Administrator and validate:

Step 5: Exit the Configuration Utility;

Step 6: Validate the SMTP relay and Administrator Email Address with the following commands:

```
# yum install mailx
```

```
# mail -s "Hello OCSPd" root
> Hello From OCSPd
.
```

Step 7: Ensure that the email defined step 4 receives the test email.

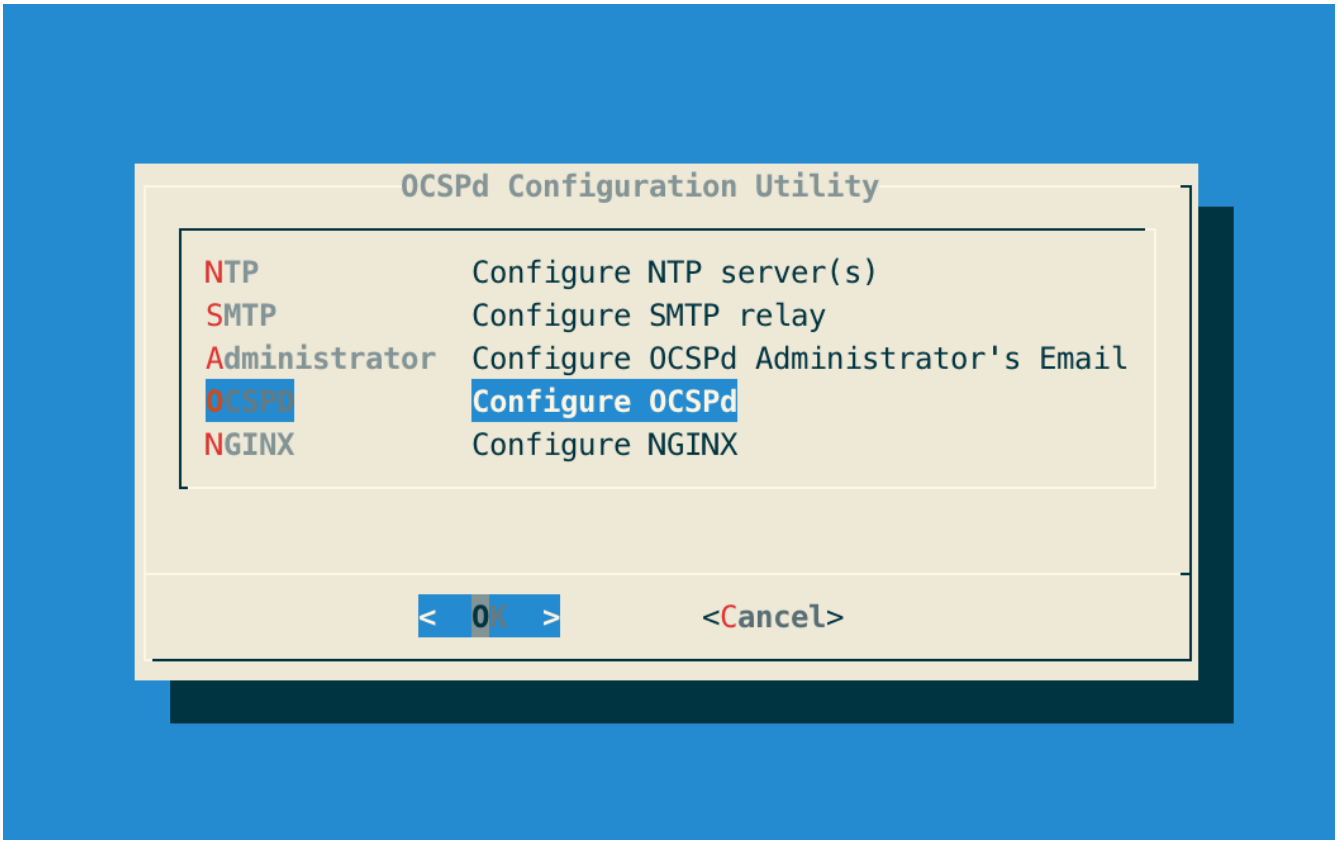
Configuring the Radius Server

Step 1: Access the server through SSH with an account with administrative privileges;

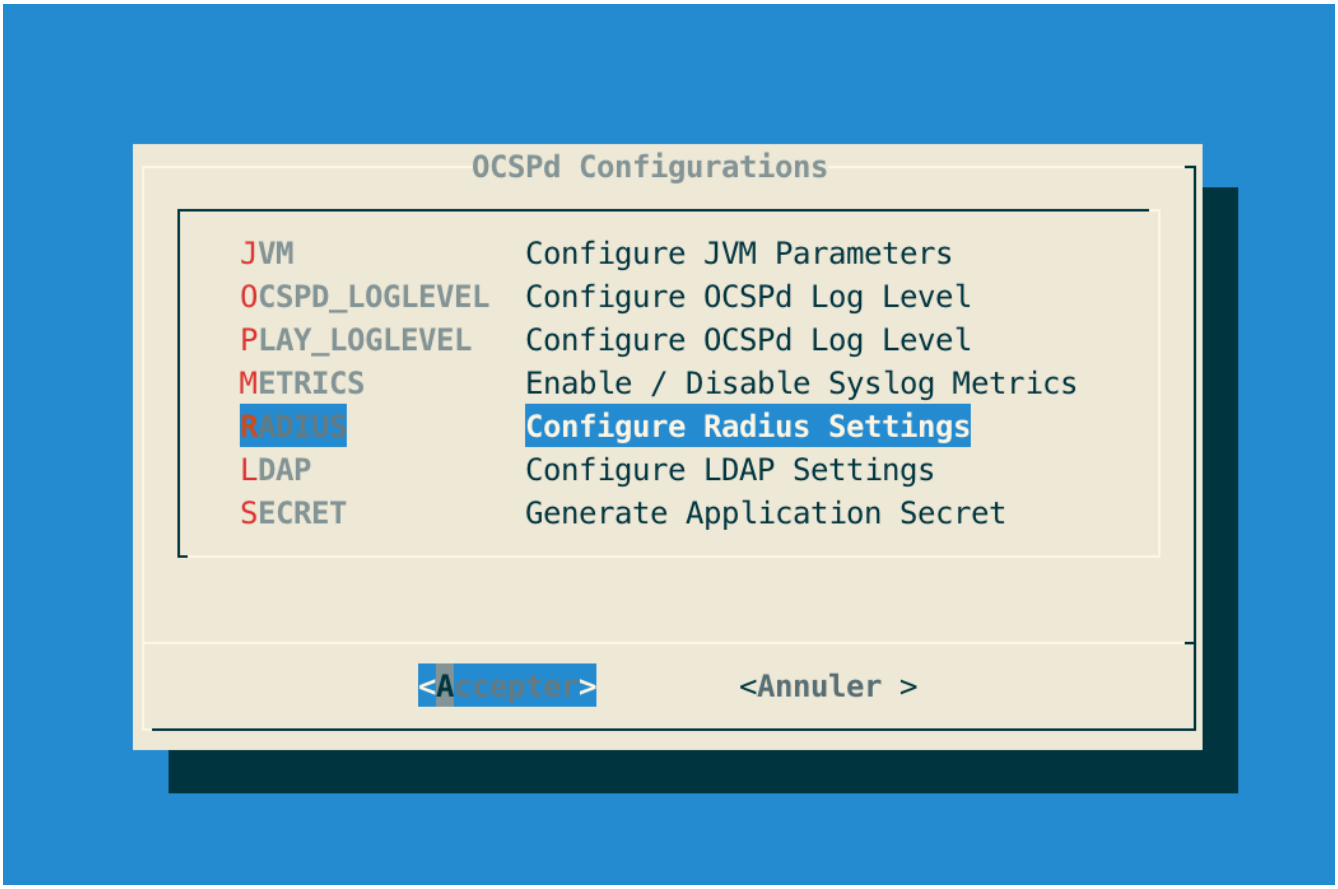
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**OCSPd**':

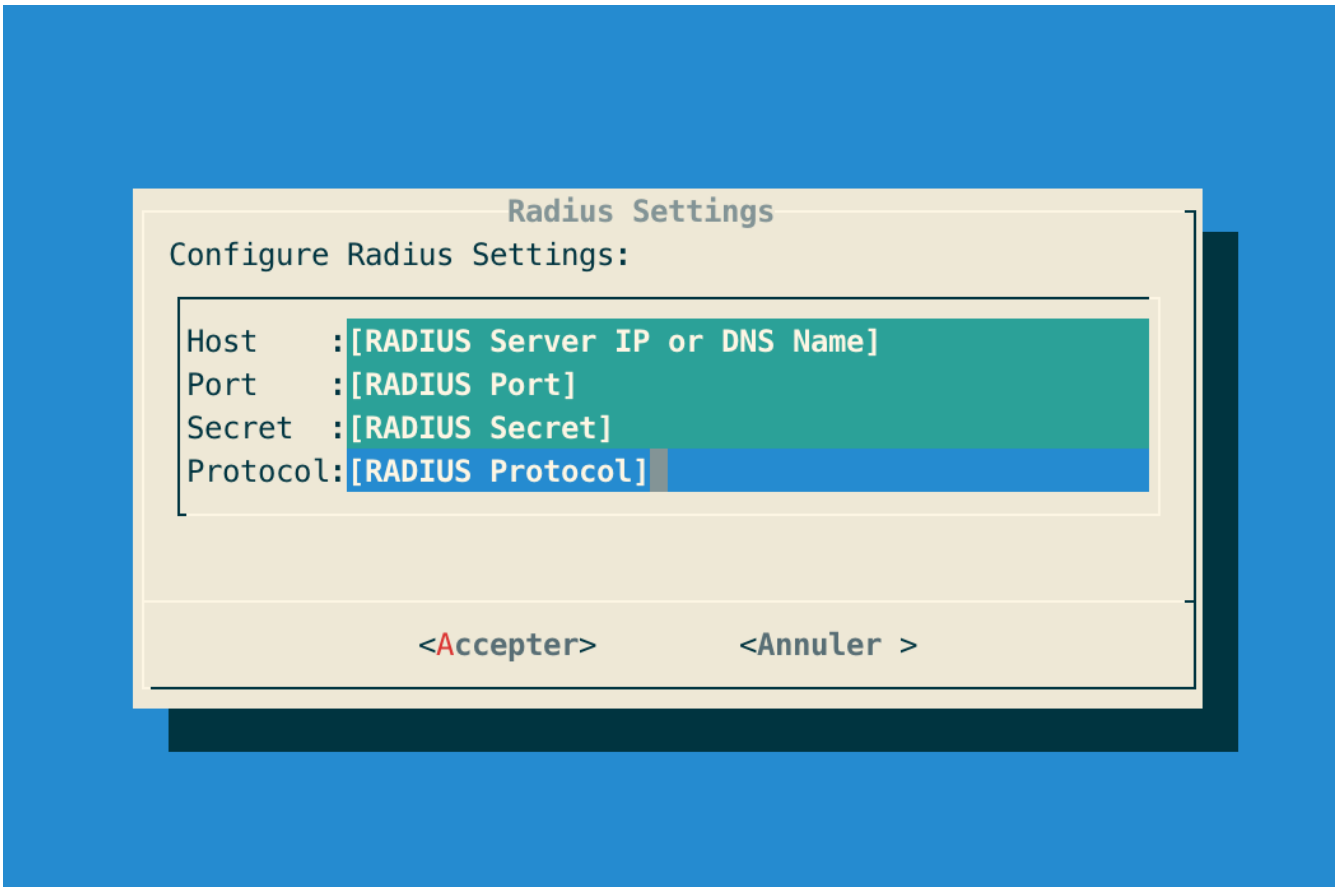


Step 4: In the OCSPd menu, select '**RADIUS**':

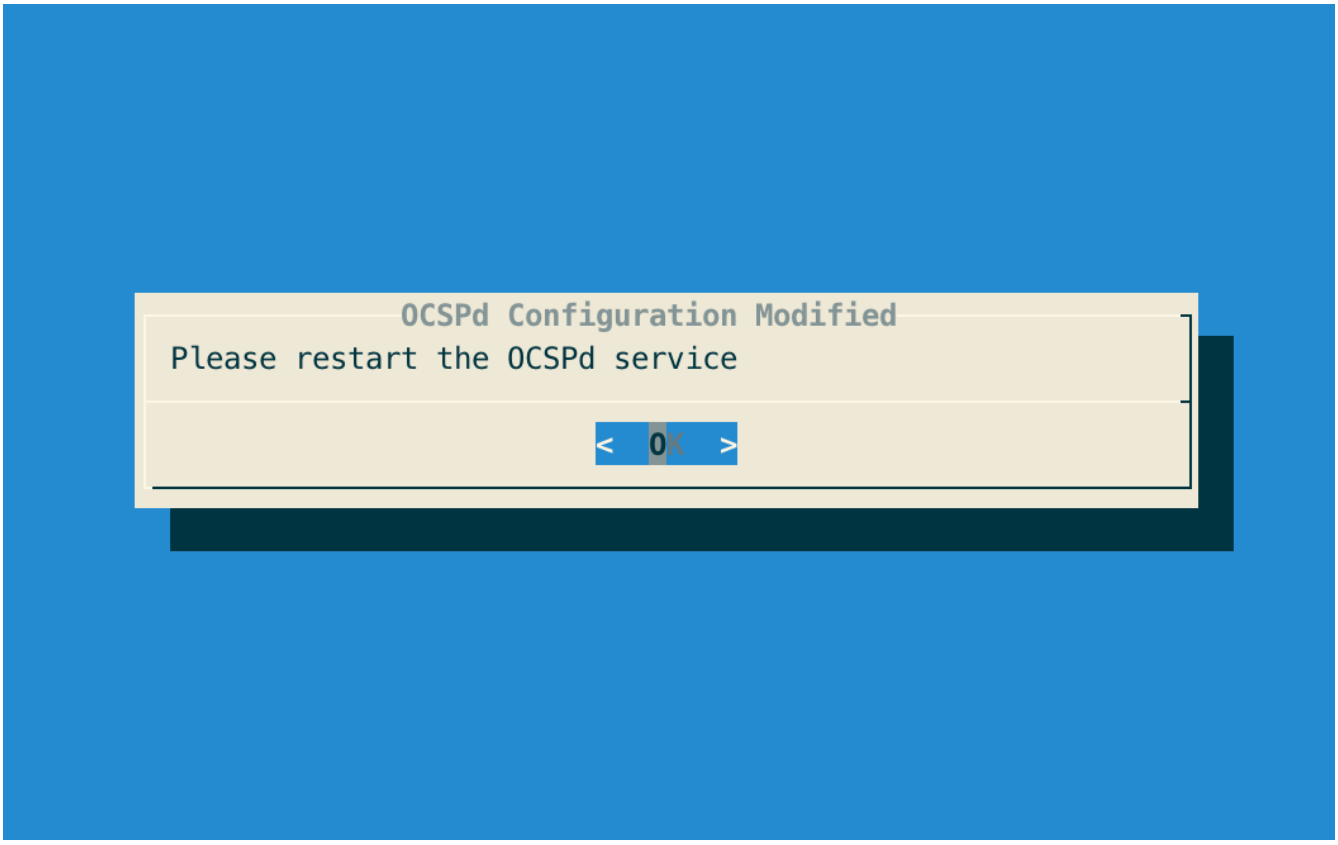


Step 5: Specify the following Radius configuration settings and validate:

'CHAP' and 'PAP' protocols are supported by OCSPd.



Step 6: The OCSPd configuration is updated:



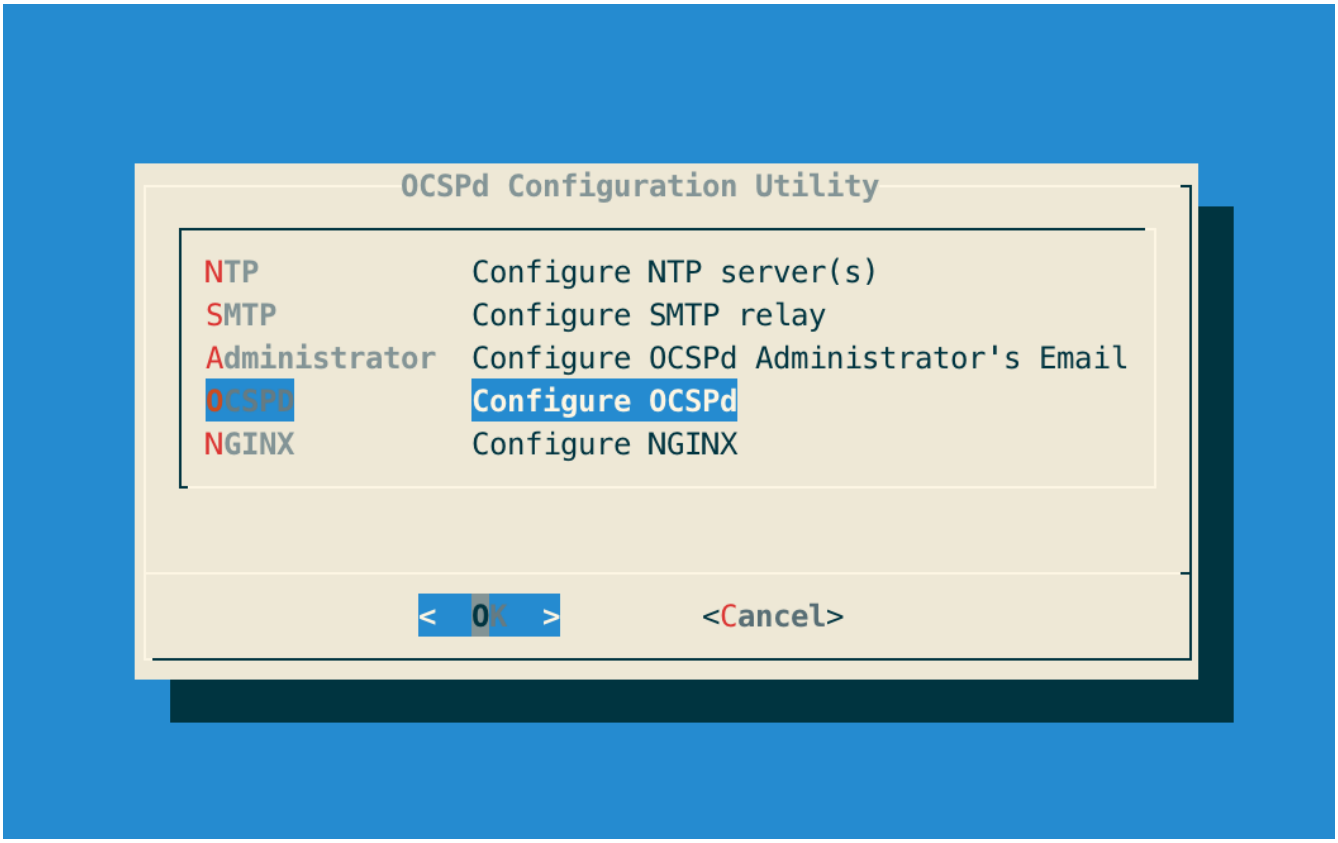
Configuring the LDAP Server

Step 1: Access the server through SSH with an account with administrative privileges;

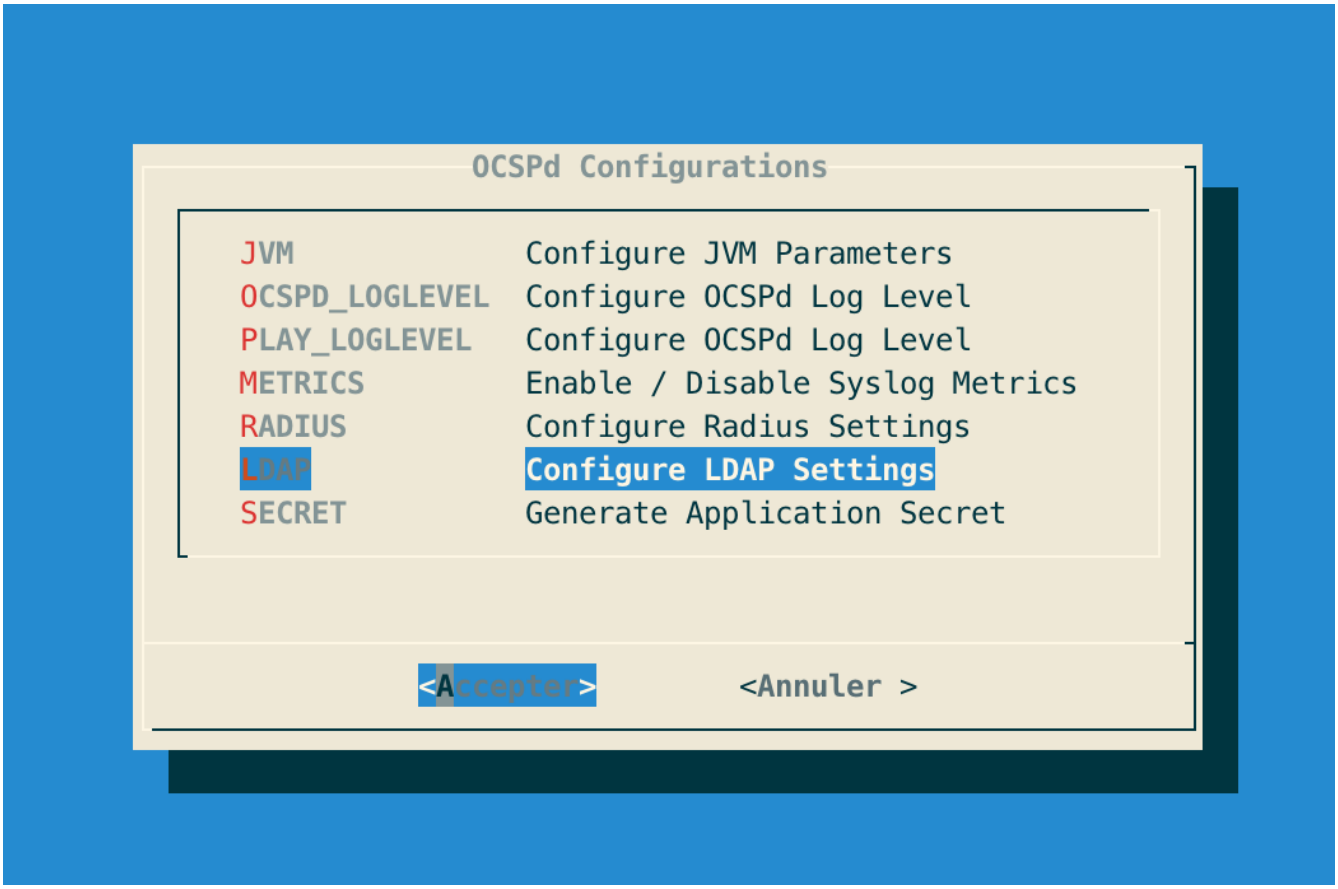
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**OCSPd**':



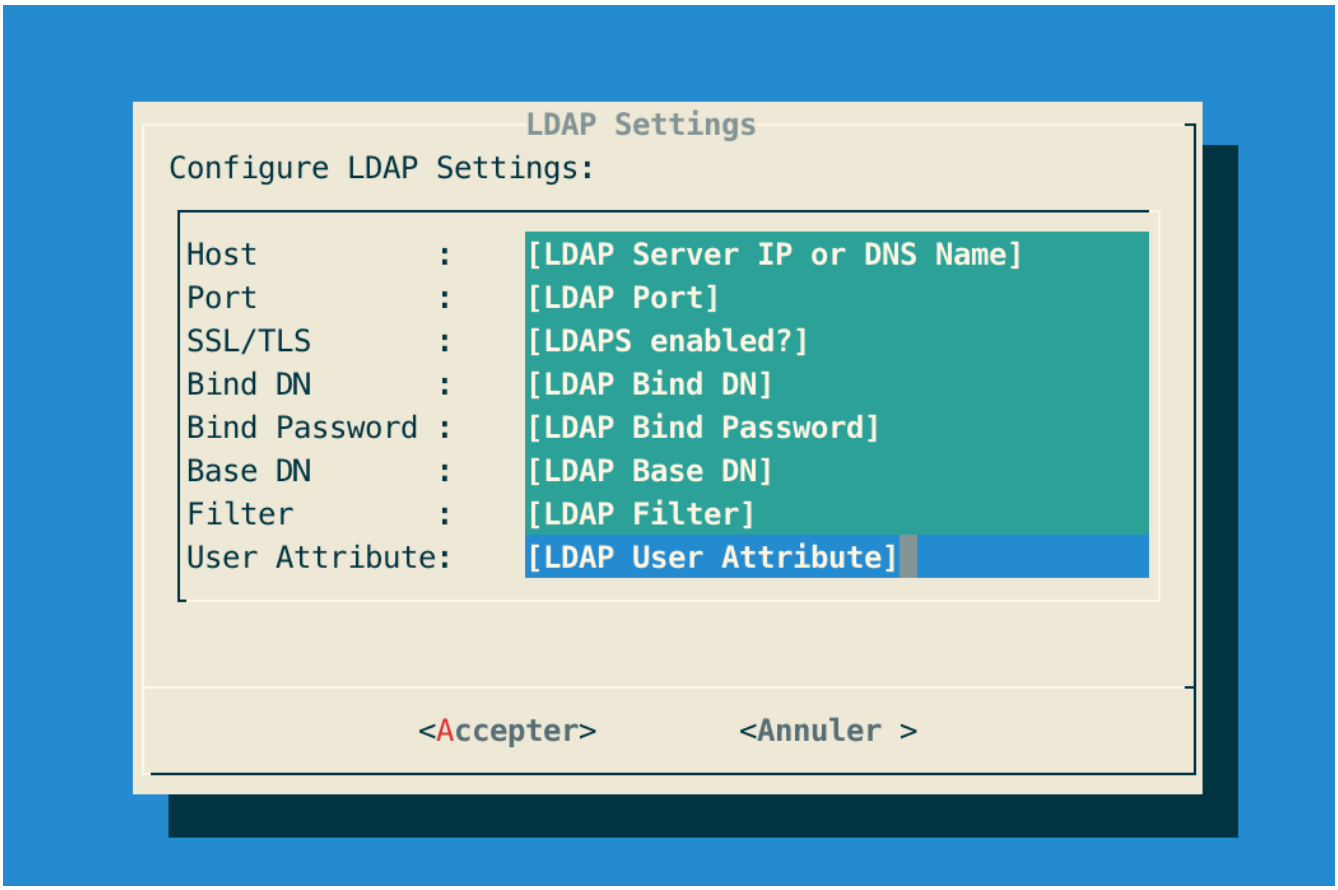
Step 4: In the OCSPd menu, select '**RADIUS**':



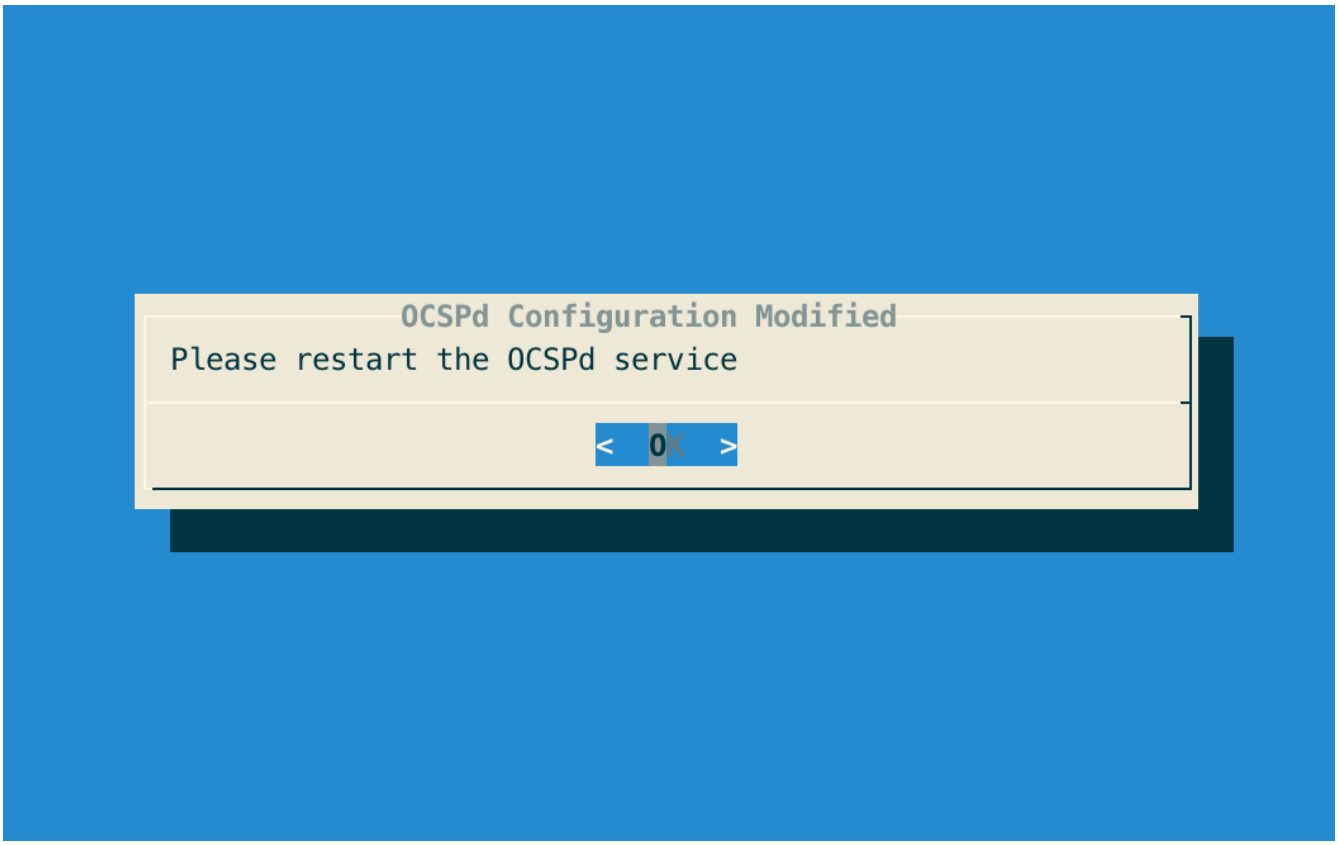
Step 5: Specify the following LDAP configuration settings and validate:

By default the LDAP configuration will use port 389 and SSL/TLS 'false'.

The filter settings is optionnal.



Step 6: The OCSPd configuration is updated:



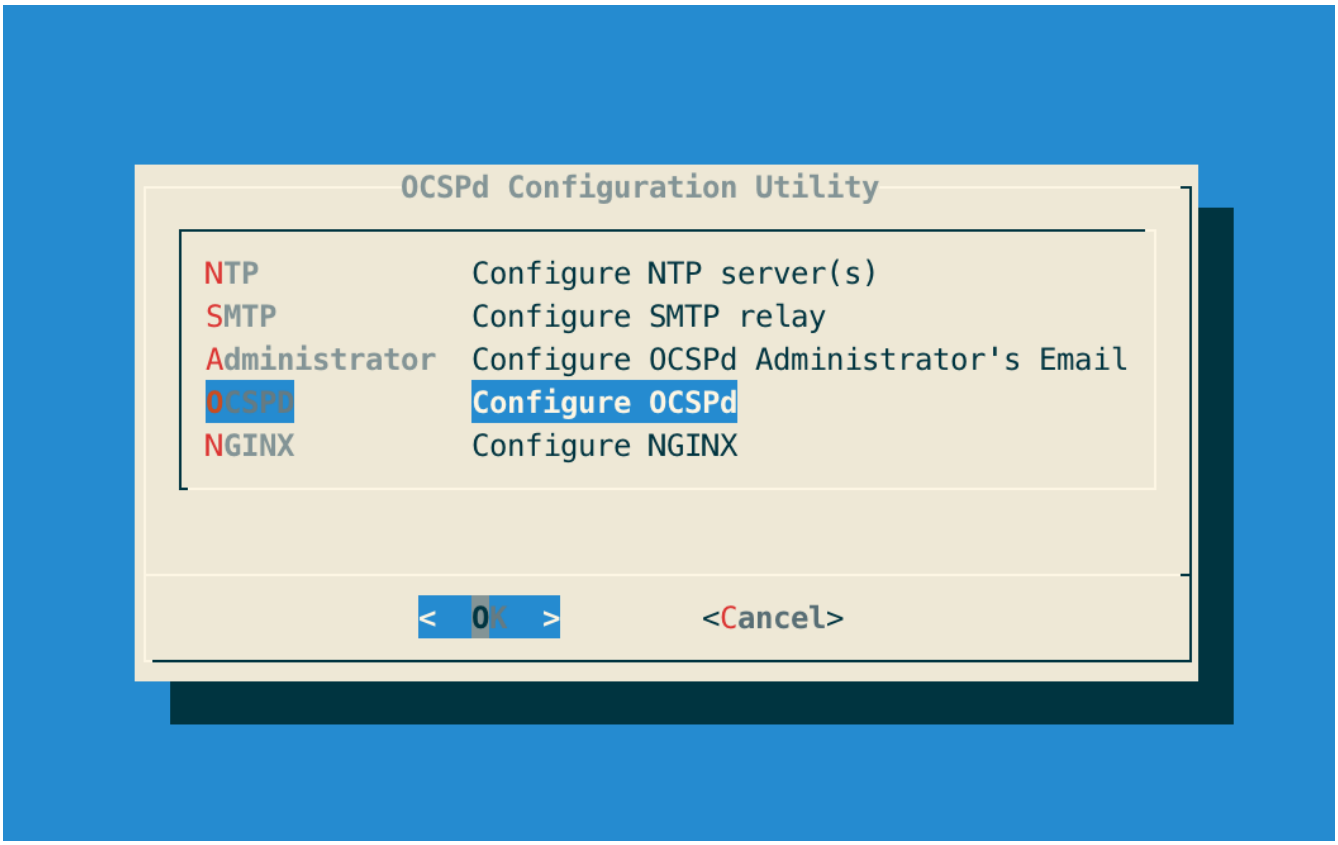
Generating a new OCSPd Application Secret

Step 1: Access the server through SSH with an account with administrative privileges;

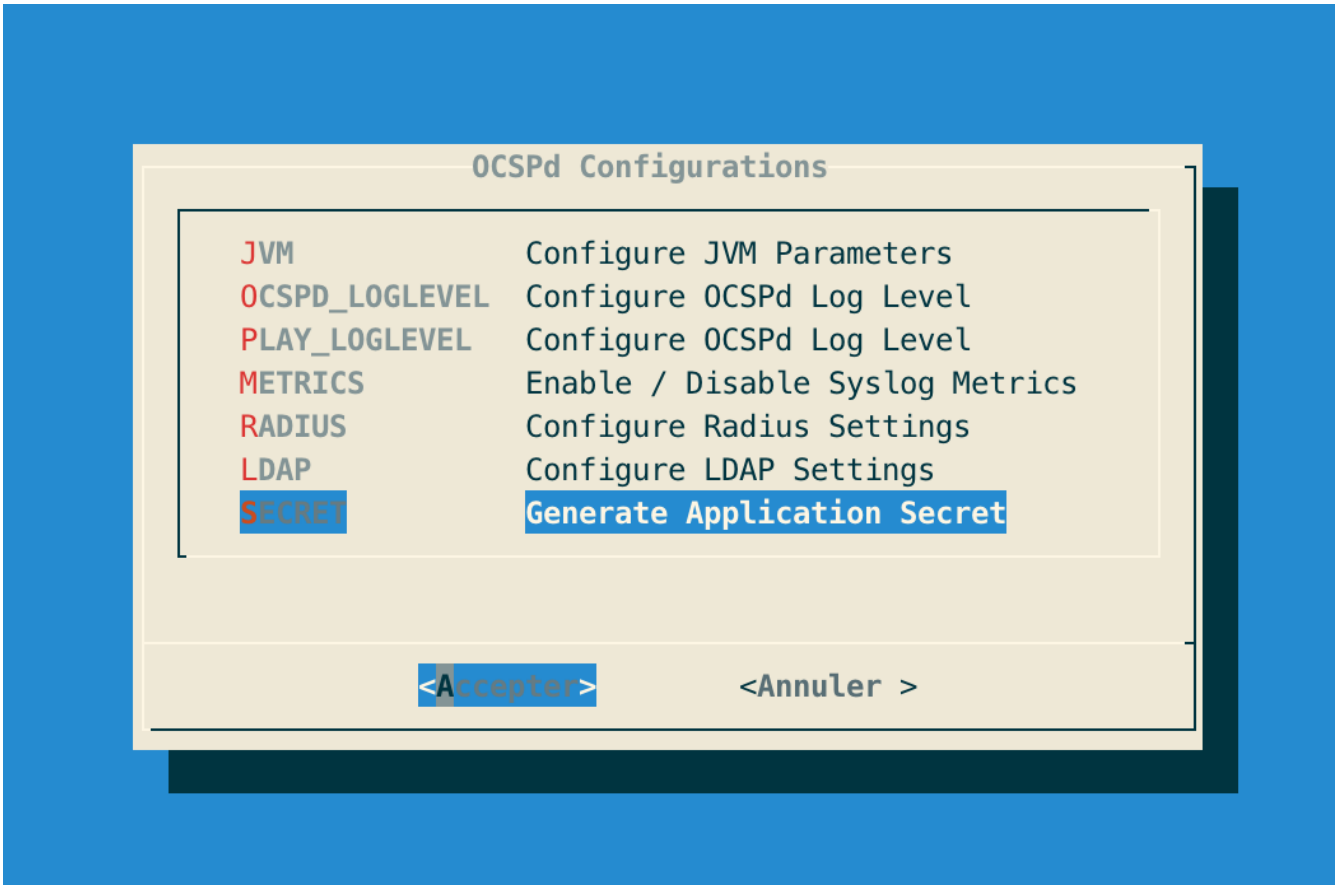
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

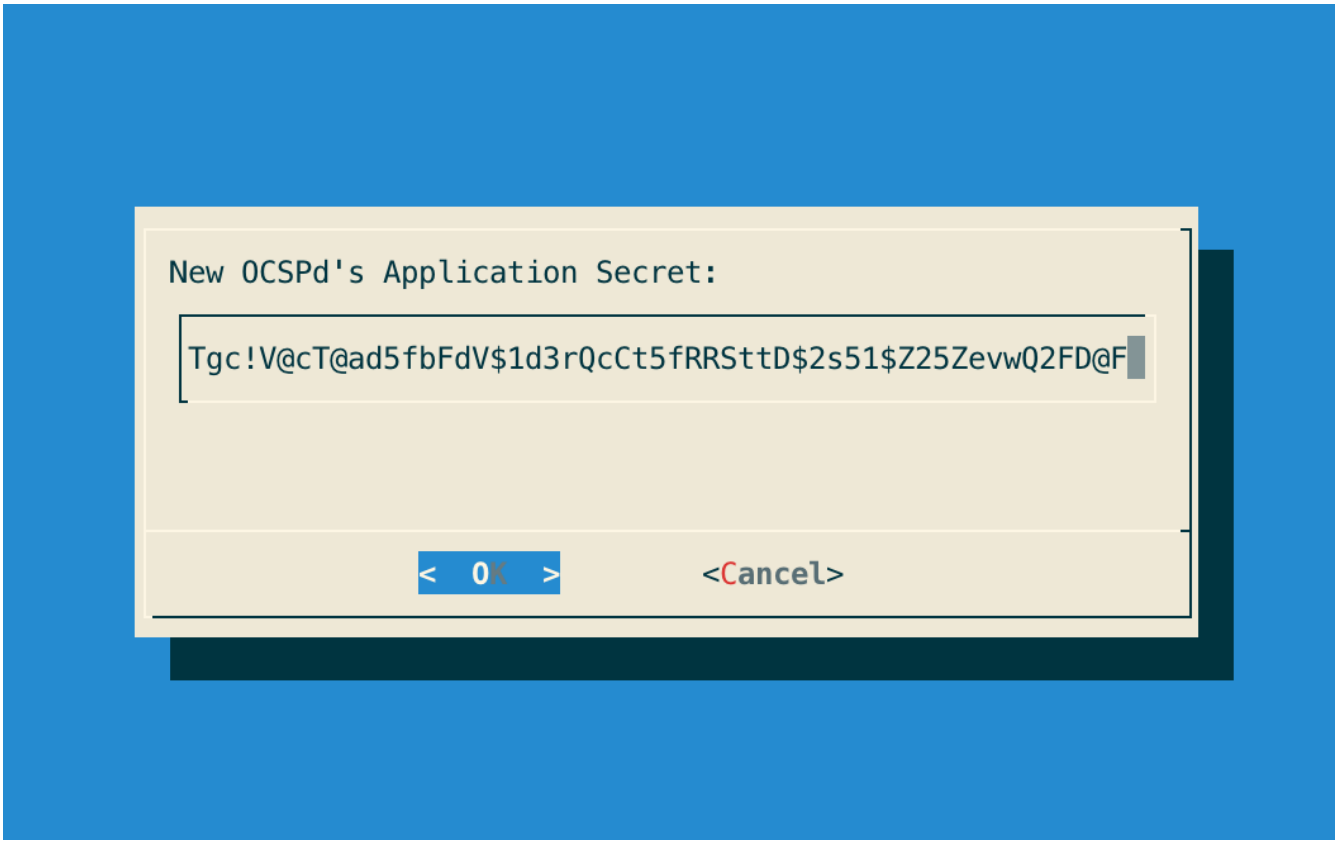
Step 3: In the main menu, select '**OCSPd**':



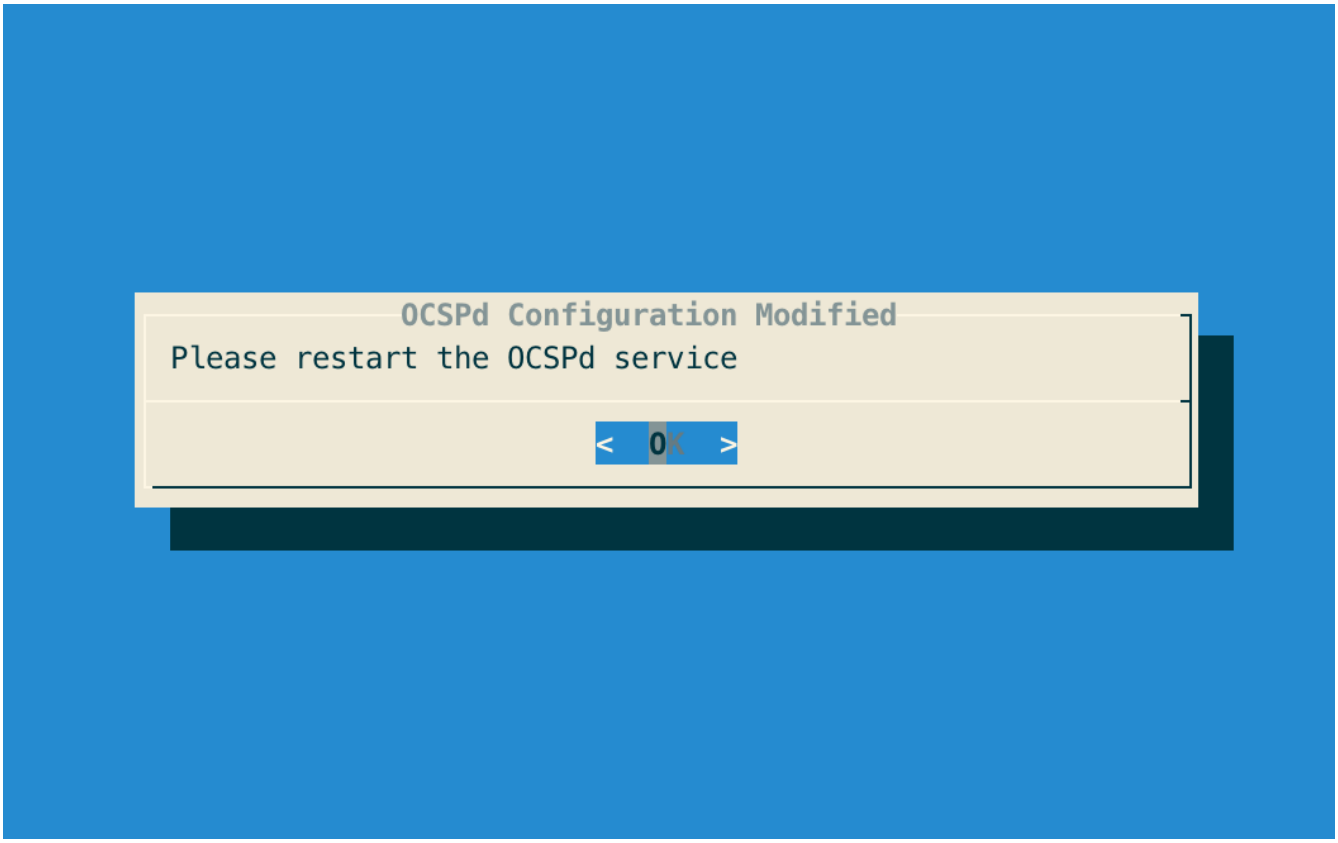
Step 4: In the OCSPd menu, select '**SECRET**':



Step 5: Validate the new OCSPd Application Secret:



Step 6: The OCSPd configuration is updated:



Installing the OCSPd license

Step 1: Upload the 'ocspd.lic' file through SCP under '/tmp/ocspd.lic':

Step 2: Access the server through SSH with an account with administrative privileges;

Step 3: Move the license file and set the permissions using the following commands:

```
# mv /tmp/ocspd.lic /opt/ocspd/etc
# chown ocspd:ocspd /opt/ocspd/etc/ocspd.lic
# chmod 640 /opt/ocspd/etc/ocspd.lic
```

1.4.1. Configuring NGINX

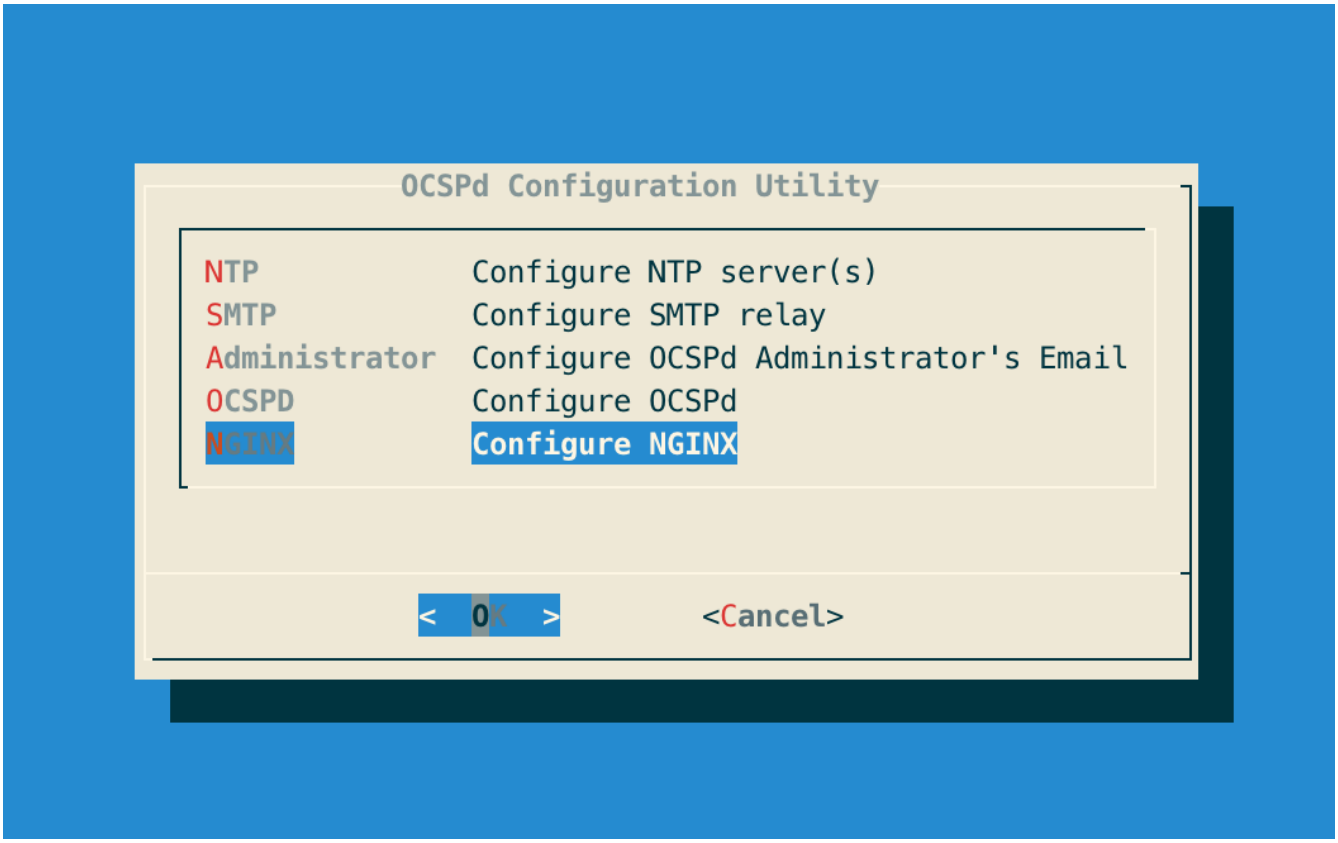
Issuing a Certificate Request (PKCS#10)

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

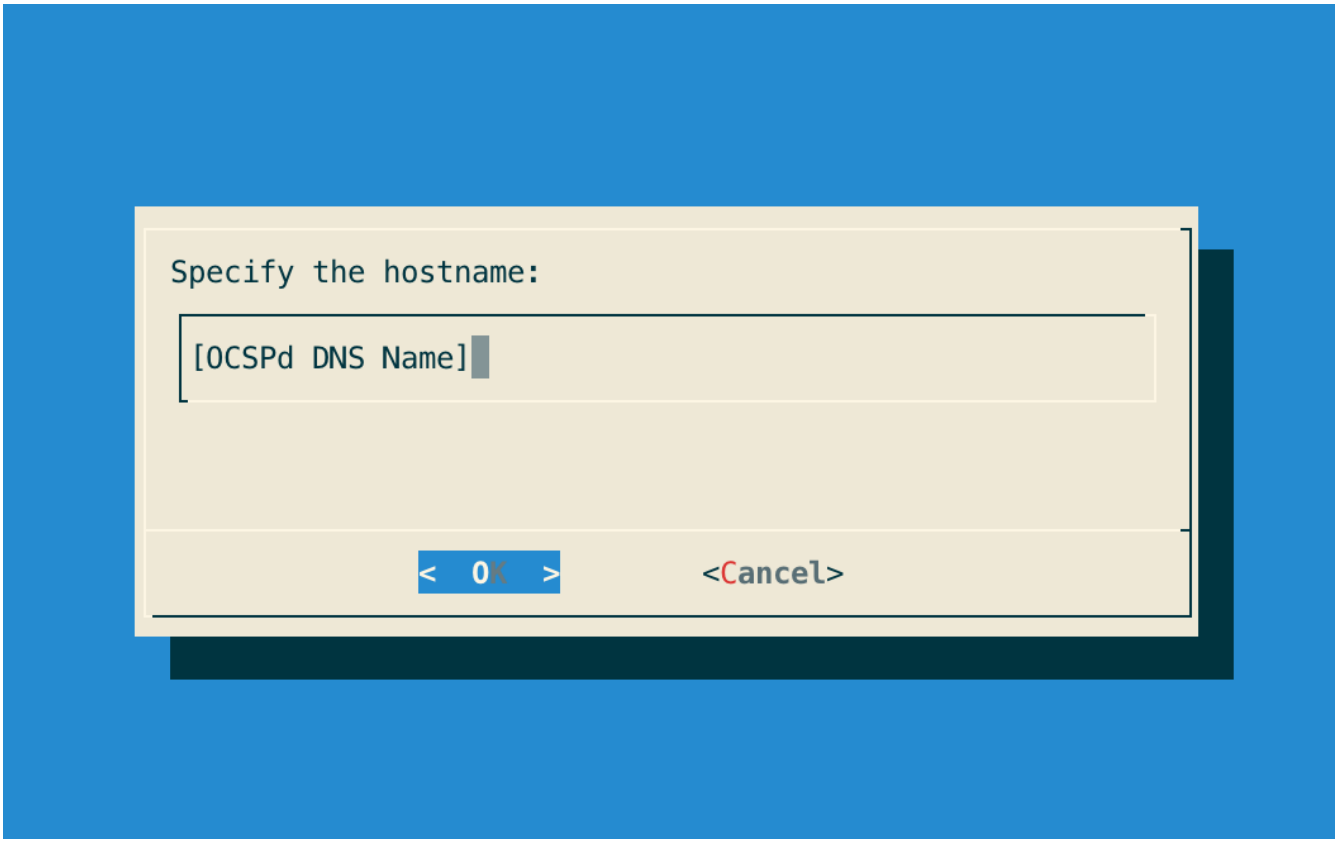
```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**NGINX**':



Step 4: In the NGINX menu, select '**CSR**':

Step 5: Specify the DNS Name of the OCSPd server:



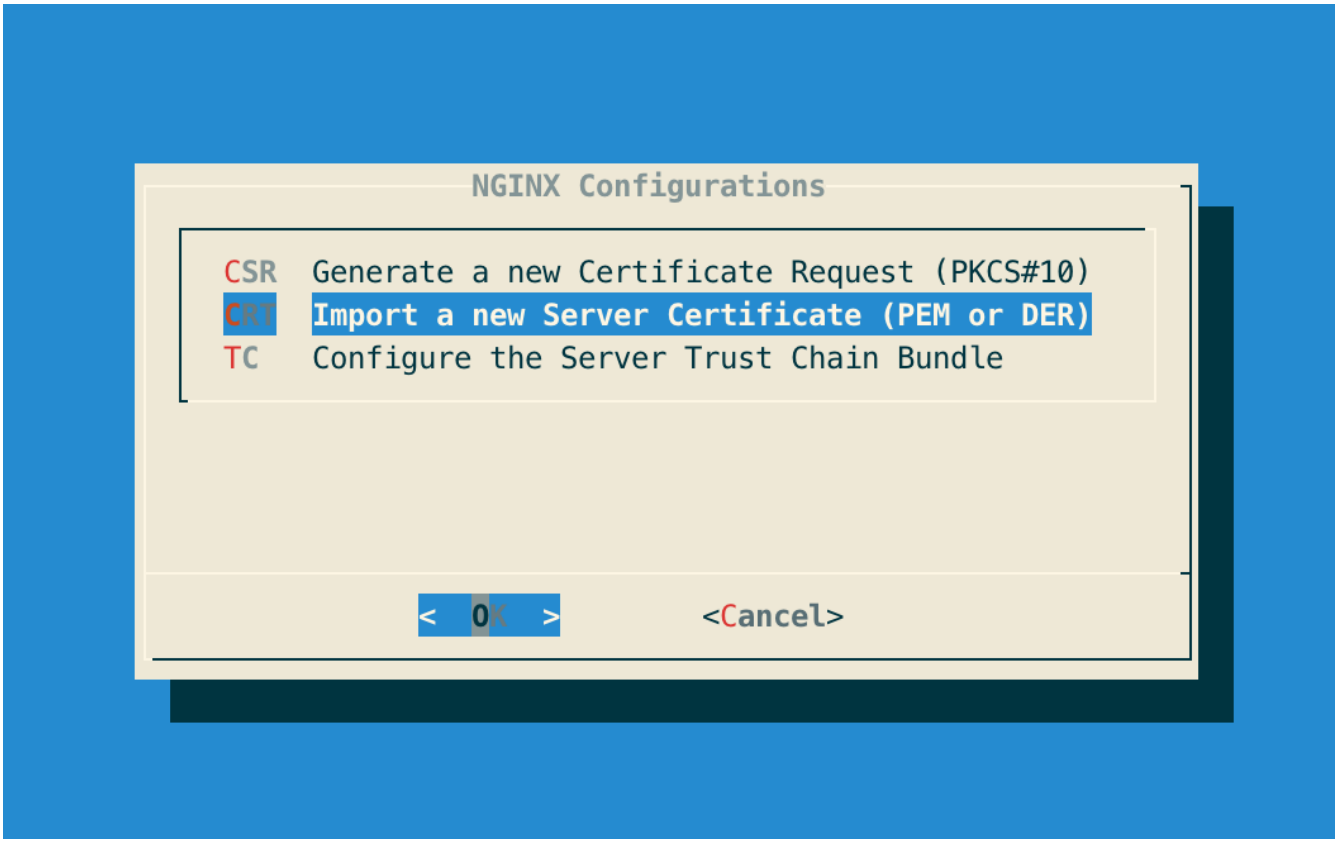
Step 6: The certificate request is generated and available under '***/etc/nginx/ssl/ocspd.csr.new***':

Step 7: Sign the certificate request using the corporate PKI.

Installing a Server Certificate

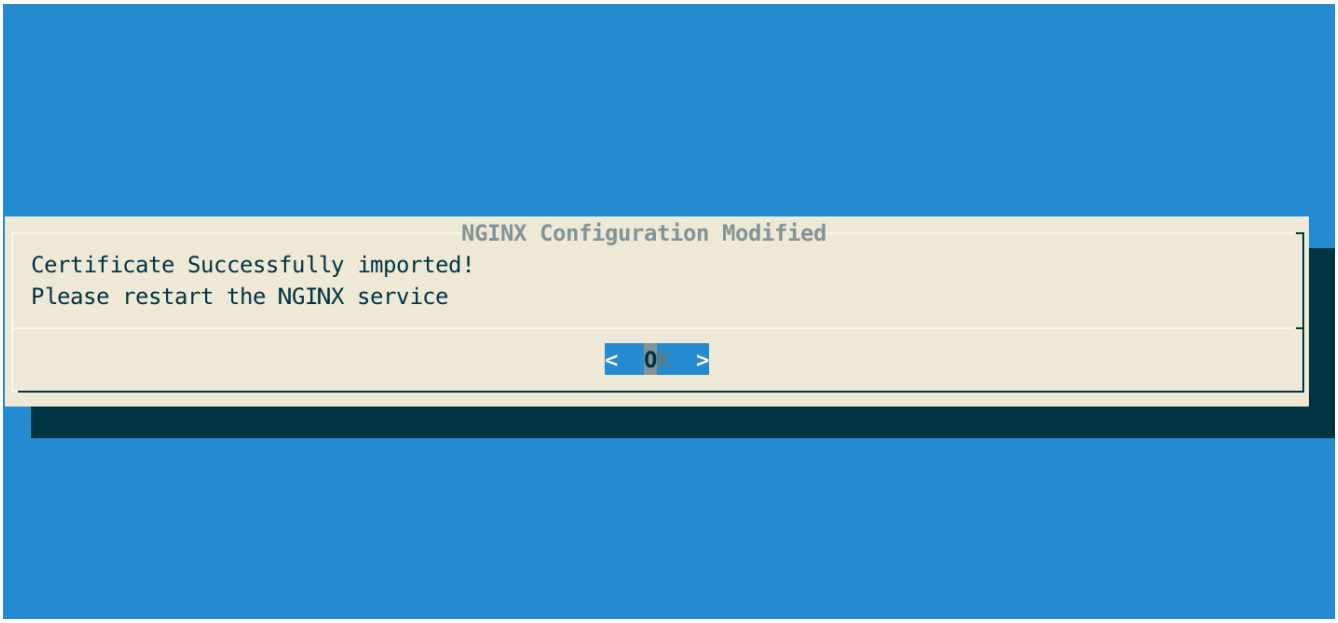
Step 1: Upload the generated server certificate on the OCSPd server under '***/tmp/ocspd.pem***' through SCP;

Step 2: In the NGINX configuration menu, select '**CRT**':



Step 3: Specify the path '***/tmp/ocspd.pem***' and validate:

Step 4: The server certificate is successfully installed:

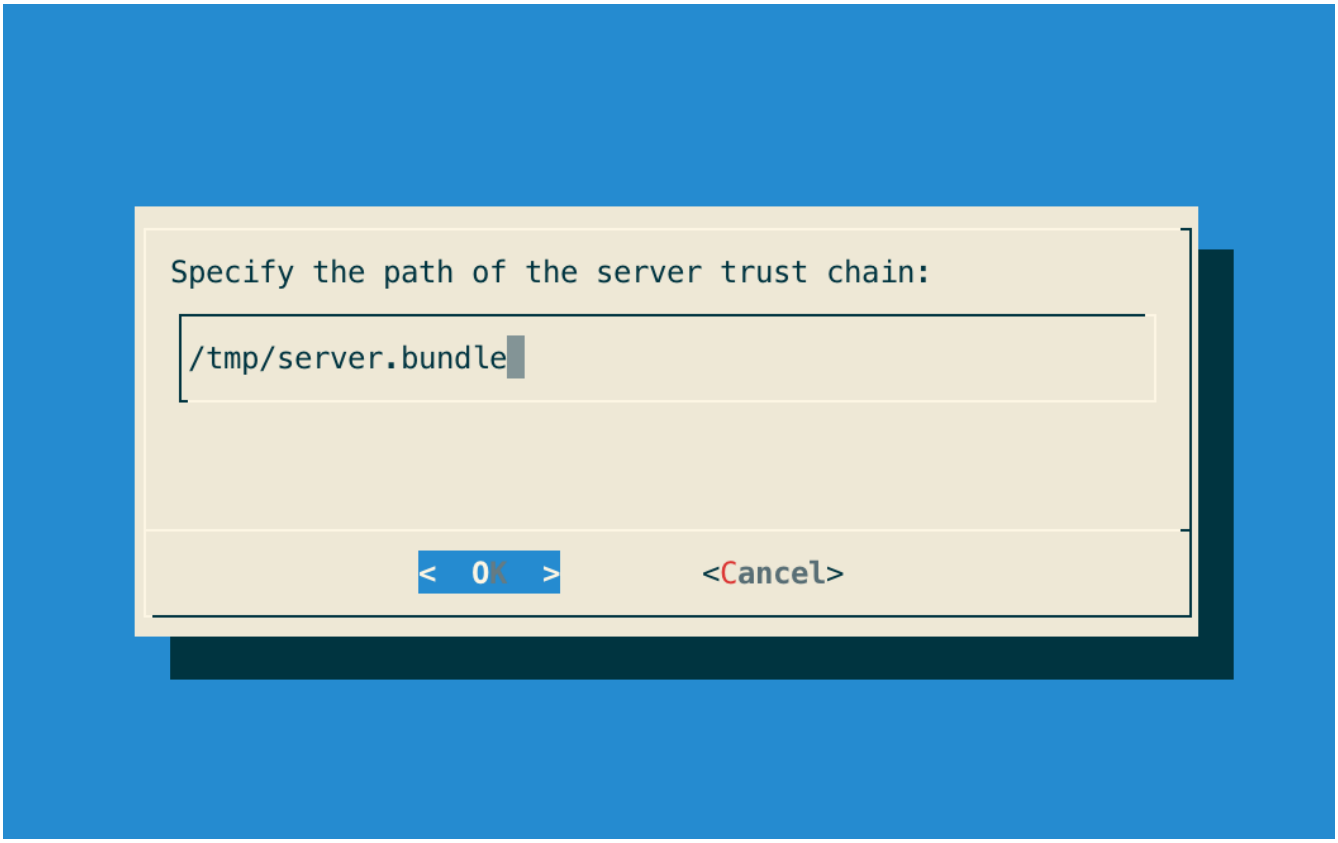


Installing the Server Certificate Trust Chain

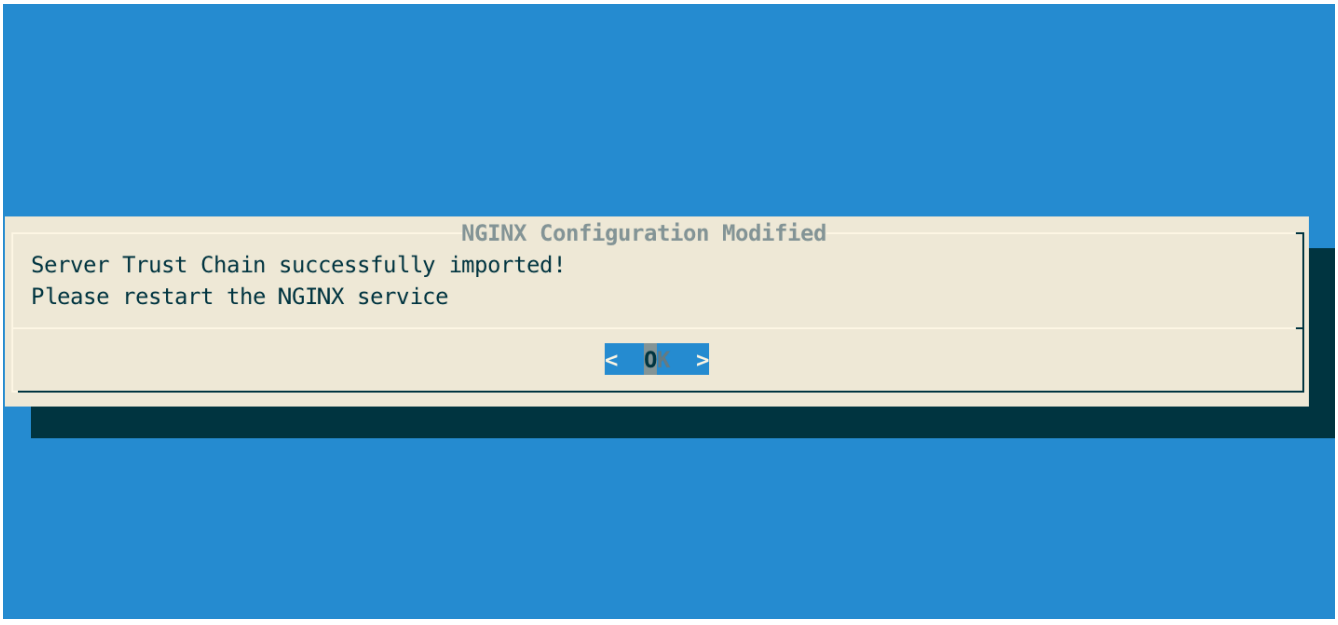
Step 1: Upload the server certificate trust chain (the concatenation of the Certificate Authority certificates in PEM format) on the OCSPd server under '***/tmp/server.bundle***' through SCP;

Step 2: In the NGINX configuration menu, select '**TS**':

Step 3: Specify the path '***/tmp/server.bundle***' and validate:



Step 4: The server bundle is successfully installed:



1.4.2. Configuring the Firewall

EL6

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Open ports TCP/80 and TCP/443 on the local firewall with the following commands:

```
# iptables -I INPUT 1 -p tcp -m tcp --dport 443 -j ACCEPT
```

```
# iptables -I INPUT 1 -p tcp -m tcp --dport 80 -j ACCEPT
```

Step 3: Save the local firewall configurations with the following command:

```
# /etc/init.d/iptables save
```

EL7

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Open ports TCP/80 and TCP/443 on the local firewall with the following commands:

```
# firewall-cmd --zone=public --permanent --add-service=http
# firewall-cmd --zone=public --permanent --add-service=https
```

1.5. Running as container

OCSPd is also packaged as a container, and can be run on container runtimes such as Docker or Kubernetes CRI-compliant runtimes.

Database considerations

OCSPd uses an embedded database to store application configuration. The database is created automatically when OCSPd is started for the first time. The database is stored in the `/ocspd/database` directory and needs to be persisted :

- On Docker, this can be done through a Docker volume or a bind mount.
- On Kubernetes, this can be done through a persistent volume claim.

Docker example

The bare minimum requirements to start an OCSPd instance is to pass through environment variables at least :

- a valid license through the `LICENSE` variable
- an application secret through the `APPLICATION_SECRET` variable

To do so, just run the following command :

```
docker run -p 9000:9000 -e LICENSE=$(cat ./ocspd.lic) -e
APPLICATION_SECRET=QA3BgXqapXaEzLbX -v ./database:/ocspd/database:rw
registry.evertrust.io/ocspd:3.1.3
```

The OCSPd server will be available at http://localhost:9000. To configure the instance, please refer to

the configuration section.

Configuration

The Docker image is configured through environment variables. The following environment variables are available :

General configuration

Variable	Type	Description	Default
LICENSE	`string`	A valid OCSPd license string, base64-encoded. Can be used if `LICENSE_PATH` is empty.	
LICENSE_PATH	`path`	Path where an OCSPd license file is mounted inside the container. Can be used if the license is not passed directly through `LICENSE`.	
APPLICATION_SECRET	`string`	Application secret used by OCSPd	

Your license usually contains newline characters, that you must replace by '\n' when setting it through the environment.

Configuring HTTPS

In production, it is strongly recommended to ensure all requests go through a layer of encryption. Configuring TLS for OCSPd will allow your reverse proxy to request OCSPd data using TLS.

If all settings are left empty, OCSPd will generate a self-signed certificate upon startup and still expose its HTTPS endpoint on

Variable	Type	Description	Default
HTTP_PORT	`port`	Port of the HTTP server	`9000`
HTTPS_PORT	`port`	Port of the HTTPS server	`9443`
HTTPS_KEYSTORE_PATH	`string`	Location where the keystore containing a server certificate is located.	

Variable	Type	Description	Default
HTTPS_KEYSTORE_PASSWORD	`string`	Password for the given keystore, if required by the keystore type	
HTTPS_KEYSTORE_TYPE	`string`	Format in which the keystore is. Can be either `pkcs12`, `jks` or `pem` (a base64-encoded DER certificate)	`pkcs12`
HTTPS_KEYSTORE_ALGORITHM	`string`	The key store algorithm	Platform default algorithm

Mailer configuration

Variable	Type	Description	Default
SMTP_HOST	`string`	SMTP host	
SMTP_PORT	`port`	SMTP port	
SMTP_SSL	`boolean`	Whether SSL should be used	
SMTP_TLS	`boolean`	Whether TLS should be used	
SMTP_USER	`string`	SMTP user	
SMTP_PASSWORD	`string`	SMTP password	

Radius configuration

Variable	Type	Description	Default
RADIUS_HOST	`string`	Radius host	
RADIUS_SECRET	`string`	Radius secret	
RADIUS_PORT	`port`	Radius port	
RADIUS_PROTOCOL	`string`	Radius protocol, `PAP` or `CHAP`	`PAP`

LDAP configuration

Variable	Type	Description	Default
LDAP_HOST	`string`	LDAP host	
RADIUS_SECRET	`string`	Radius secret	
LDAP_PORT	`port`	LDAP port	

Variable	Type	Description	Default
LDAP_SSL	`boolean`	Whether SSL should be used for LDAP	
LDAP_BIND_DN	`string`	Bind DN used to authenticate to LDAP	
LDAP_BIND_PASSWORD	`string`	Bind password used to authenticate to LDAP	
LDAP_BASE_DN	`string`	LDAP base DN	
LDAP_USERNAME_ATTRIBUTE	`string`	LDAP username attribute	

1.6. Initial OCSPd Access

Starting the OCSPd services

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Start the ocspd service with the following command:

```
# /etc/init.d/ocspd start
```

Step 3: Start the nginx service with the following command:

```
# /etc/init.d/nginx start
```

Accessing the OCSPd Web Management Console

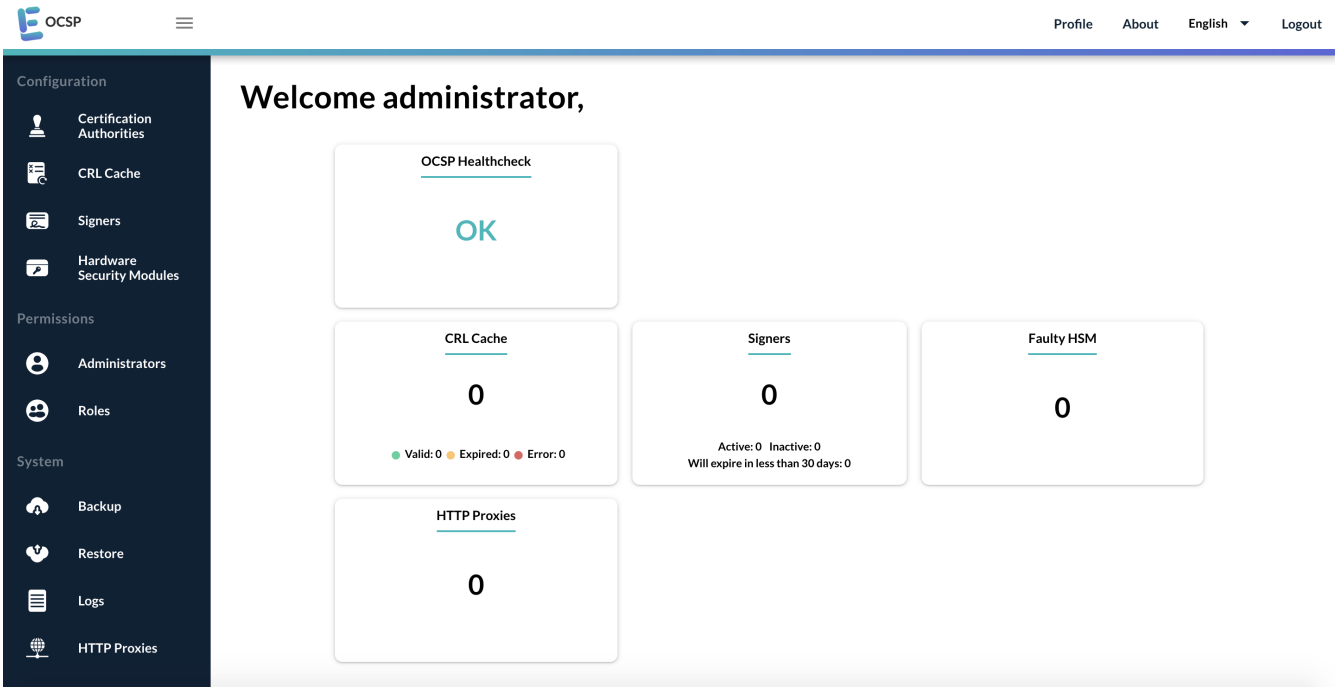
Step 1: Launch a web browser;

Step 2: Browse to '***https://[IP or DNS Name of the OCSPd component]***':

The default administration credentials are:

- Login: '**administrator**'
- Password: '**ocspd**'

Step 3: Specify the default administration credentials and hit the '**Login**' button:



It is **highly recommended** to create a dedicated administration account and delete the default one, or at least modify the default administrator password.

1.7. Uninstallation Procedure

Prior to uninstalling, please ensure that you have a **proper backup of the OCSPd component**. Once uninstalled, all the OCSPd data will be **irremediably lost**!

Uninstalling OCSPd consists in uninstalling:

- The OCSPd service;
- The NGINX service.

Uninstalling OCSPd

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Uninstall OCSPd with the following commands:

```
# /etc/init.d/ocspd stop
# yum remove ocspd
# rm -rf /opt/ocspd
# rm -rf /var/log/ocspd
# rm -f /etc/default/ocspd
```

Uninstalling NGINX

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Uninstall NGINX with the following commands:

```
# /etc/init.d/nginx stop
# yum remove nginx
# rm -rf /etc/nginx
# rm -rf /var/log/nginx
```

2. Admin guide

2.1. Introduction

Description

OCSPd (OCSP daemon) is an OCSP responder compliant with the following RFCs:

- RFC 6960
- RFC 5019

This project is powered up by:

- Akka
- BouncyCastle
- EHCache
- H2 Database
- IAIK PKCS#11 Wrapper
- Kamon
- Play! Framework
- Scala
- NGINX

This document is specific to OCSPd version **3.1.3**.

Scope

This document is an Administration Guide and details how to:

- Manage NGINX specific configuration (authentication, OCSP stapling);
- Manage Permissions (Administrators and Roles);
- Manage Hardware Security Modules (HSM);
- Manage Certificate Authorities;
- Manage OCSP Signers;

- Perform Backup and Restore operations;
- Monitor the service;
- Obtain Key Performance Indicators (KPI);
- Consume the OCSP service;
- Troubleshooting.

Out of Scope

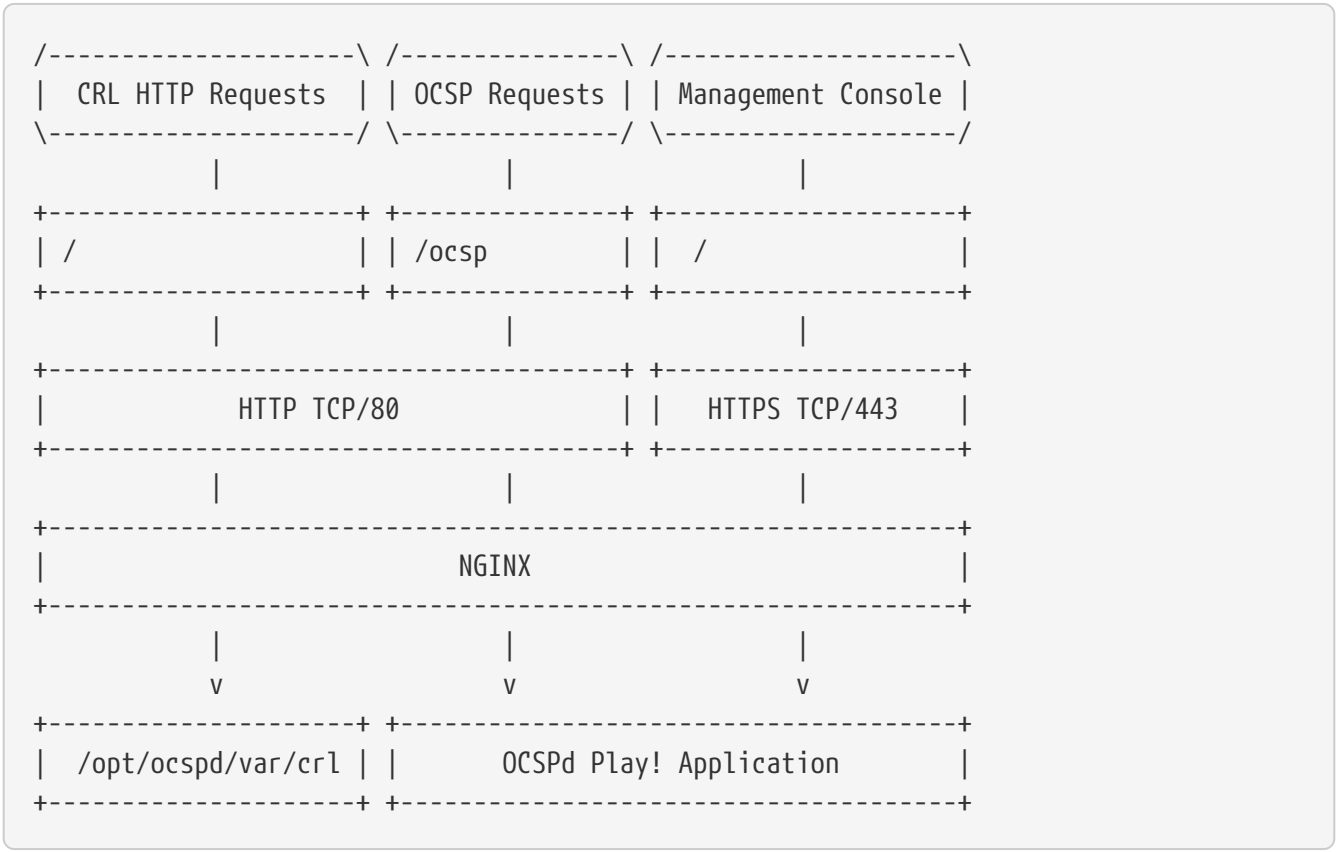
This document does not detail how to install the OCSPd component. For installation and uninstallation procedures, please refer to the '**OCSPd Installation Guide**'.

2.2. NGINX Specific Configurations

OCSPd uses the NGINX web server to:

- Act as a proxy for the OCSPd Play! application (Web Management Console & OCSP responder);
- Serve the CRLs when the OCSPd component is used as an HTTP CRL Distribution Point.

The following schema summarizes the interaction between NGINX, the filesystem and the OCSPd Play! Application:



The NGINX configuration is defined in the file '***/opt/ocspd/etc/ocspd-httpd.conf***' and loaded through a symbolic link under '***/etc/nginx/conf.d/***'. Tweaking this configuration is possible, but any modification not specifically documented in this guide is **not supported**.

The NGINX configuration file can be tweaked to enable OCSP stapling.

Enabling OCSP Stapling

OCSPd can be natively used to perform OCSP Stapling. This section simply details how to activate OCSP Stapling on the OCSPd NGINX instance for the Web Management Console. This configuration is optional.

More information regarding OCSP Stapling can be found here OCSP Stapling.

To enable OCSP Stapling, OCSPd must be able to process OCSP request regarding the Certificate Authority used to issue the server certificate.

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Edit the file '***/opt/ocspd/etc/ocspd-httpd.conf***';

Step 3: Uncomment the following lines:

```
ssl_stapling on;
ssl_stapling_verify on;
ssl_stapling_responder http://127.0.0.1:9000/ocsp;
```

Step 4: Reload the NGINX configuration with the following command:

```
# /etc/init.d/nginx reload
```

Renewing the Server certificate

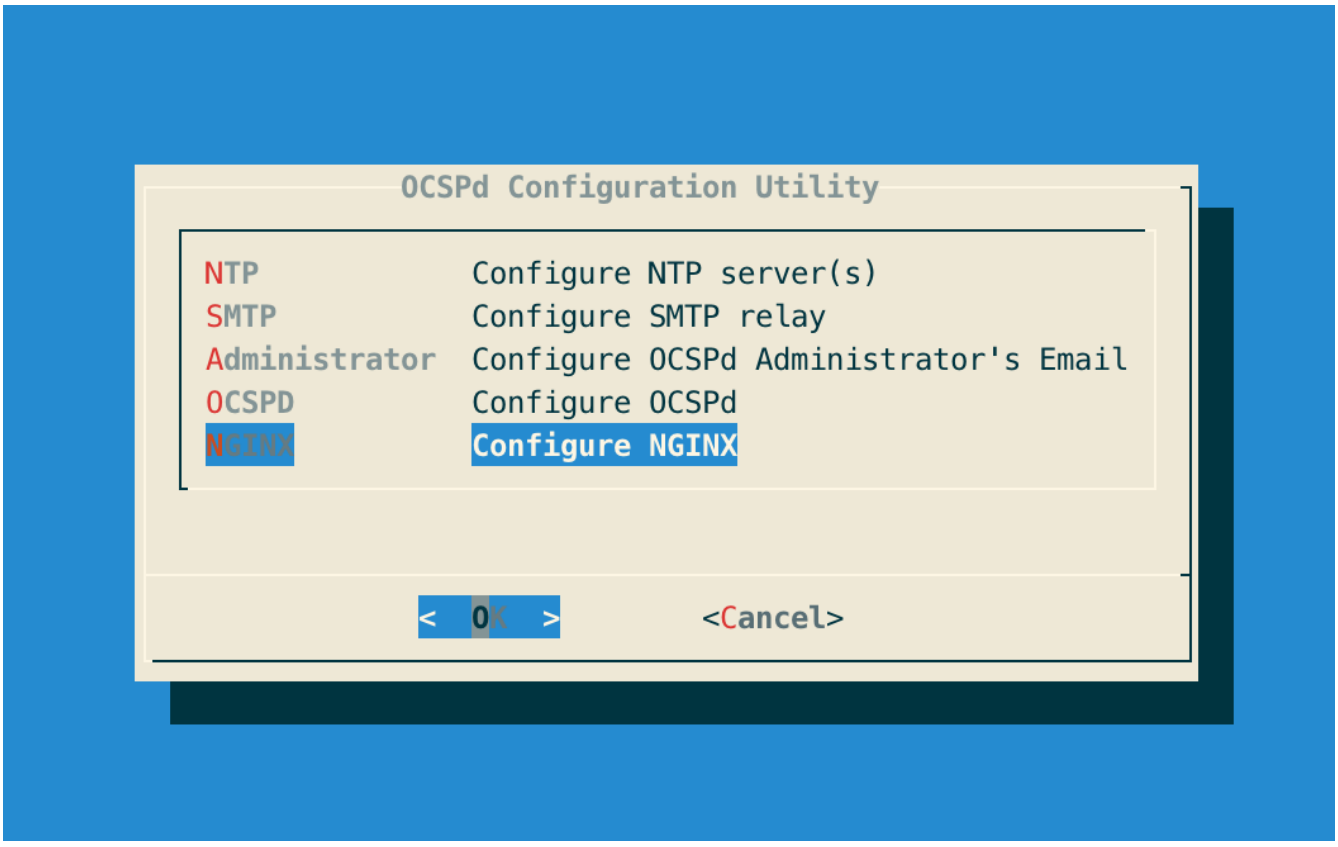
Issuing a Certificate Request (PKCS#10)

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

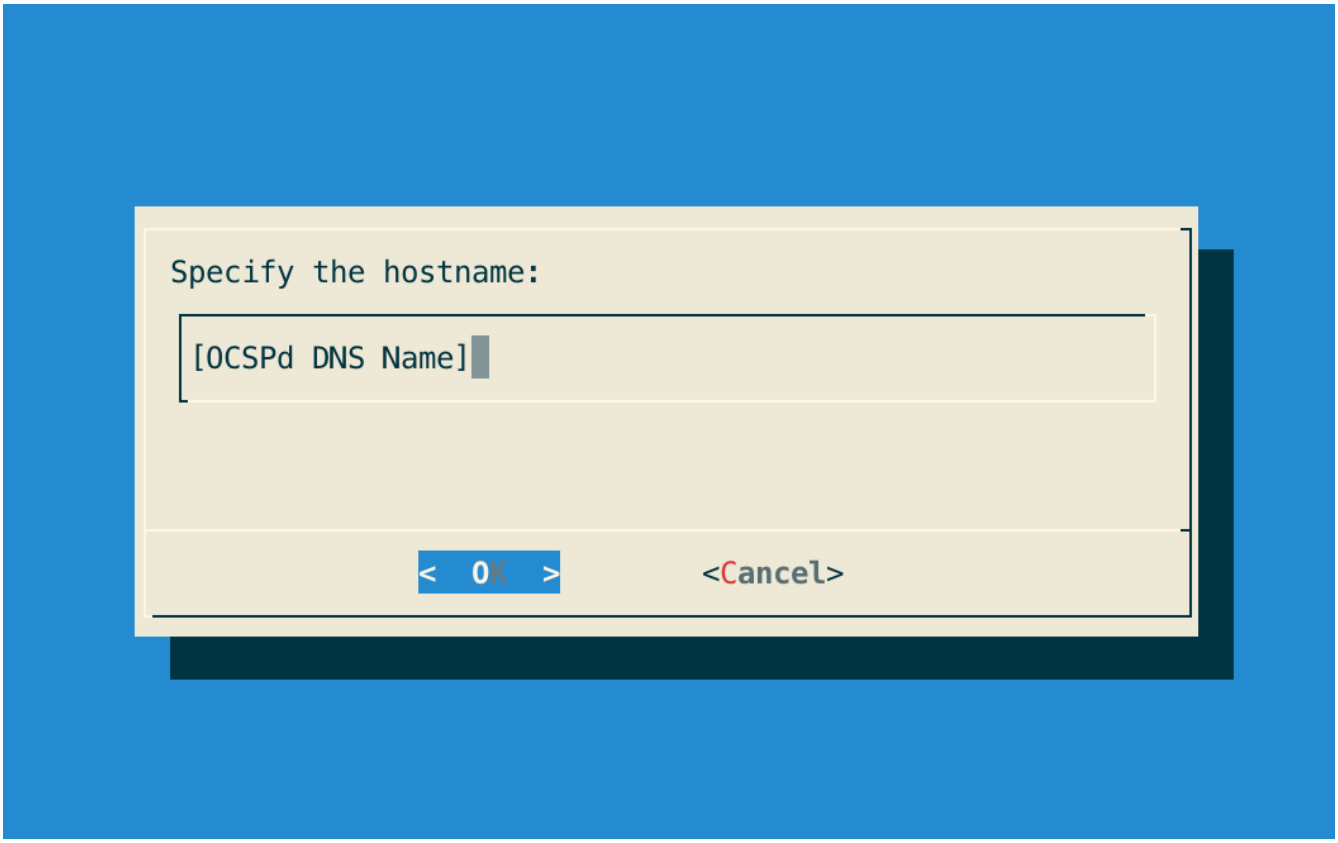
```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**NGINX**':



Step 4: In the NGINX menu, select '**CSR**':

Step 5: Specify the DNS Name of the OCSPd server:



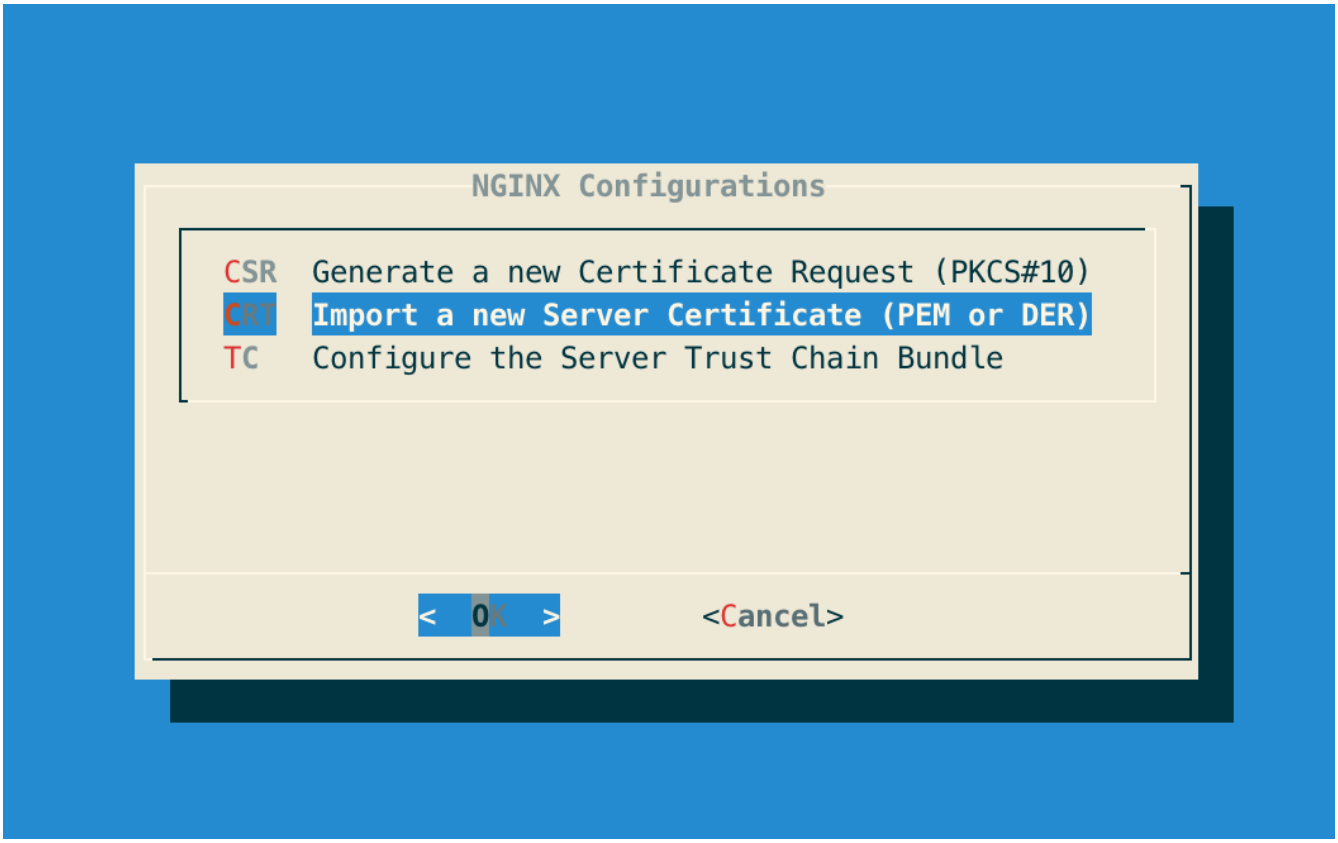
Step 6: The new certificate request is generated and available under '***/etc/nginx/ssl/ocspd.csr.new***':

Step 7: Sign the certificate request using the corporate PKI.

Installing a Server Certificate

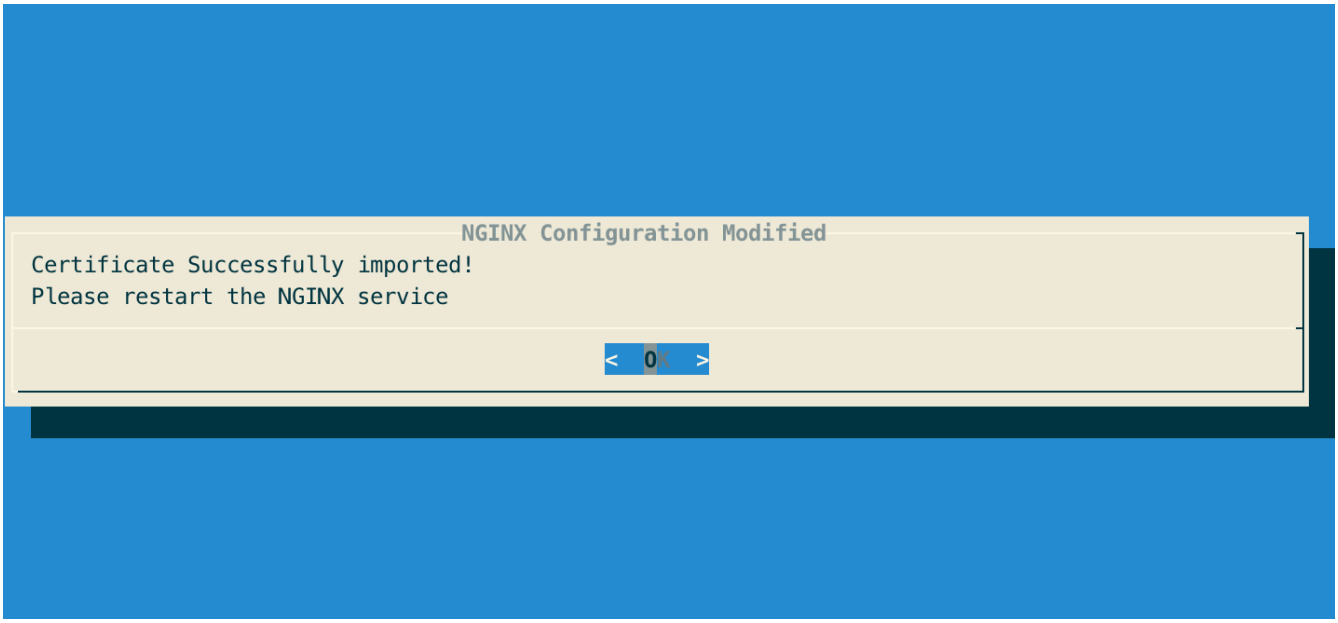
Step 1: Upload the generated server certificate on the OCSPd server under '***/tmp/ocspd.pem***' through SCP;

Step 2: In the NGINX configuration menu, select '**CRT**':



Step 3: Specify the path '***/tmp/ocspd.pem***' and validate:

Step 4: The server certificate is successfully installed:



Step 5: Exit the configuration utility and reload the NGINX service with the following command:

```
# /etc/init.d/nginx reload
```

2.3. Initial Management Console Access and Logout

Management Console Access

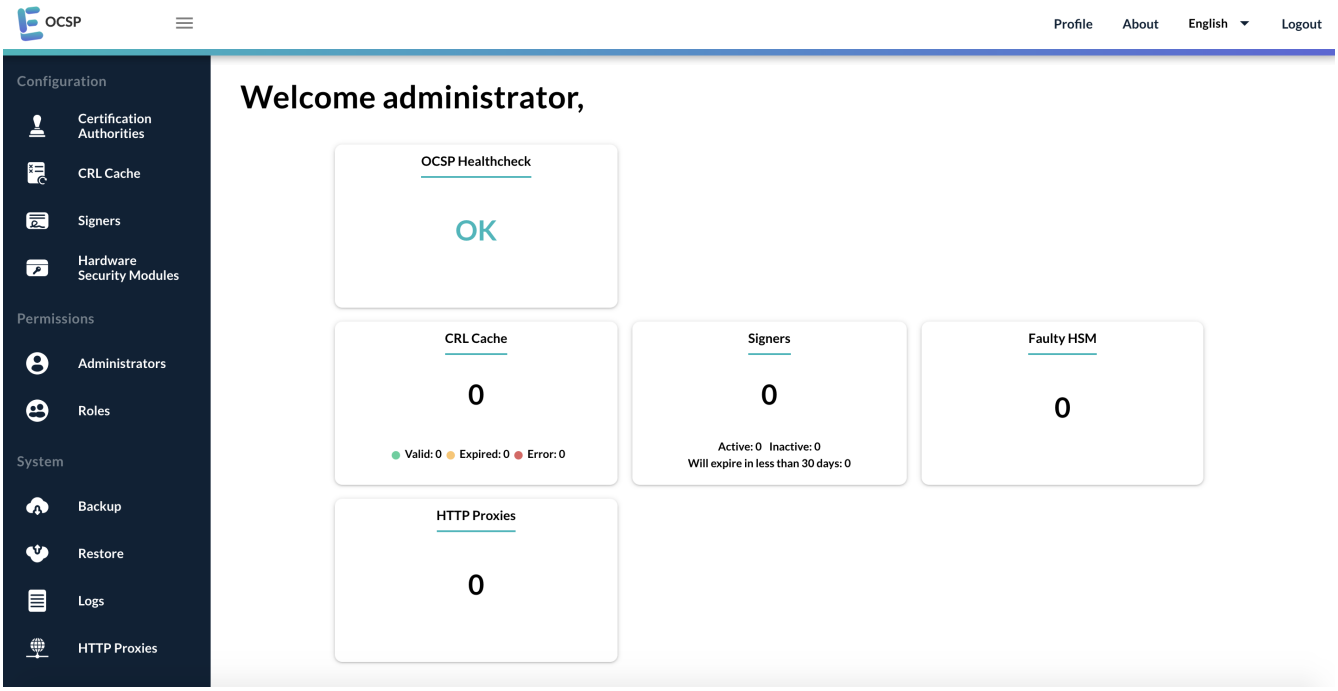
Step 1: Access the Web Management Console using a Web browser ***https://[IP or DNS Name of the OCSPd component]***;

Default credentials are:

- Login: **administrator**
- Password: **ocspd**

Step 2: Provide the default credentials and hit the '**Login**' button:

Step 3: The Web Management Console is displayed:



It is highly recommended to either:

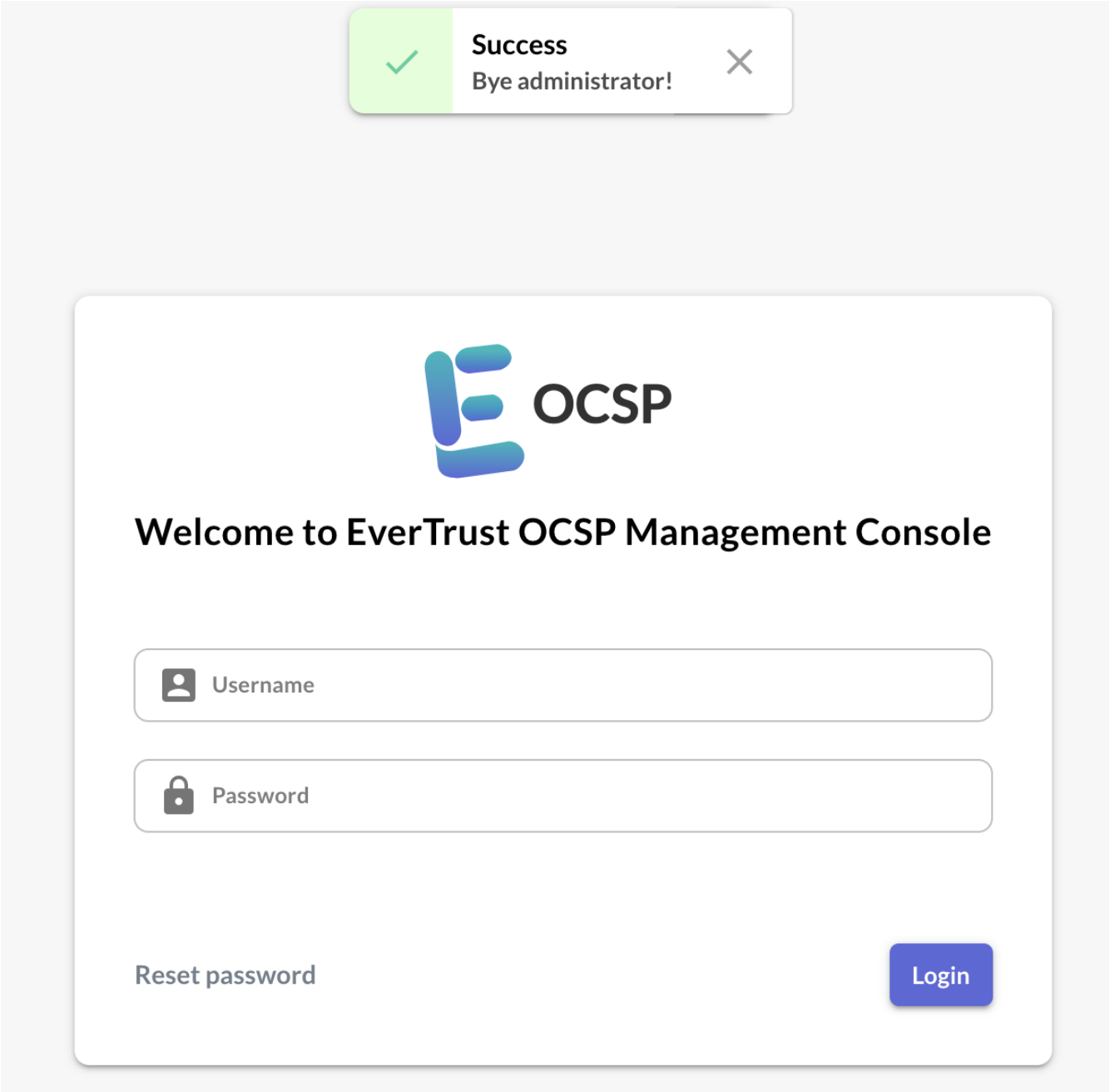
- Modify the default administrator password
- Or Create a new administrator account and delete the default administrator one (to perform this operation, you need to create the new administrator account with the default administrator account, logout, login with the new administrator account and delete the default one).

Management Console Logout

Logout when logged in with Password (Local, Radius or LDAP)

Step 1: Hit 'Logout' in the header:

Step 2: The Administrator is successfully logged out:



Logout when logged in with Certificate

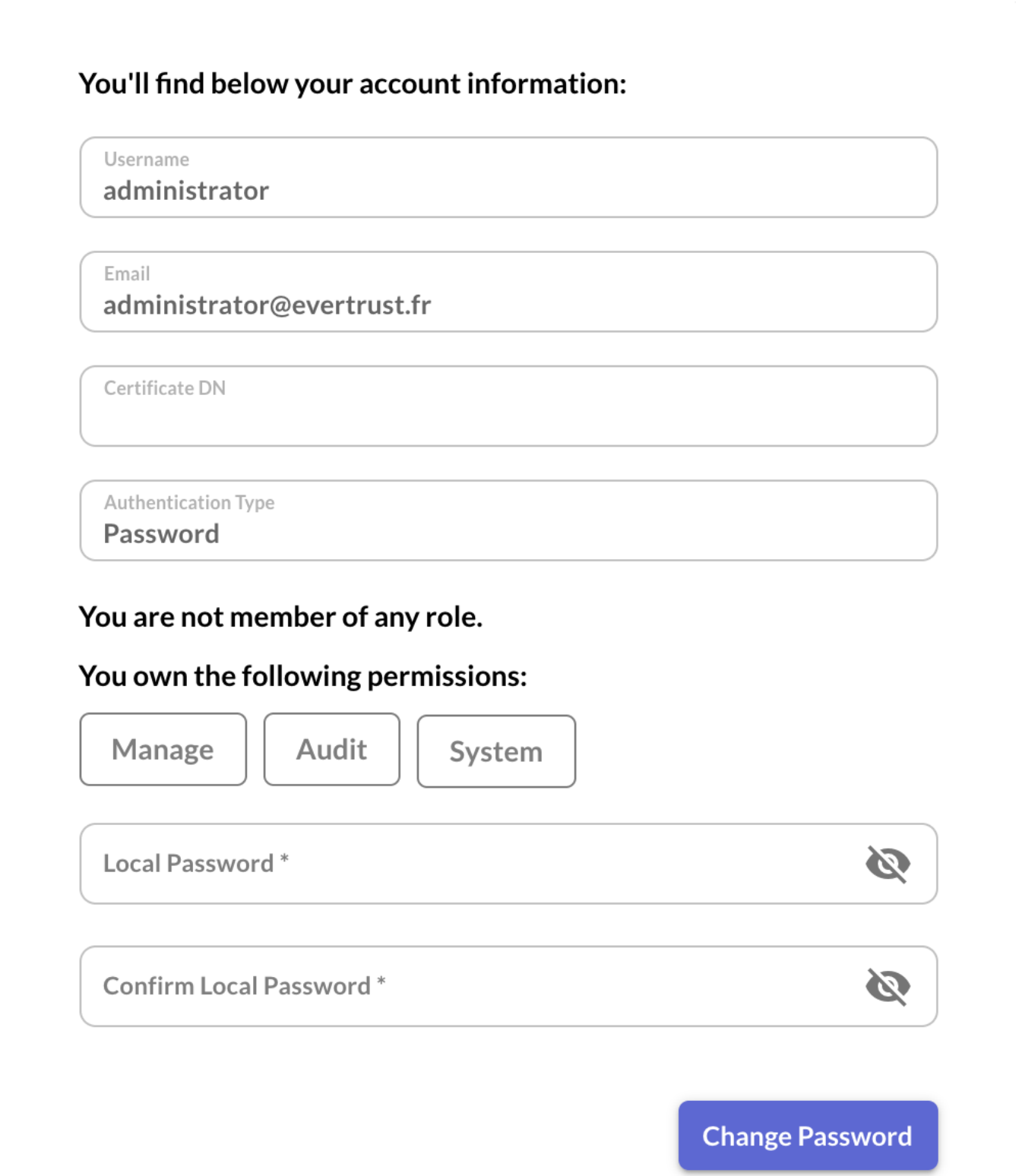
The 'Logout' is not available when logged in with Certificate. Simply close the Web Browser.

2.4. Administrator Profile

Account Information

Step 1: Hit 'Profile' in the header to access to the profile page:

Step 2: Administrator’s account information that is logged in is displayed:



The following elements are displayed:

- '**Username**': the currently logged in Administrator username;
- '**Email**': the currently logged in Administrator email;
- '**Certificate DN**' (*if specified*): the currently logged in Administrator certificate DN;
- '**Authentication Type**': the currently logged in Administrator authentication type;
- The complete list of roles that the currently logged in Administrator is member of;

- The detailed list of all permissions the currently logged in Administrator owns (it aggregates all permissions assigned personally and all permissions inherited from the Role(s) of which Administrator is member of). You have to mouseover each permission category to view the details.

Resetting Password

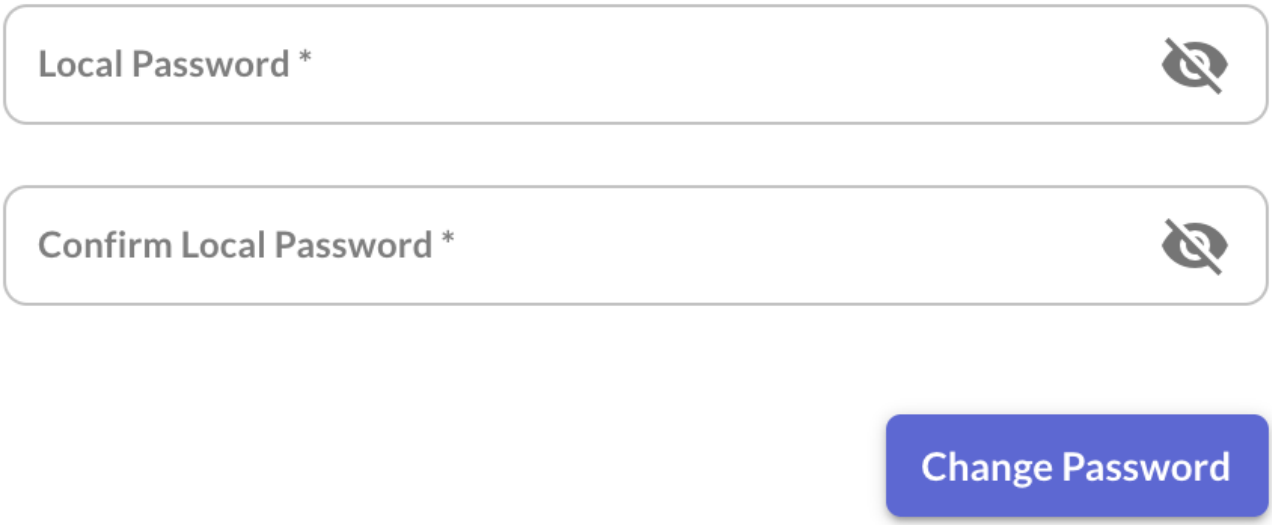
- When an administrator account is created, the associated password is not defined during the creation process and must be set afterward if password-based authentication must be configured for the administrator;
- Local Password can be changed if only the '**Authentication Type**' of the Administrator account has been set to '**Password**'.

The password must be compliant with the Password Policy defined.

An administrator can authenticate using a password even if a certificate DN was provided.

Step 1: Hit 'Profile' in the header to access to the profile page:

Step 4: Specify the Administrator password (double input) and hit the '**Change Password**' button:



Step 5: The Administrator password is set / reset:

2.5. Managing Administrators

2.5.1. Creating an Administrator

When an administrator is created, the associated password is not set. Setting the password is mandatory to be able to consume the administrator account with password authentication.

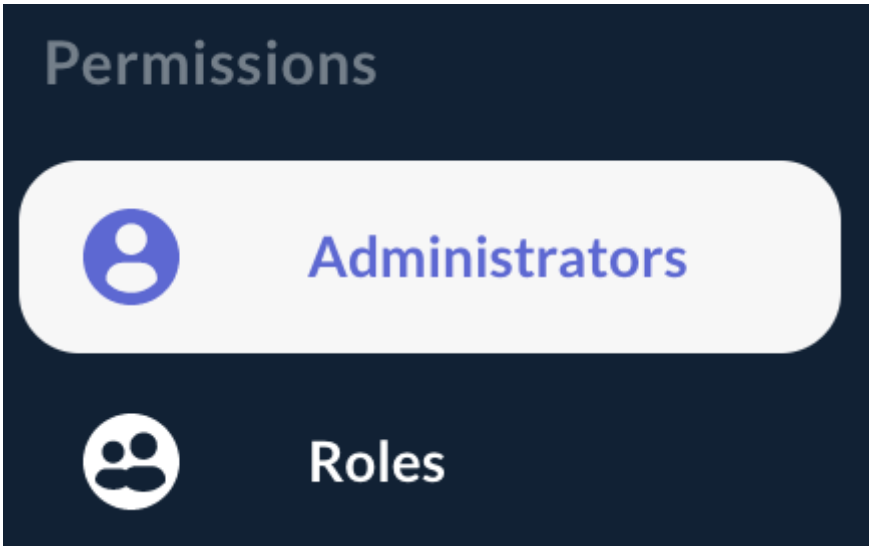
Administrators can be declared:

- Manually;
- By providing a certificate.

Creating an Administrator Manually

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Administrators**':



Step 3: In the Administrators page, hit the '+' button at the bottom right of the table:

Step 4: Specify the following elements and hit the '**Add**' button:

- '**Username**': this is the username used to login on the Web Management Console;
- '**Email**': email of the administrator. For now, this field is not used, but in an upcoming version, it will be used to allow password reset;
- '**Certificate DN**' (*optional*): this allow to map the administrator account to a certificate DN when

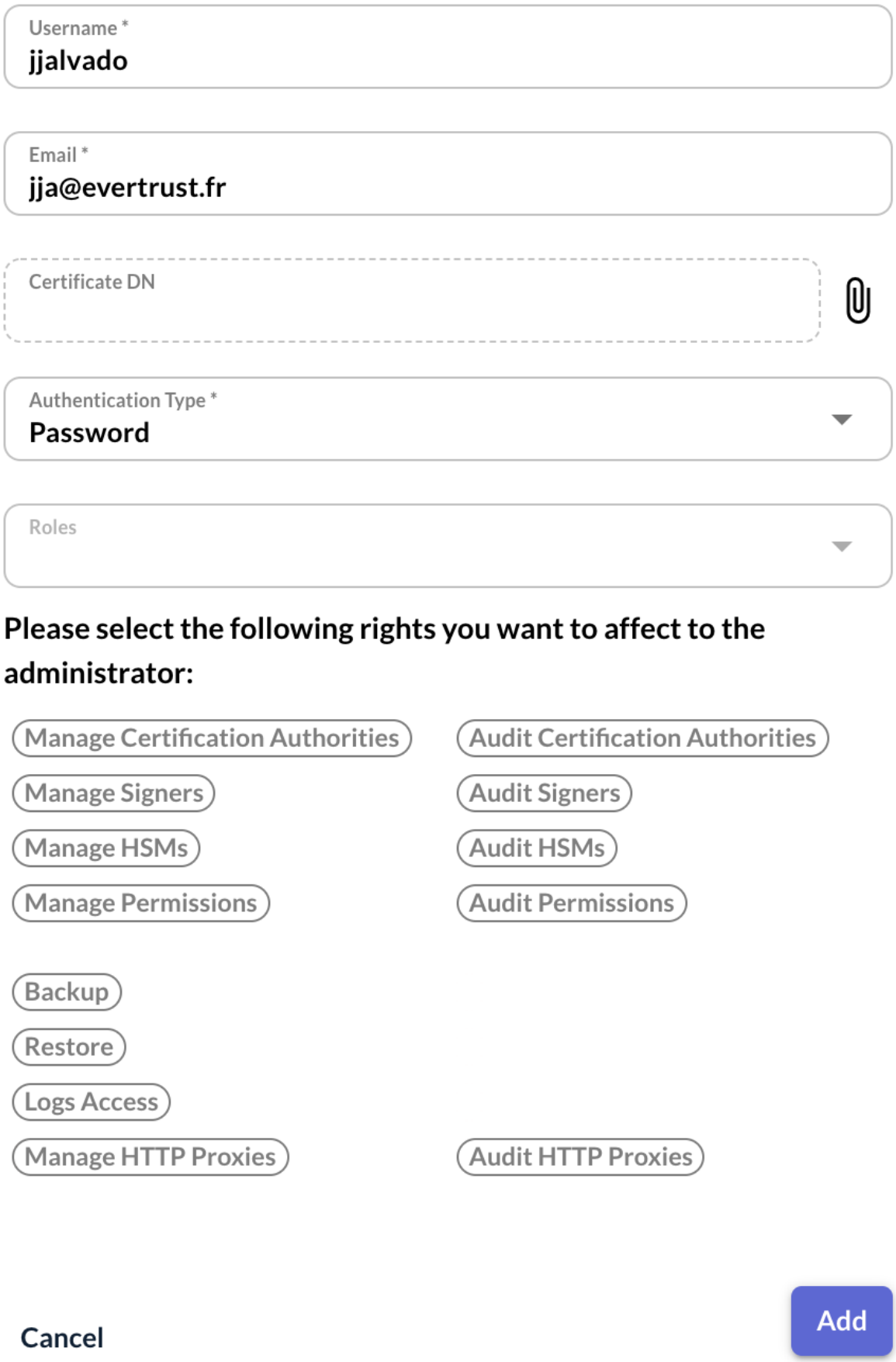
performing certificate-based authentication;

- '**Authentication Type**': for now, OCSPd supports Password, Radius, LDAP and Certificate based authentication (X509);
- '**Roles**' (*optional* and *multiple select*): role(s) given to the administrator;
- '**Permissions**' (*click on each right to select it*): right(s) of manage/audit each module and perform system tasks given to the administrator.

Radius and LDAP authentication methods are available after configurating the dedicated servers on OCSPd. For more information about Radius and LDAP server's configuration, please refer to the '**OCSPd Installation Guide**'.

The issuing CA of the LDAP certificate has to be declared in the OCSPd if you want to use the LDAPS authentication.

'**Manage**' right is a '**read and modify**' right. '**Audit**' is a '**read-only**' right.

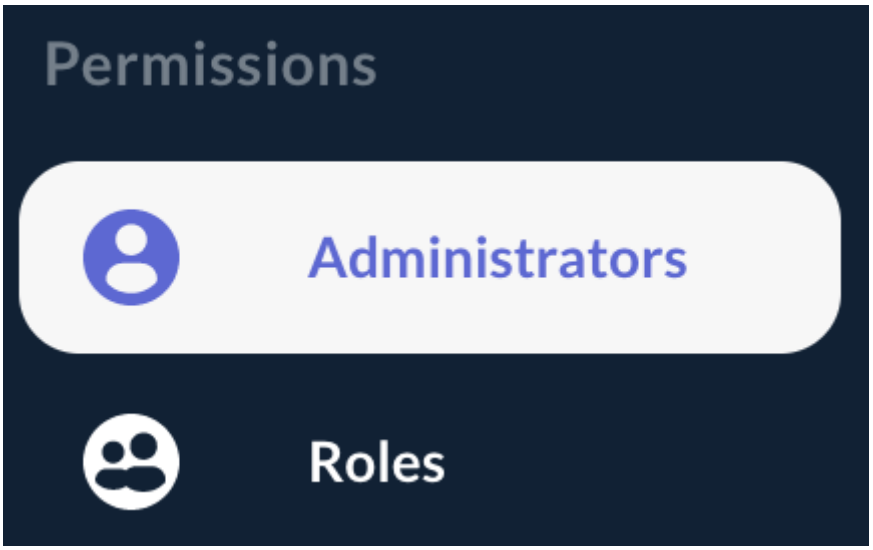


Step 5: The Administrator is successfully created:

Creating an Administrator using a Certificate

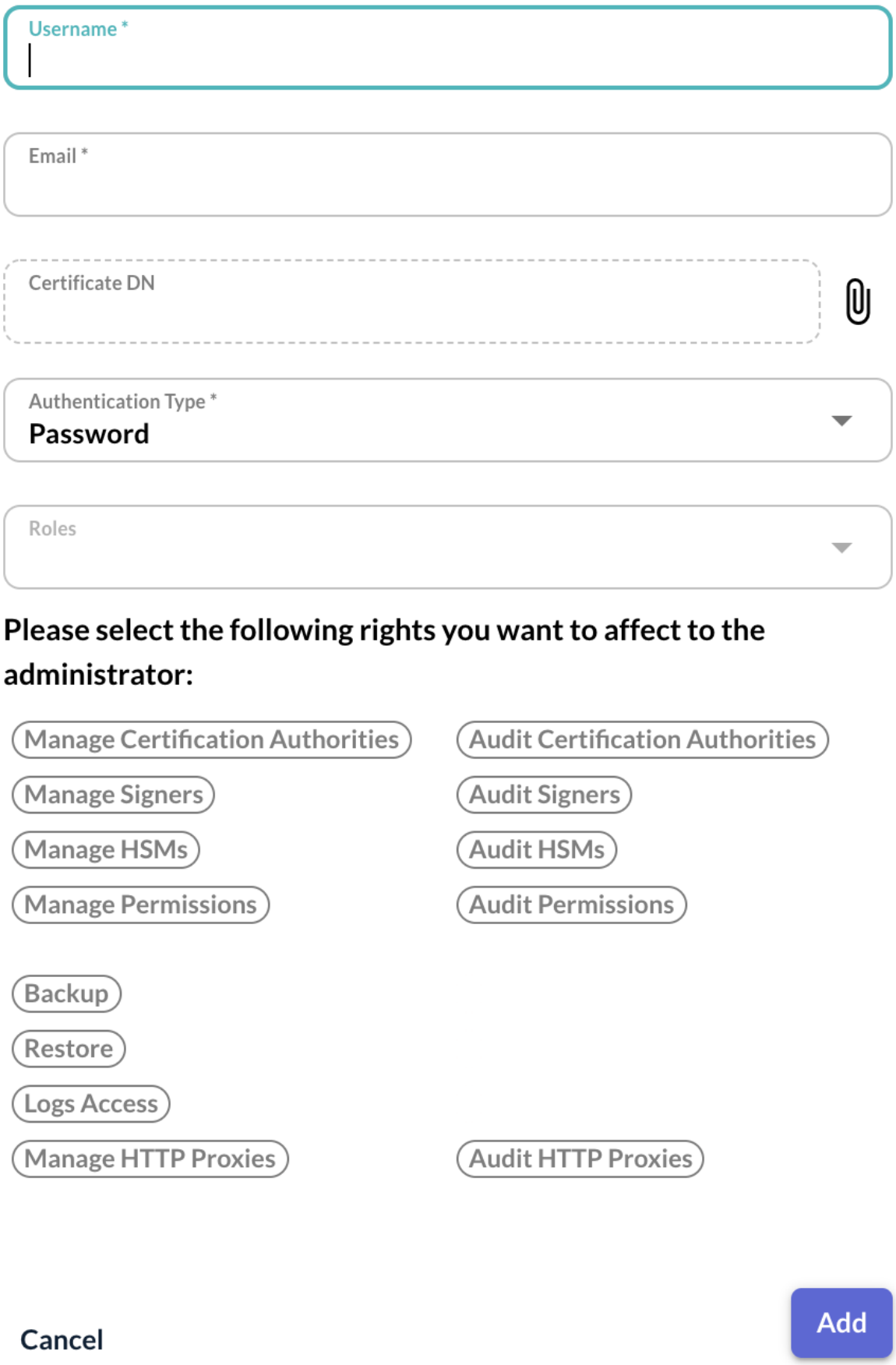
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Administrators**':

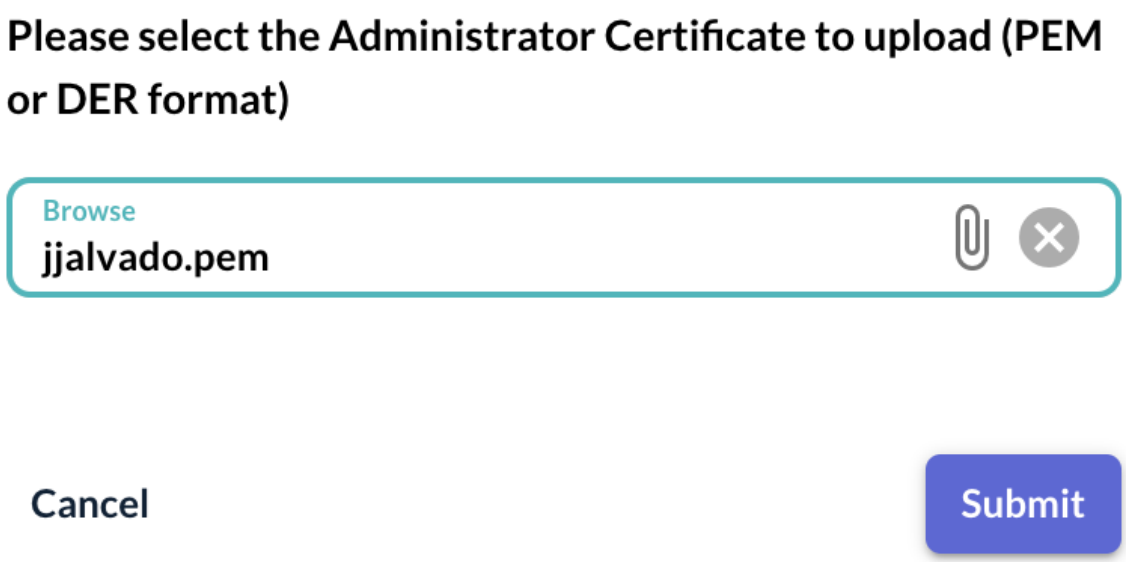


Step 3: In the Administrators page, hit the '+' button at the bottom of the page:

Step 4: In the popup, hit the button:



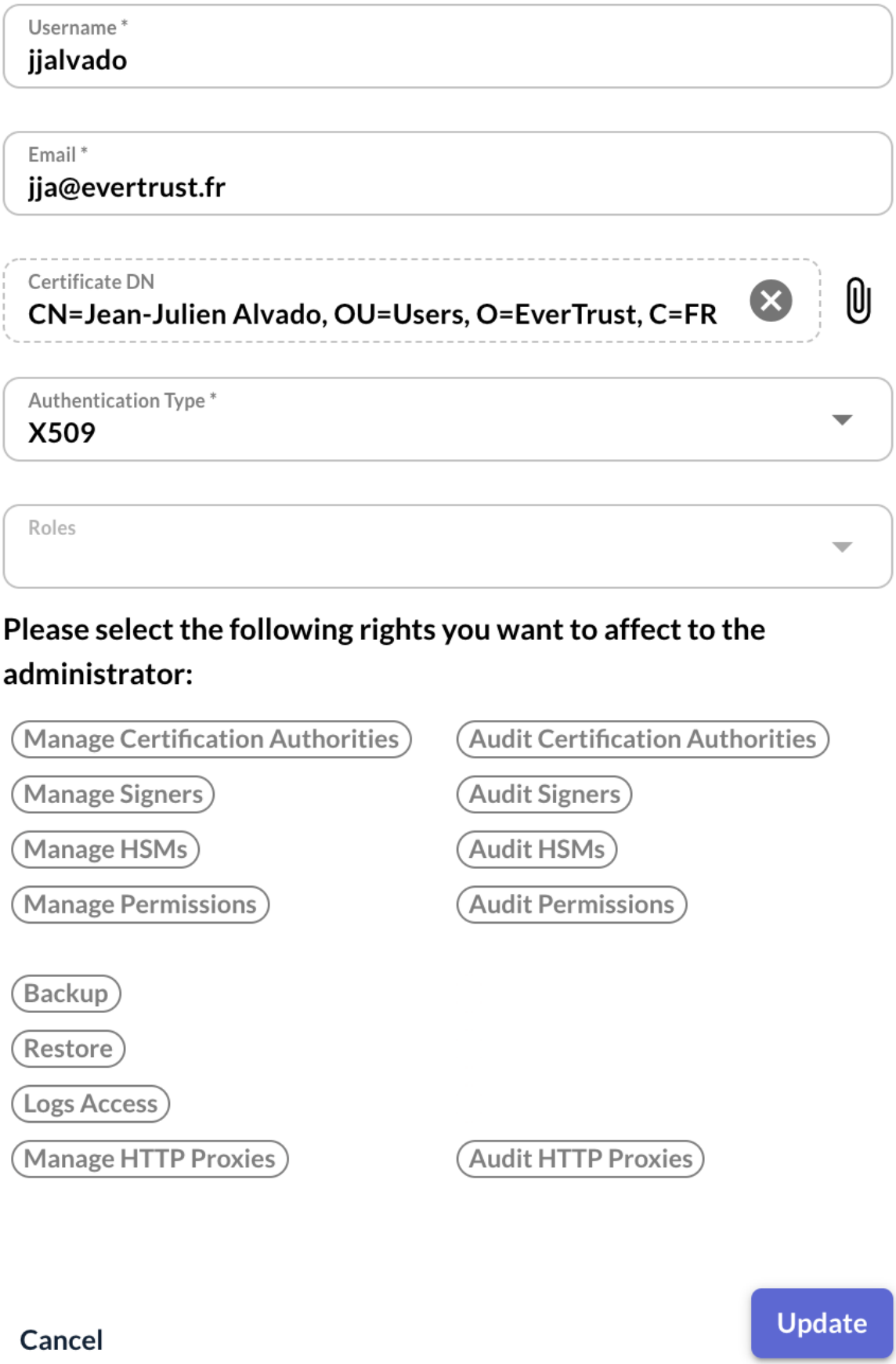
Step 5: Specify the certificate to load (PEM or DER) and hit the '**Submit**' button:



Step 6: The Administrator form is automatically populated with the following value:

- '**Username**': Common Name of the provided certificate;
- '**Email**': Extracted from the RFC822Name if defined in the certificate, empty otherwise;
- '**Certificate DN**': Distinguished Name of the provided certificate.

Specify the roles and permissions attributes (if required) and hit the '**Add**' button:



Step 6: The Administrator is successfully created:

2.5.2. Setting Administrator Password Policy

You can create your own password policy for administrators accounts on EverTrust OCSP.

The default password policy requires the use of a minimum 8-character password without any other criteria of complexity.

You can combine the following complexity criteria to create your own password policy:

Configuration file parameter	Signification
validation.length.min	Minimum length
validation.length.max	Maximum length
validation.lower.case.min	Minimum number of lowercase characters
validation.upper.case.min	Minimum number of uppercase characters
validation.digit.min	Minimum number of digits
validation.special.min	Minimum number of special characters

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Modify the following configuration file '**/opt/ocspd/etc/ocspd.conf**' to set up your password policy:

```
authentication {
    password {
      [...]
      validation.length.min=
      validation.length.max=
```

```
      validation.upper.case.min=
      validation.lower.case.min=
      validation.digit.min=
      validation.special.min=
    }
```

Step 3: Restart the OCSPd service with the following command:

```
# /etc/init.d/ocspd restart
```

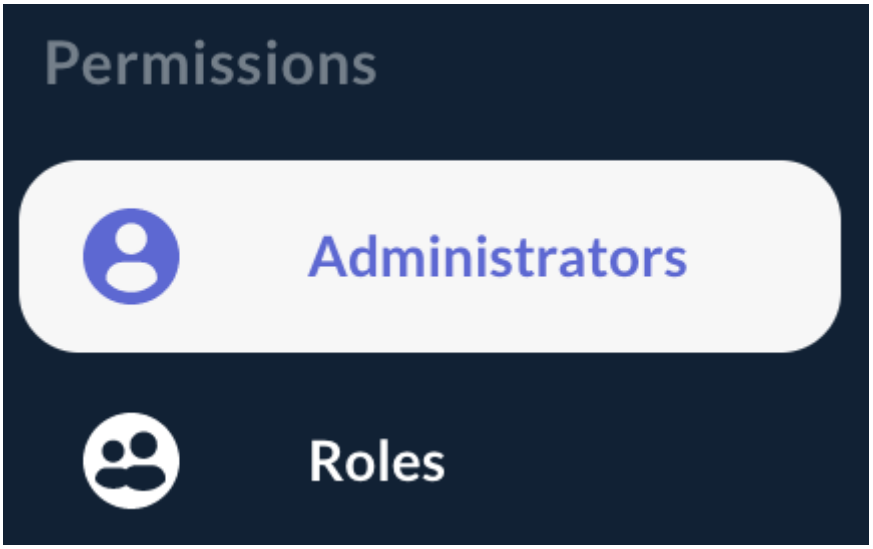
2.5.3. Editing or deleting Administrators

Editing an Administrator

Any administrator's attribute can be modified, even the username one but the administrator attributes '**username**' and '**email**' must be unique.

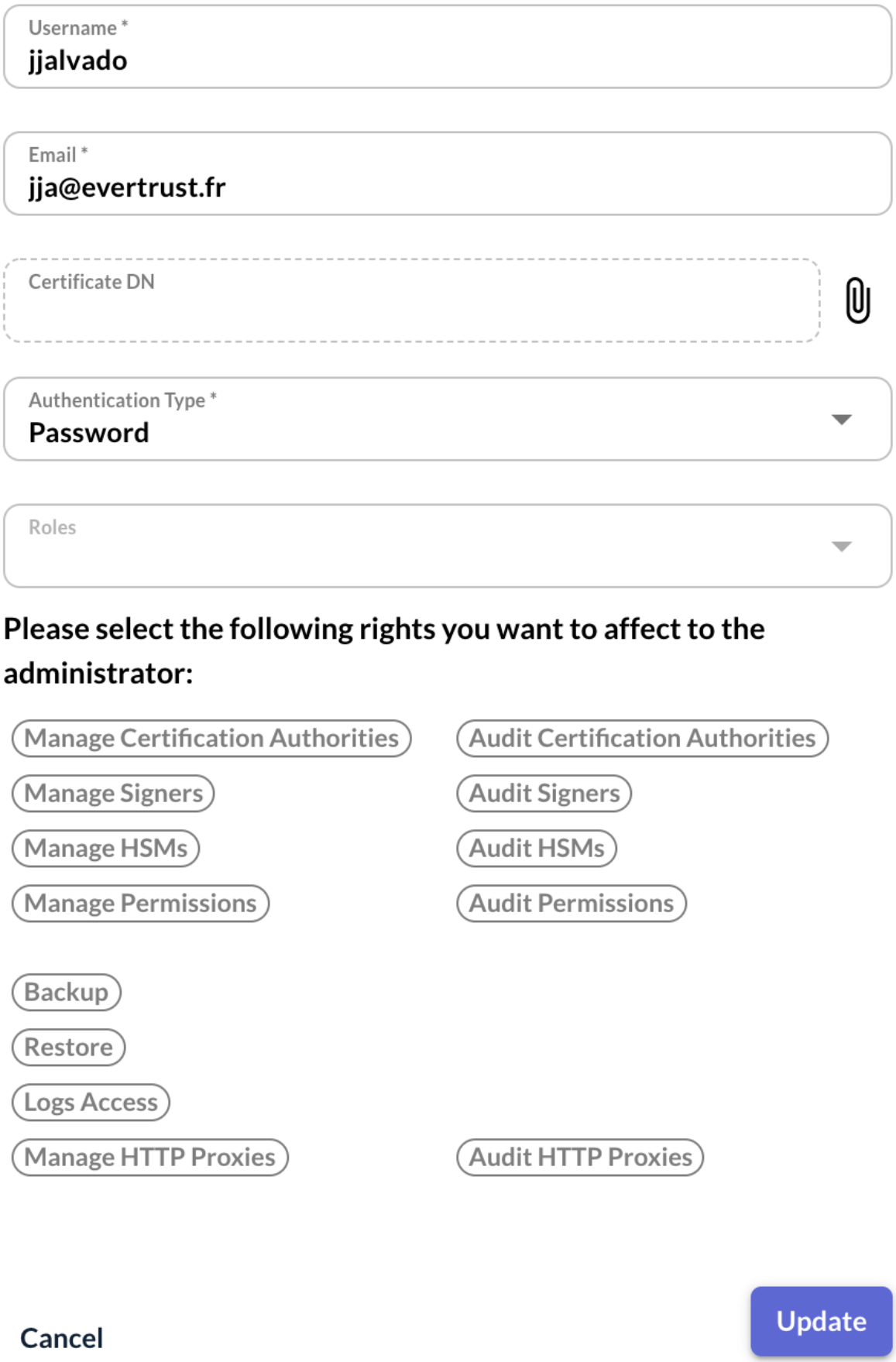
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Administrators**':

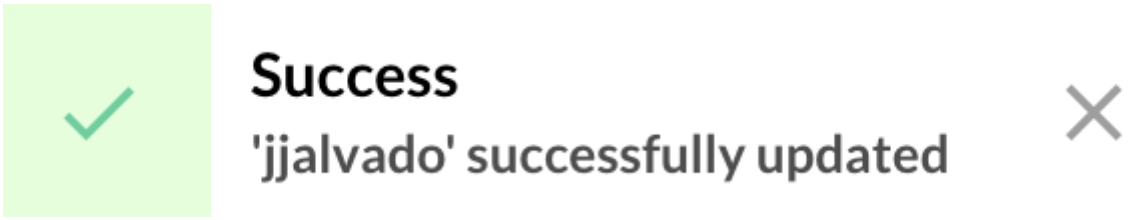


Step 3: Click on the Administrator's name you are willing to edit or hit the  button:

Step 4: Modify the Administrator attributes and hit the '**Update**' button:



Step 5: The Administrator is successfully updated:

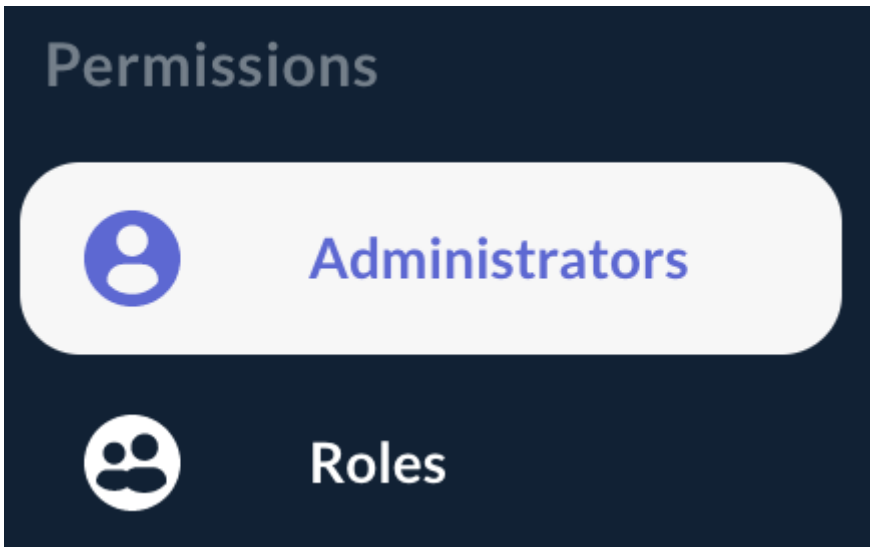

Success
'jjalvado' successfully updated

Deleting an Administrator

It is not possible to delete an Administrator account when logged in with this Administrator account.

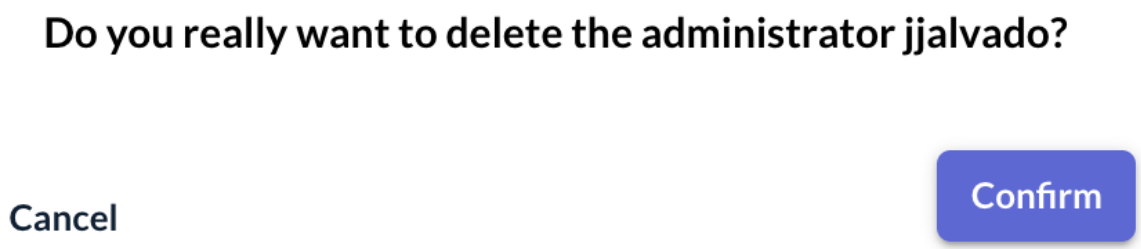
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Administrators**':

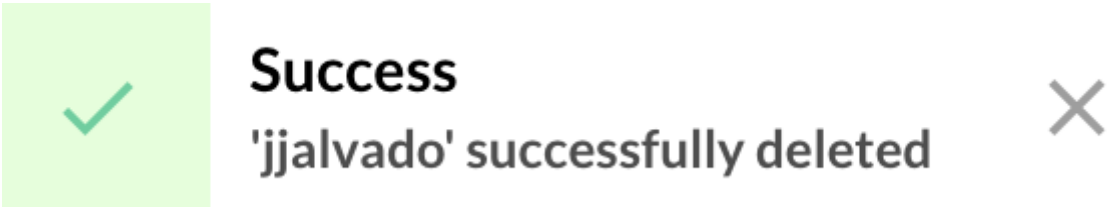


Step 3: Hit the  button of the Administrator you are willing to delete:

Step 4: Hit the '**Confirm**' button:



Step 5: The Administrator is successfully deleted:



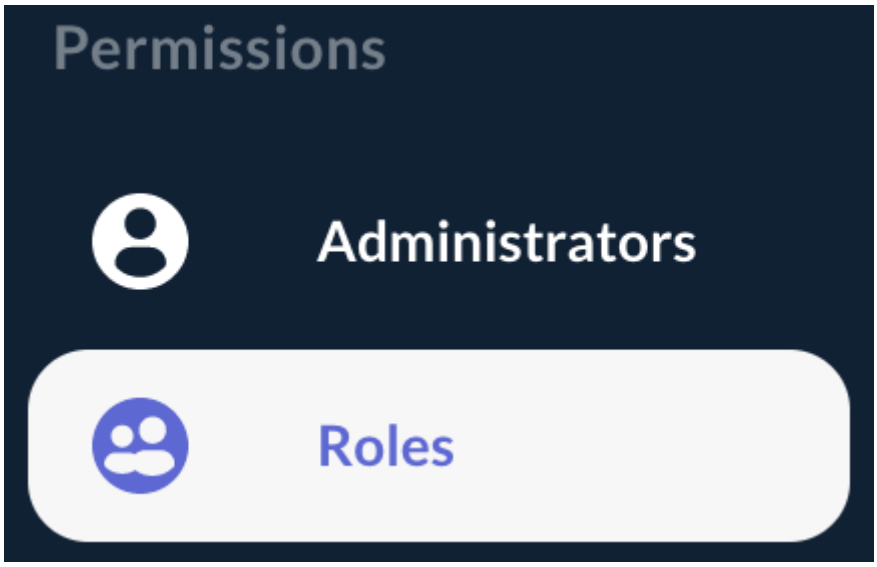
2.6. Managing Roles

This section details how to manage OCSPd Roles.

Creating a Role

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Roles**':



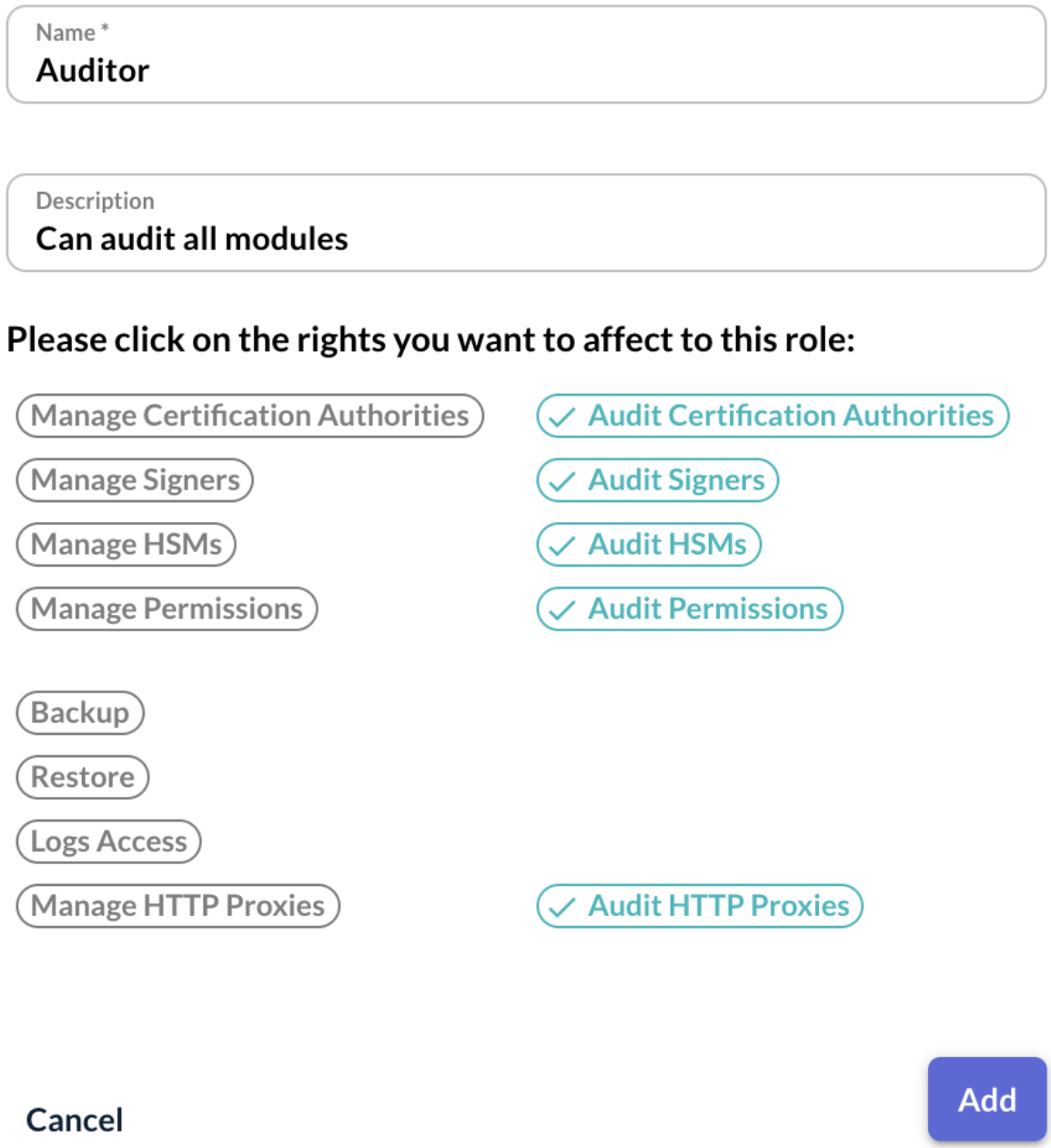
Step 3: In the Roles page, hit the '+' button at the bottom of the page:

Step 4: Specify the following elements:

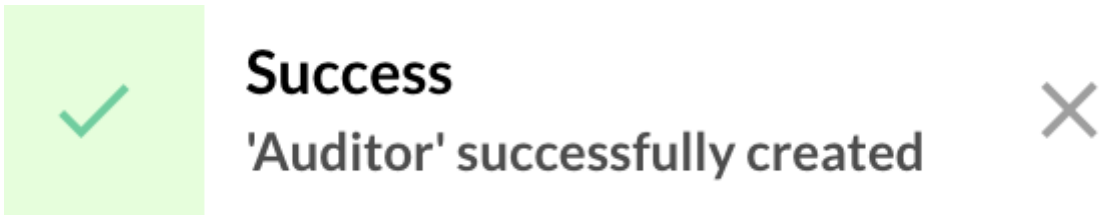
- '**Name**': name of the role;
- '**Description**' (*optional*): description of the role;
- '**Permissions**' (*click on each right to select it*): right(s) of manage/audit each module and perform system tasks given to the role.

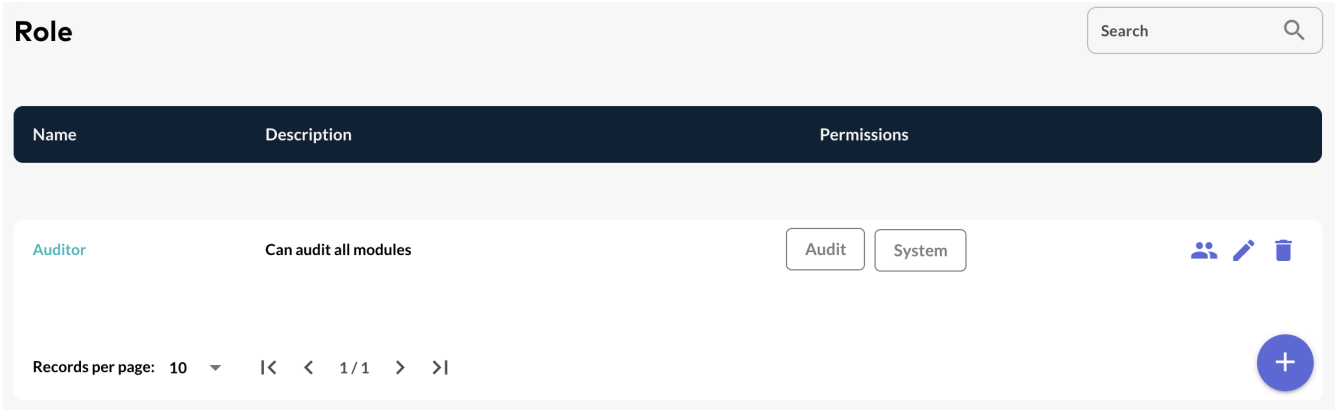
> '**Manage**' right is a '**read and modify**' right. '**Audit**' is a '**read-only**' right.

And hit the '**Add**' button:



Step 5: The Role is successfully created:

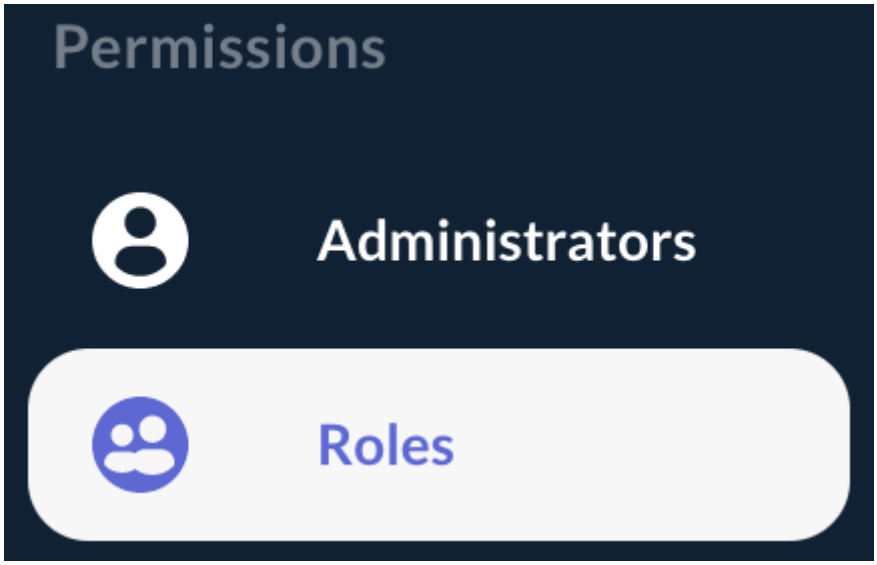



Role
Search
Name
Description
Permissions
Auditor
Can audit all modules
Audit
System
Records per page: 10
1 / 1

Editing a Role

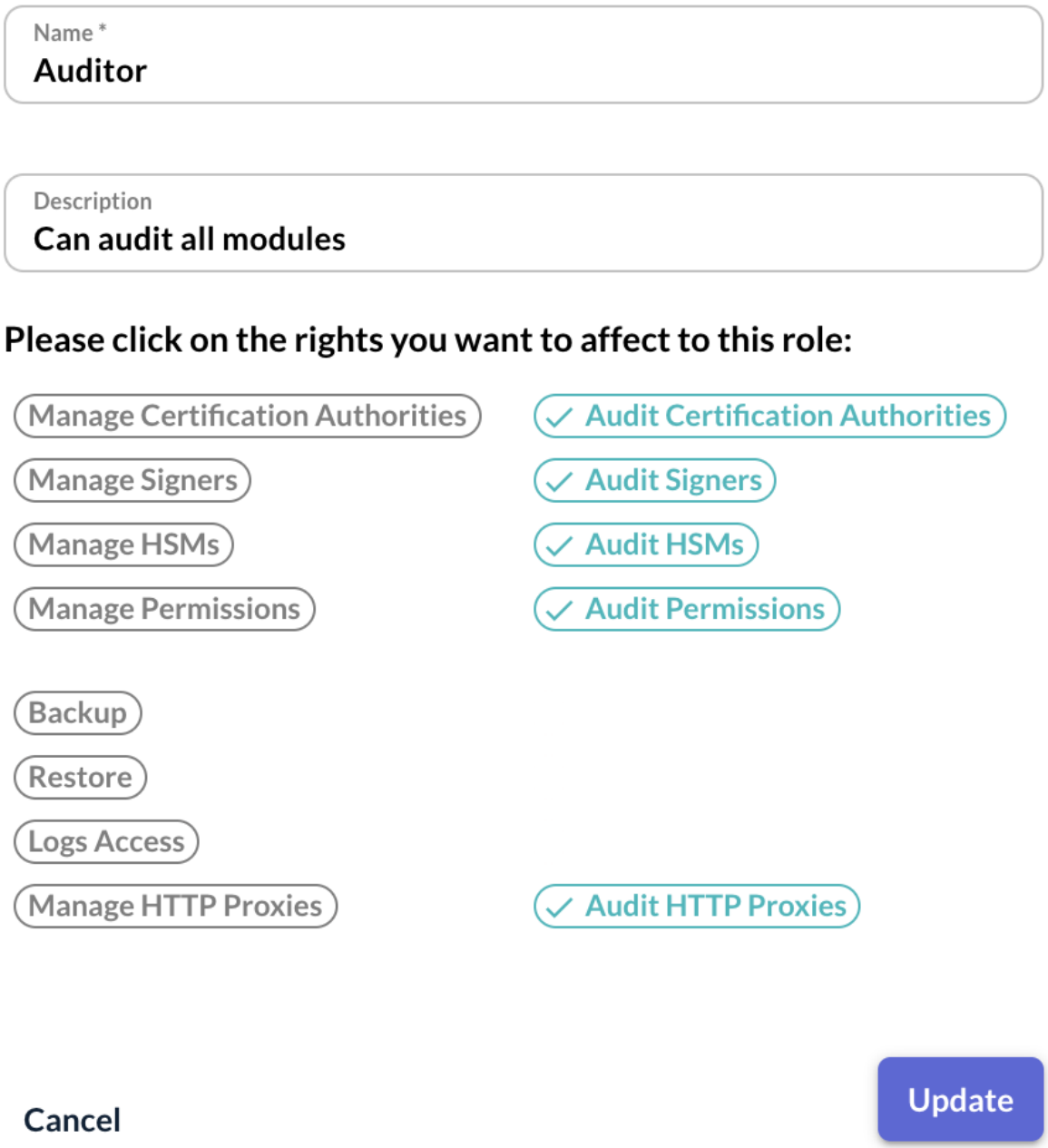
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Roles**':

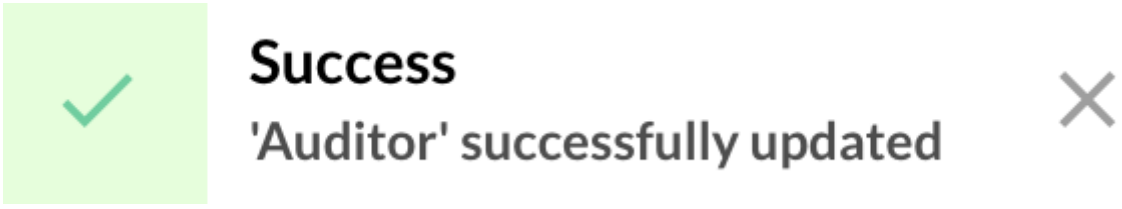


Step 3: Click on the Role's name you are willing to edit or hit the button:

Step 4: Modify the Role attributes and hit the '**Update**' button:



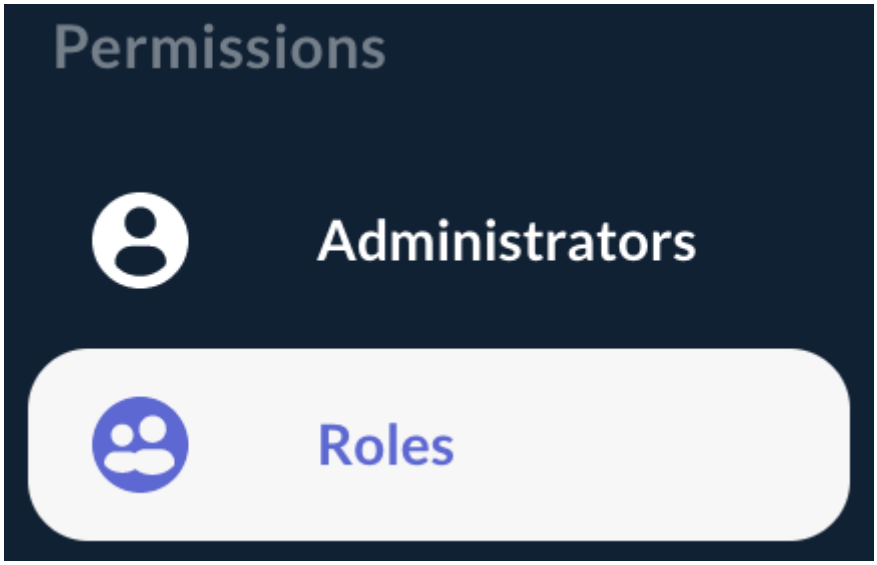
Step 5: The Role is successfully updated:



Display and manage Members of a Role

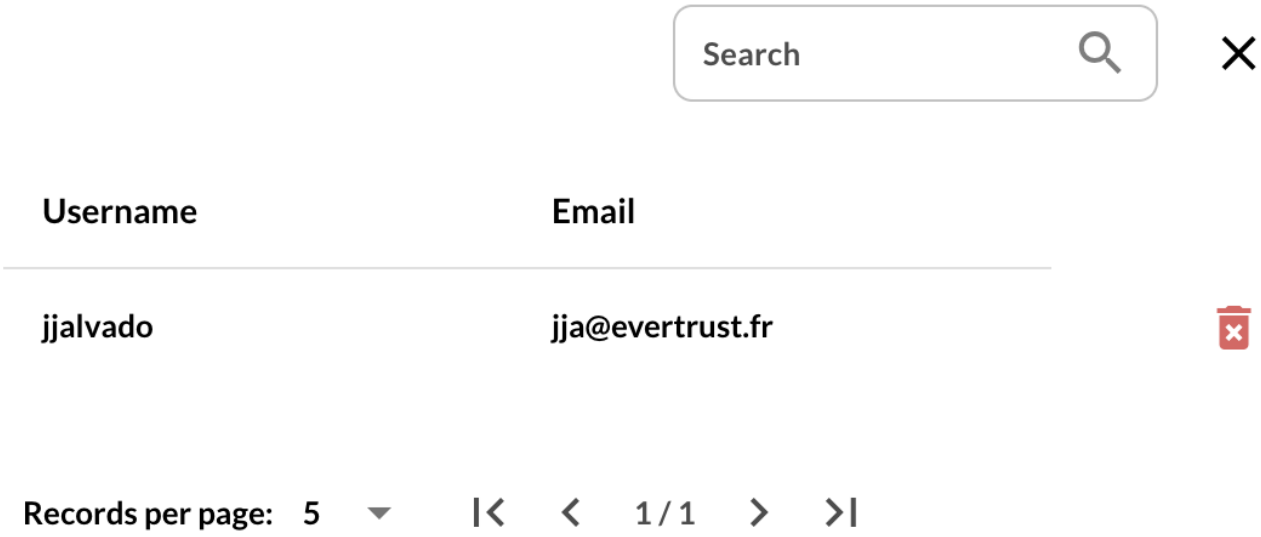
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Roles**':

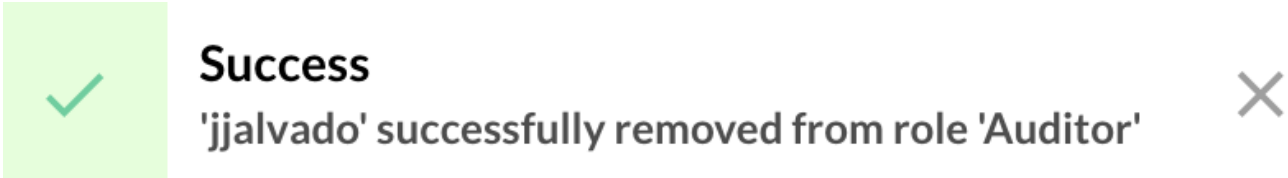


Step 3: For the Role you want to see the Members, hit the button:

Step 4: Hit the button to remove the Administrator from the Role:



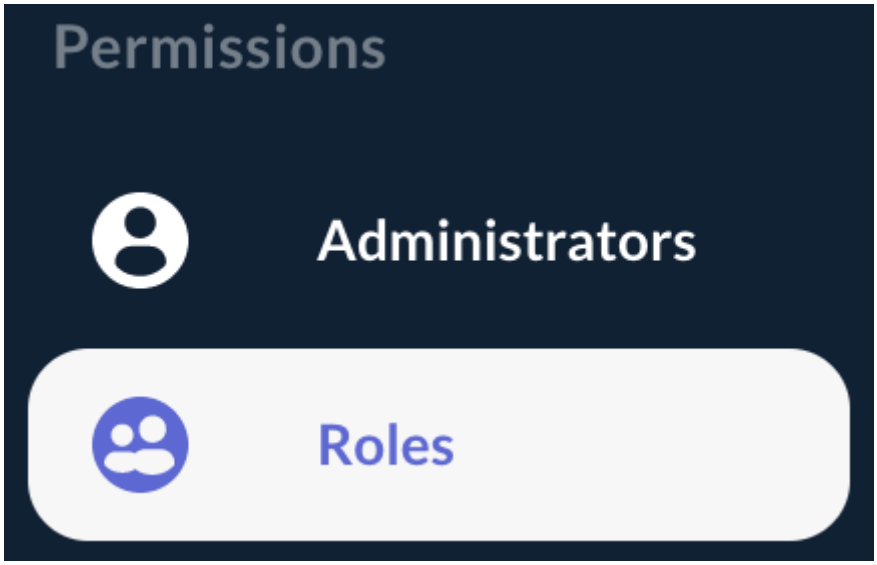
Step 5: The Administrator is successfully removed from the Role:



Deleting a Role

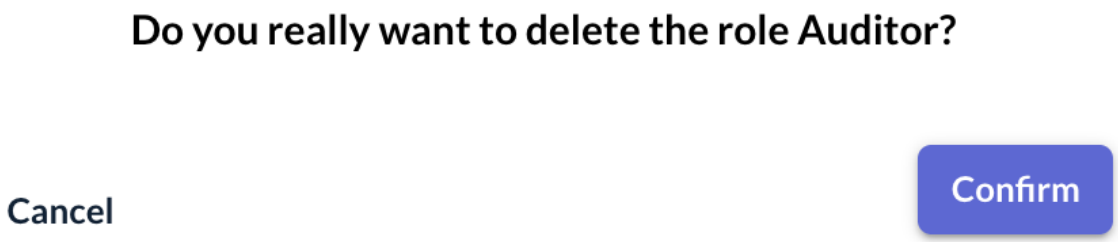
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Permissions**' left menu, select '**Roles**':

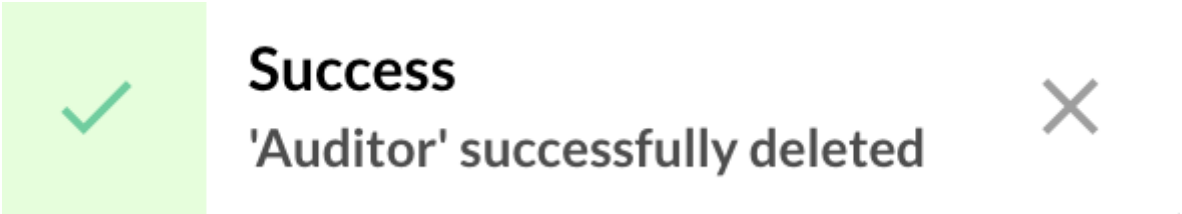


Step 3: Hit the button of the Role you are willing to delete:

Step 4: Hit the '**Confirm**' button:



Step 5: The Role is successfully deleted:



2.7. Managing Hardware Security Modules

OCSPd supports **PKCS#11 compatible crypto devices** (Hardware Security Module, Smartcard, Token) to store the private key of the OCSP Signers.

Supported Hardware Security Modules

As of today, OCSPd has been successfully testes with the following Hardware Security Modules:

- SoftHSM v1 & v2;
- Bull Proteccio;
- Gemalto Safenet Protect Server;
- Gemalto Safenet Luna Network HSM;
- nCipher nShield Connect HSM;
- Utimaco SecurityServer.

If your HSM is not in the list above, this does not necessarily mean that it is not functional, just that it is not officially supported. Contact us and we will accommodate to have it supported.

2.7.1. Managing Modules

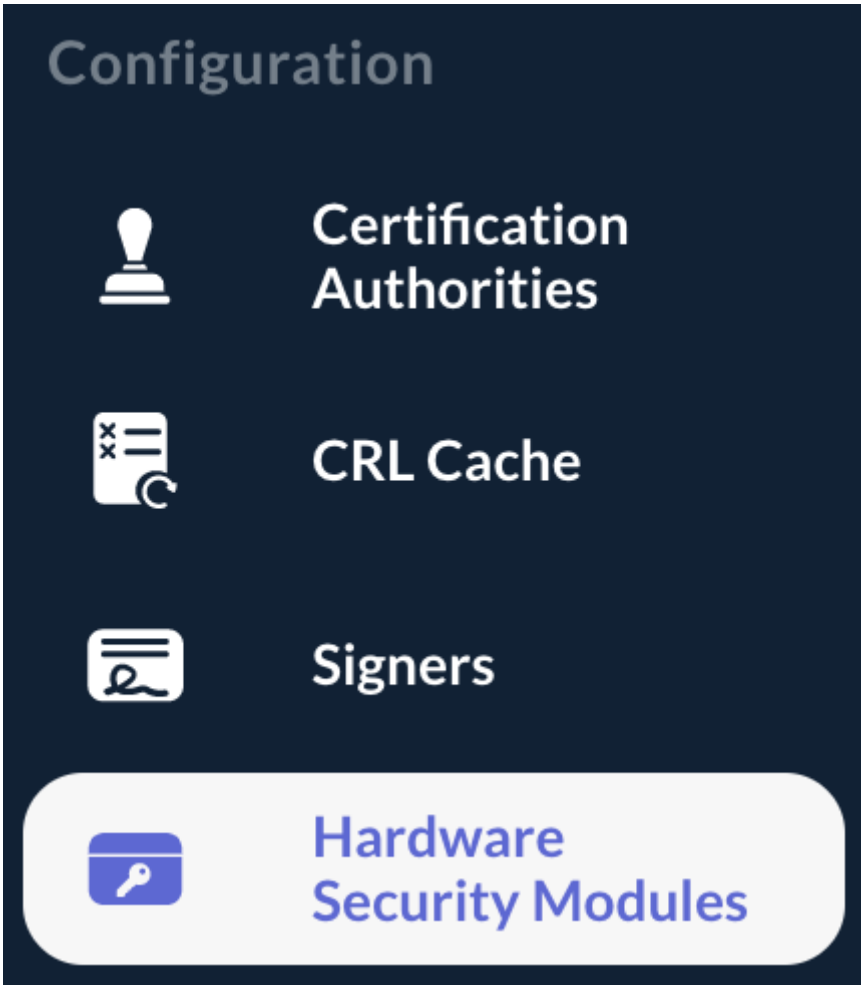
Registering a Module

Initializing the PKCS#11 module must be performed using the tools provided by the HSM provider.

Registering a PKCS#11 module consists in loading the associated PKCS#11 library.

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':



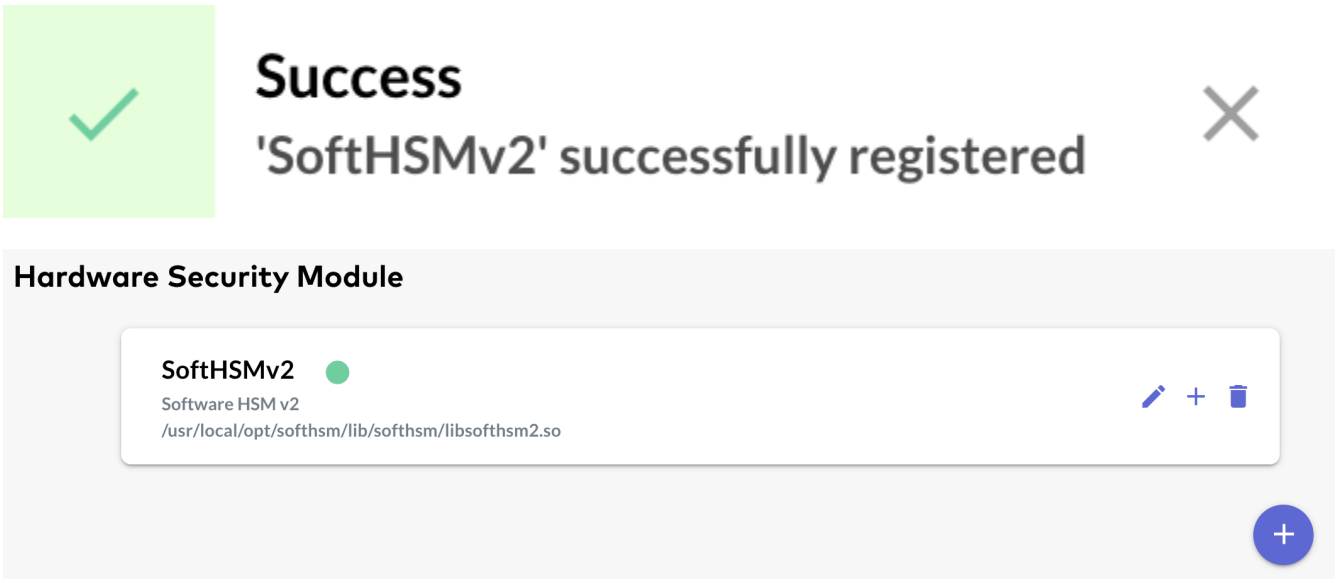
Step 3: In the HSM page, hit the '+' button at the bottom of the page:

Step 4: Specify:

- '**Name**': the name of the HSM module;
- '**Description**' (*optional*): a description of the HSM module;
- '**PKCS#11 Library**': the absolute path where the PKCS#11 library is available.

And hit the '**Register**' button:

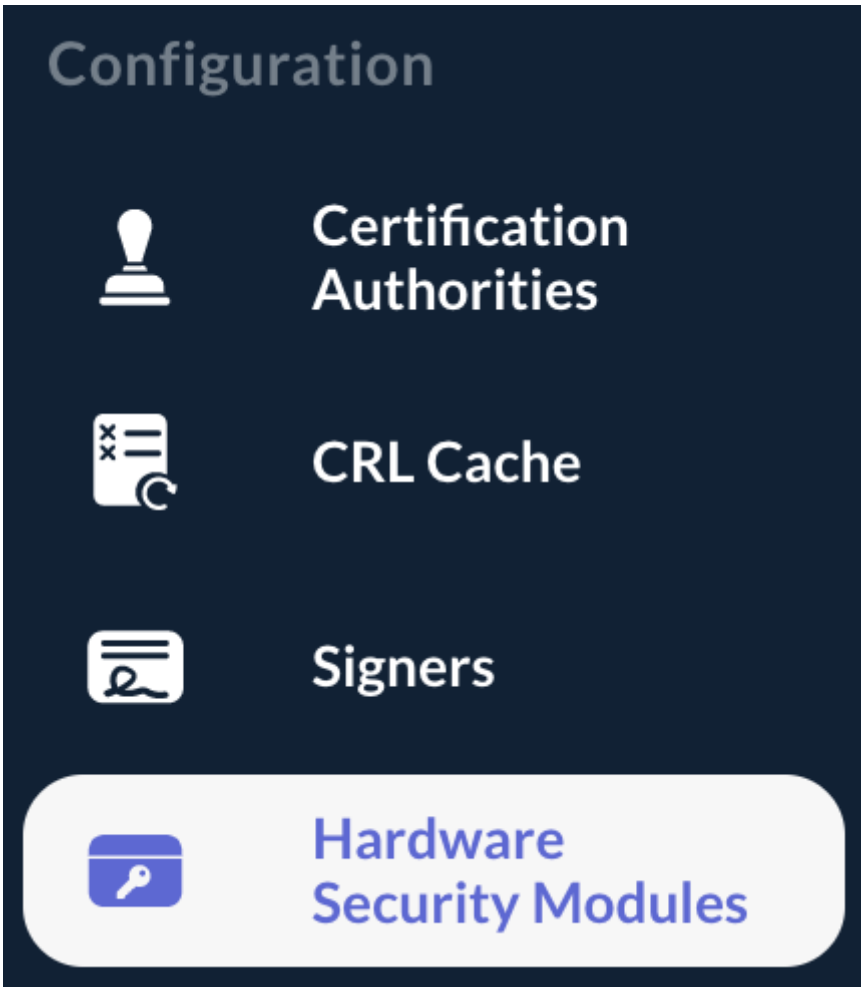
Step 5: The PKCS#11 module is registered:



Editing a Module

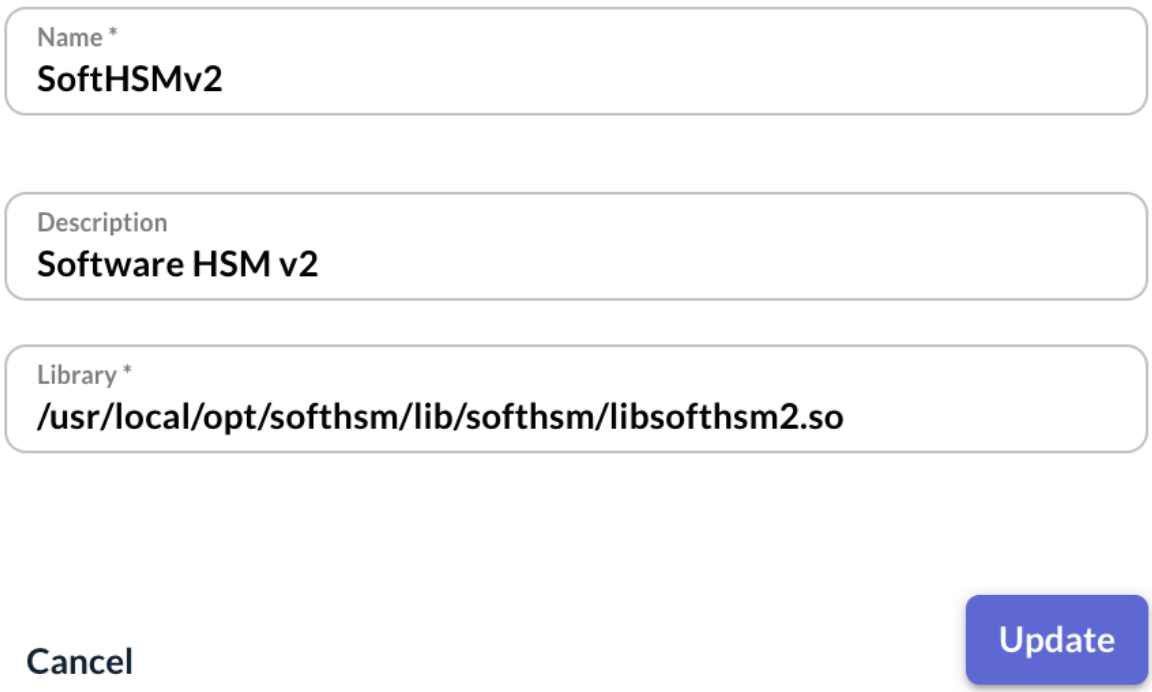
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':

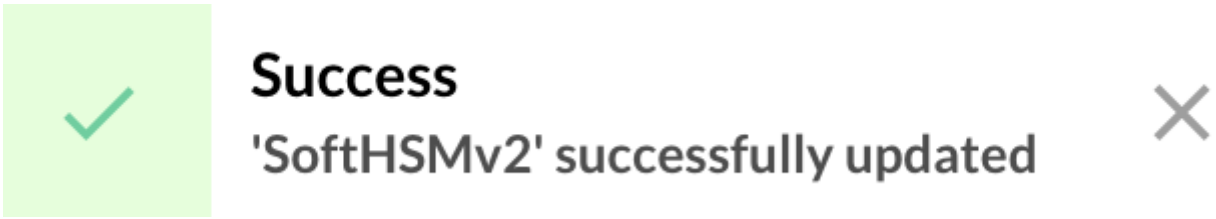


Step 3: In the HSM page, hit the ✎ button of the Module you are willing to edit:

Step 4: Modify the Module attributes and hit the '**Update**' button:



Step 5: The Module is successfully updated:

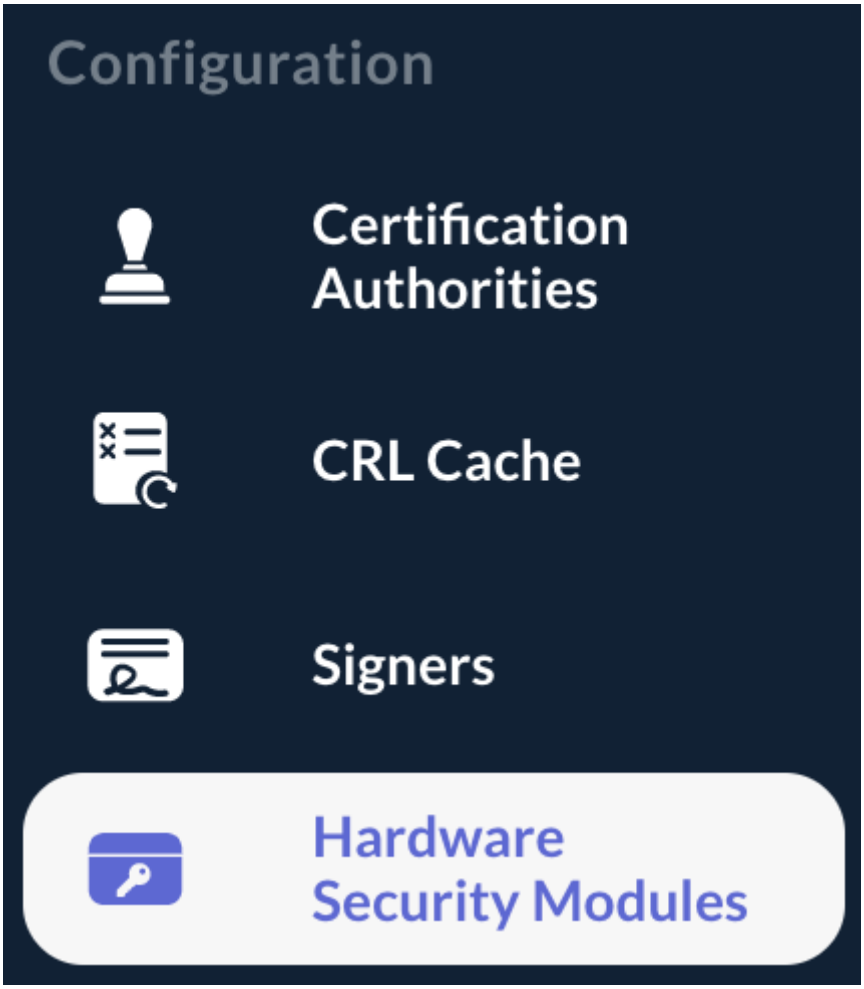


Unregistering a Module

A Module cannot be unregistered if a Slot is registered on the considered Module.

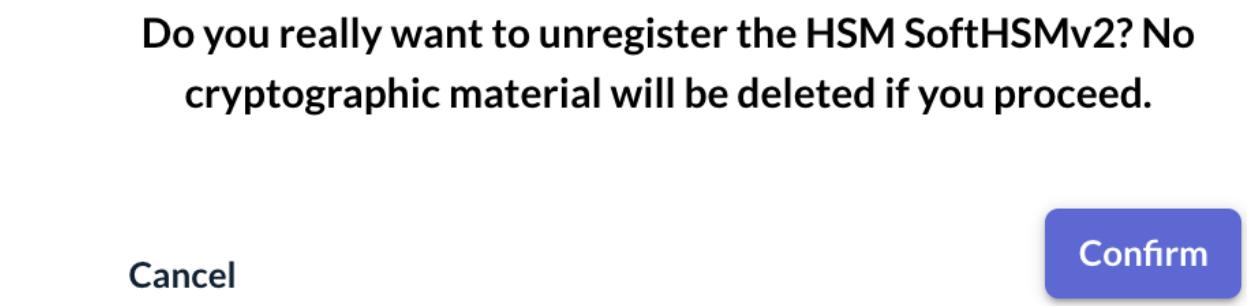
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':

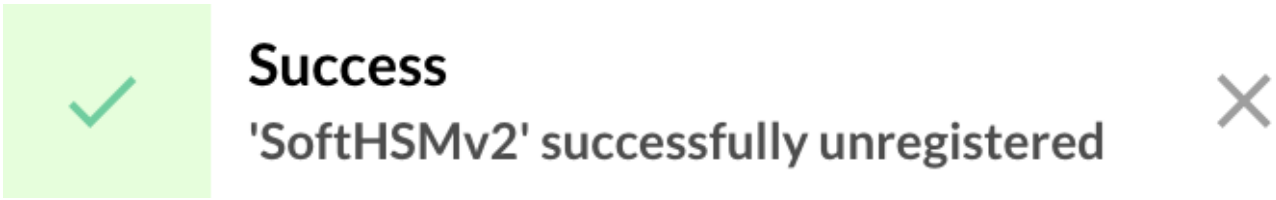


Step 3: In the HSM page, hit the button of the Module you are willing to unregister:

Step 4: Hit the '**Confirm**' button:



Step 5: The module is unregistered:



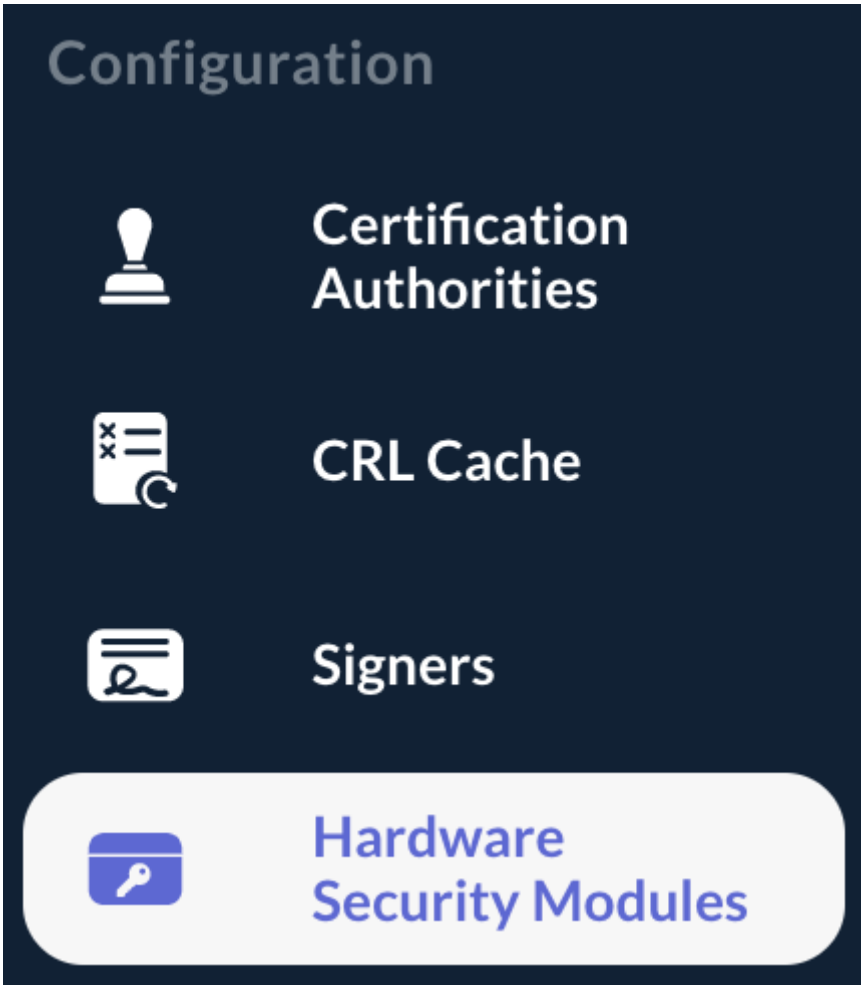
2.7.2. Managing HSM slots

Registering a Slot

Slot are registered on a Module, i.e. you need to register a Module first prior to registering a Slot.

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':

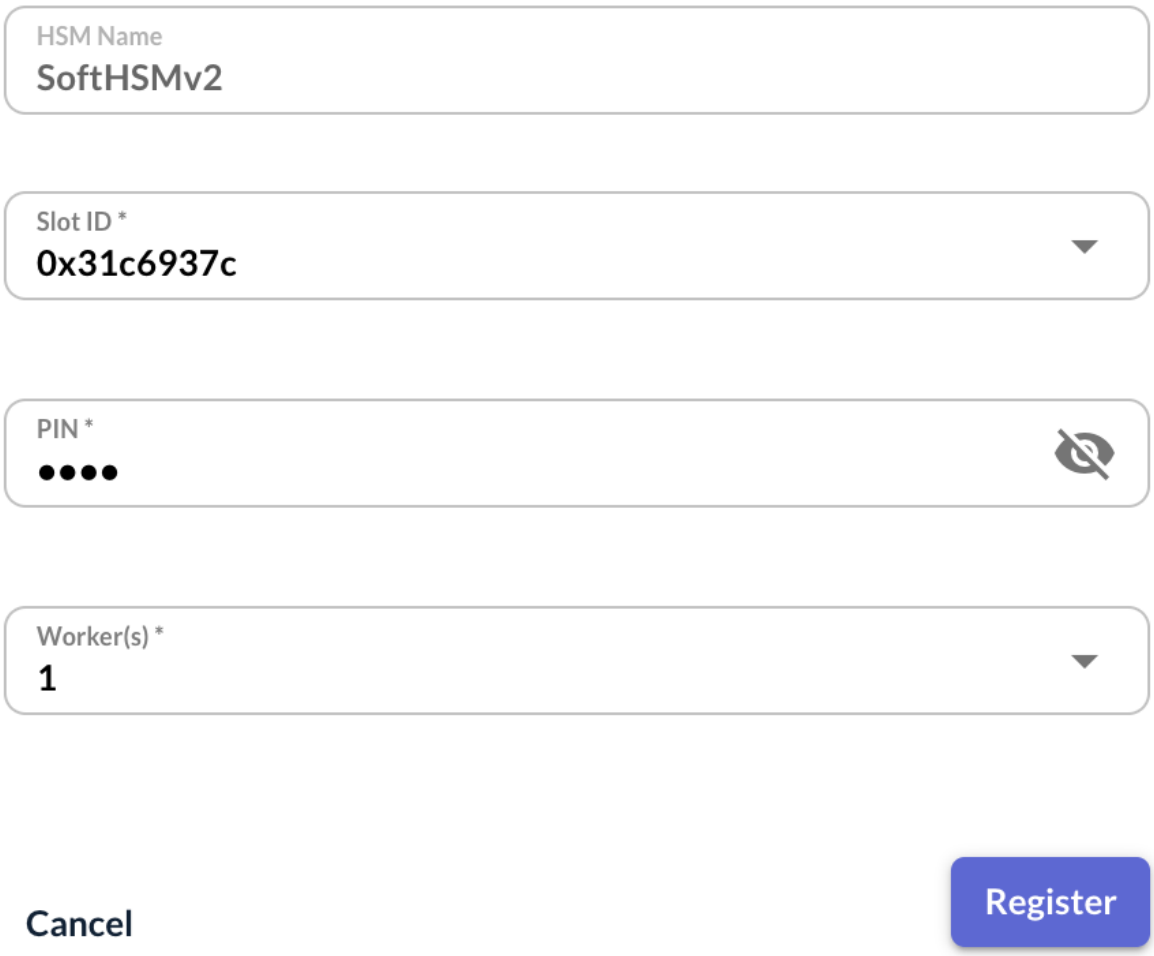


Step 3: Hit the + button of the Module for which you are willing to register a Slot:

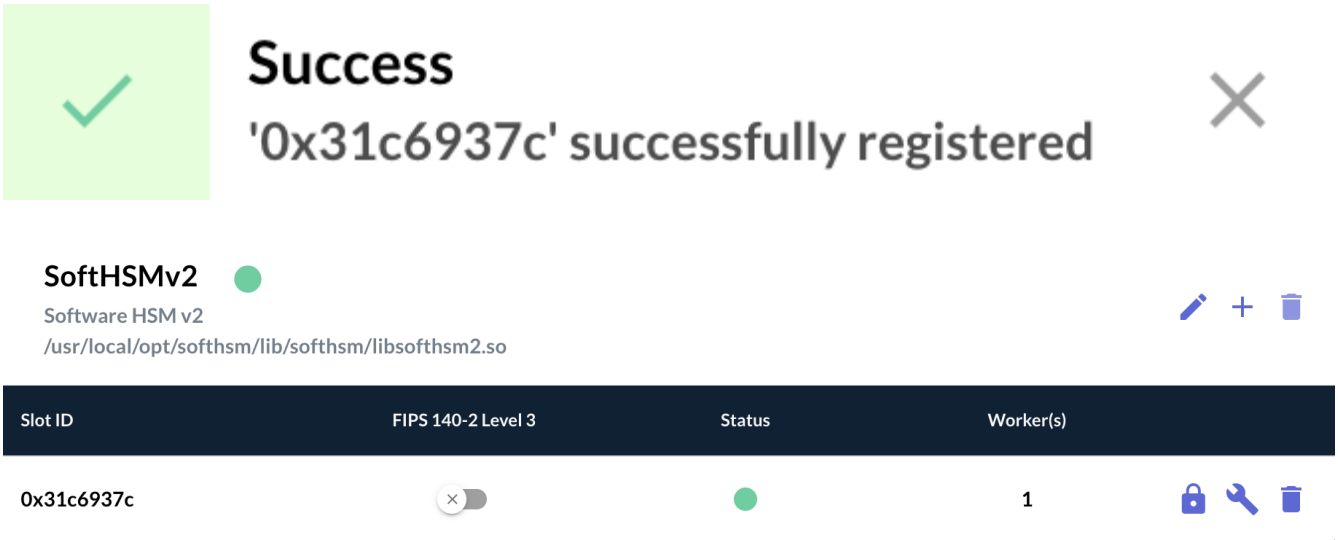
Step 4: Specify:

- '**Slot ID**' (*select*): ID of the Slot on the PKCS#11 Module;
- '**PIN**': the slot PIN;
- '**Worker(s)**': the number of concurrent sessions to open on the slot (limited to '5' by default, but this can be increased by tweaking the configuration).

And hit the '**Register**' button:



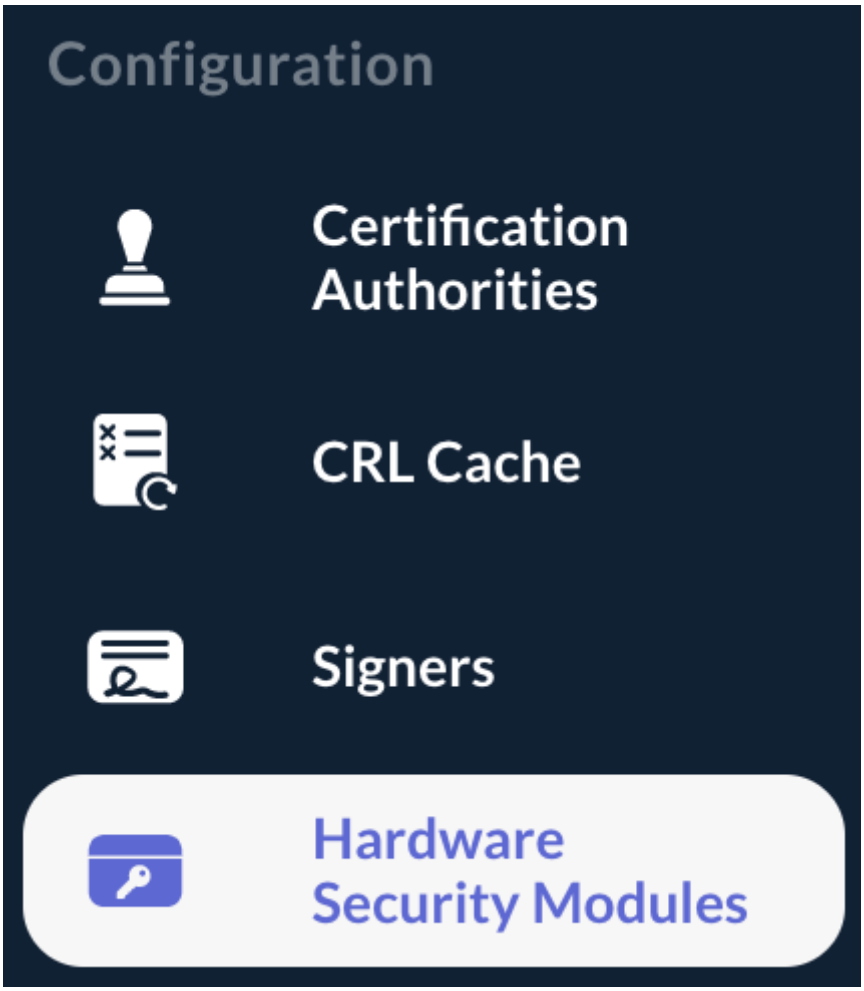
Step 5: The Slot is successfully registered:



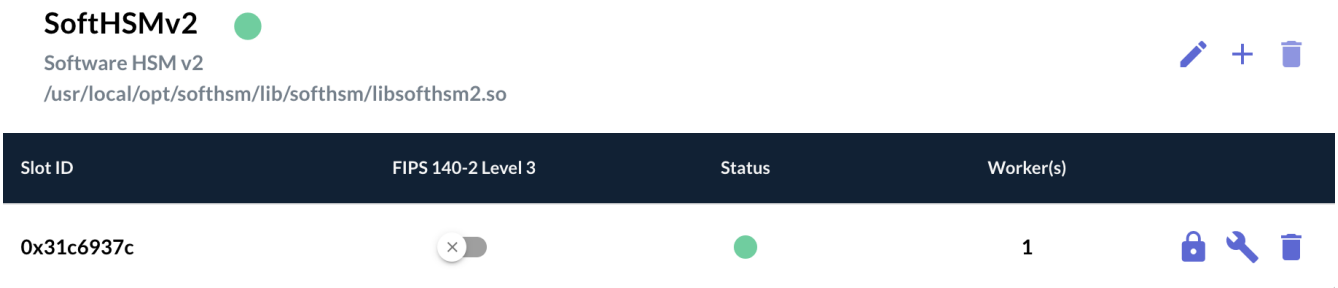
Modifying the Slot PIN

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':

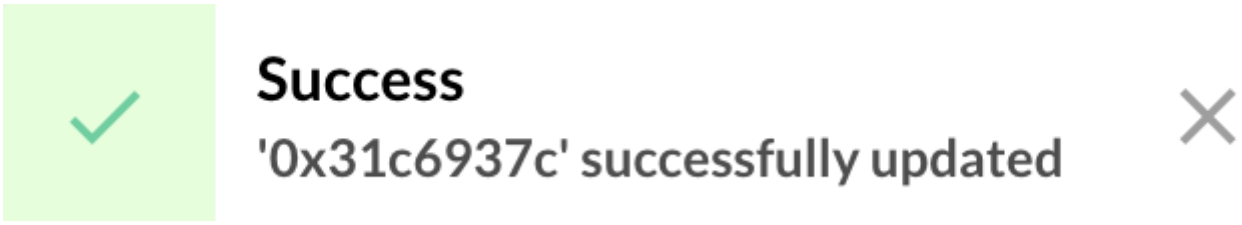


Step 3: Hit the button of the Slot for which you are willing to modify the PIN:



Step 4: Specify the new Slot PIN and hit the '**Set**' button:

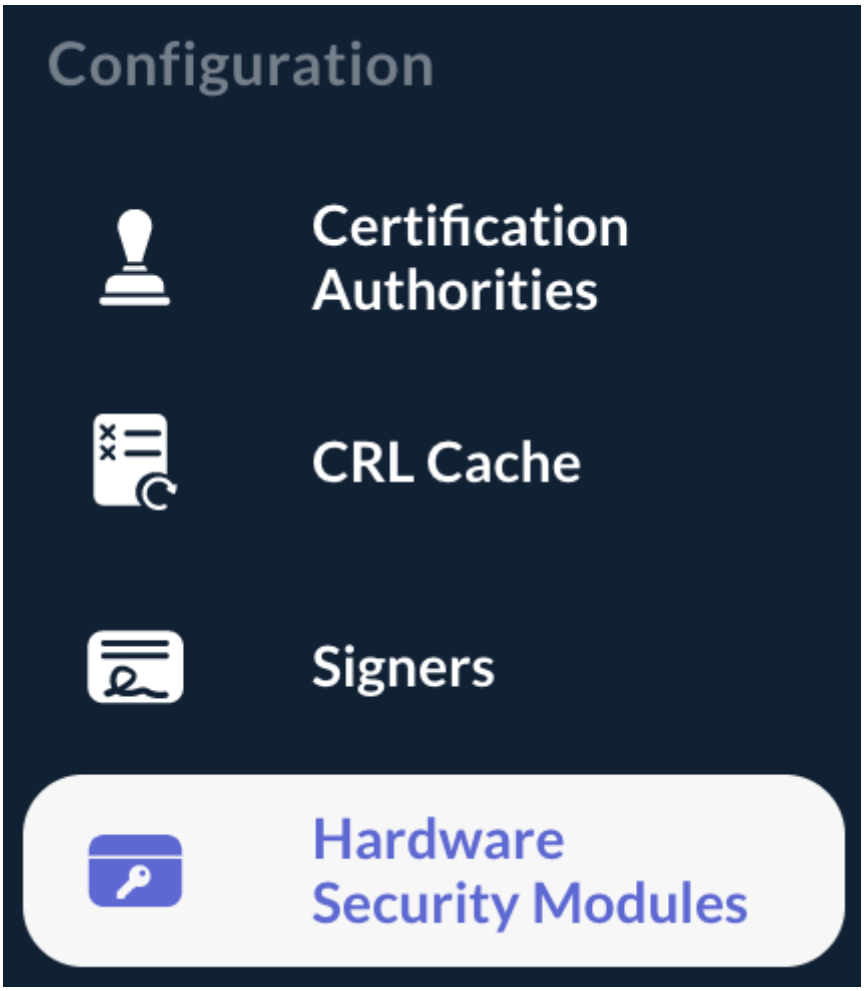
Step 5: The Slot PIN is successfully set:



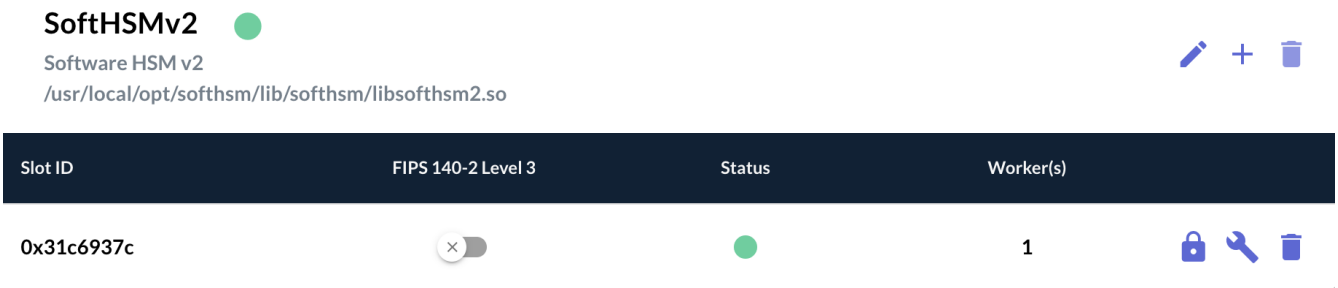
Modifying the Slot Worker(s)

Step 1: Access the OCSPd Web Management Console;

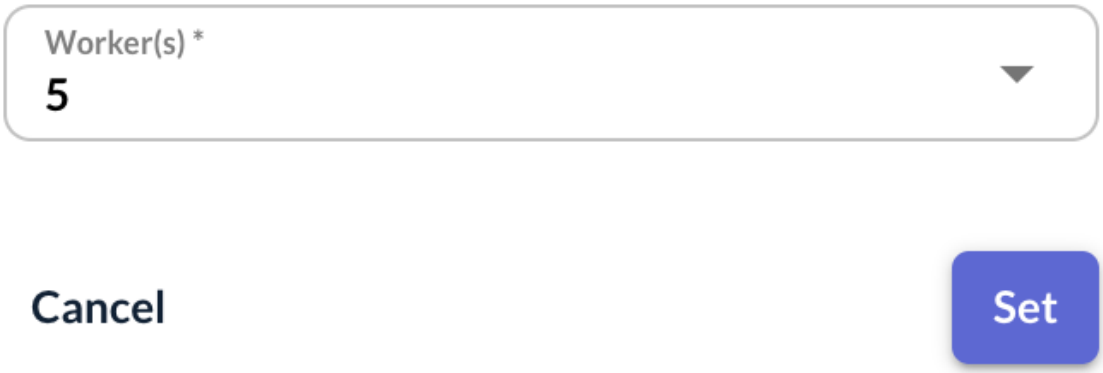
Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':



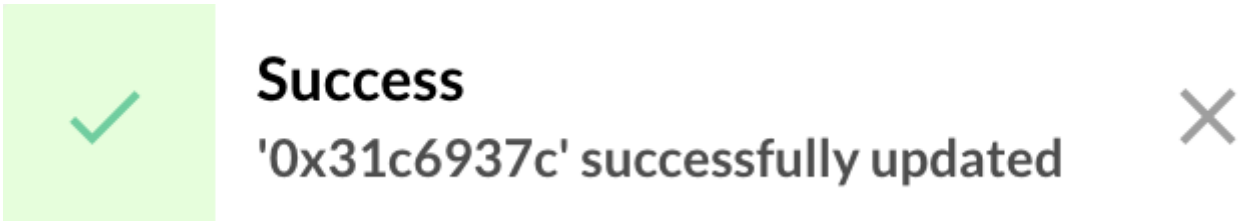
Step 3: Hit the button of the Slot for which you are willing to modify the Worker(s):



Step 4: Specify the new '**Worker(s)**' value and hit the '**Set**' button:



Step 5: The Worker(s) is successfully set:

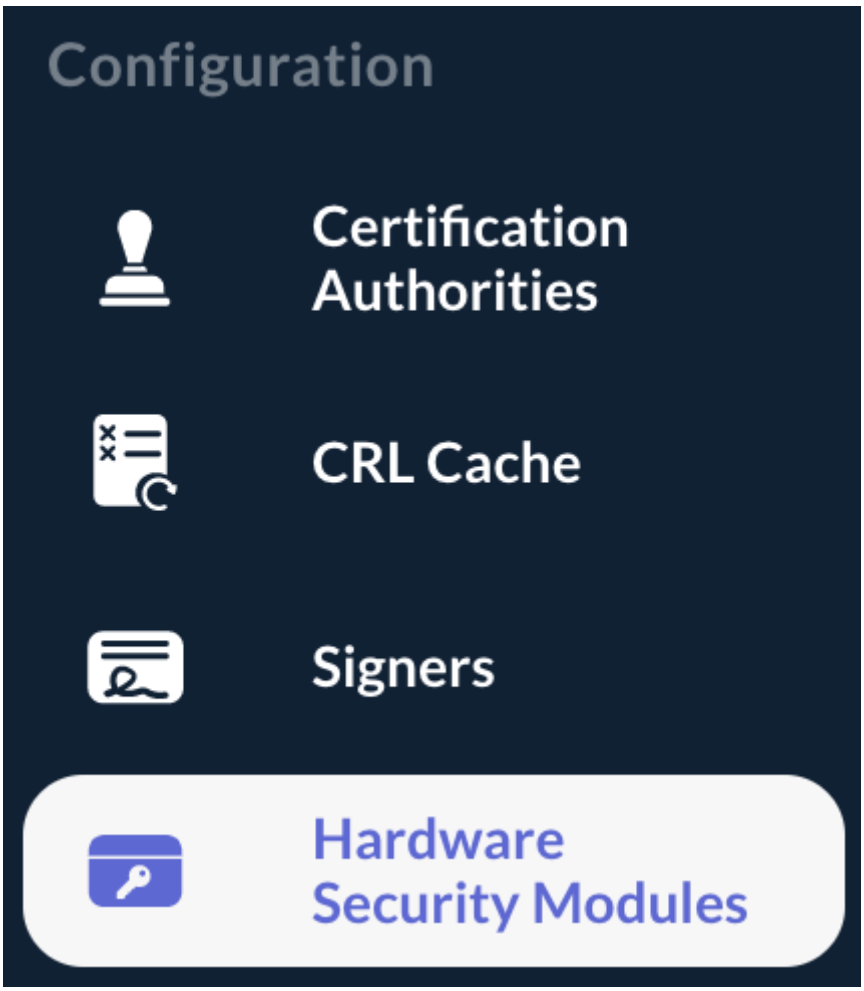


Unregistering a Slot

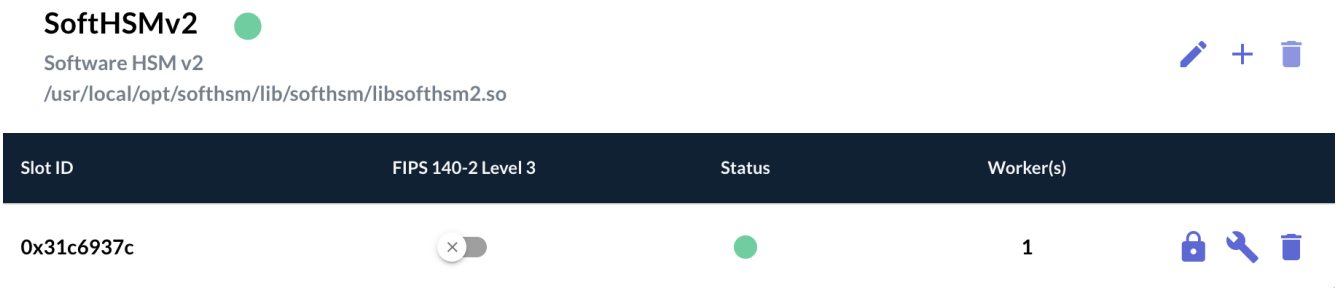
A Slot cannot be unregistered if it is referenced by a Signer, i.e. the Signer storing its private key within the considered Slot must be deleted first.

Step 1: Access the OCSPd Web Management Console;

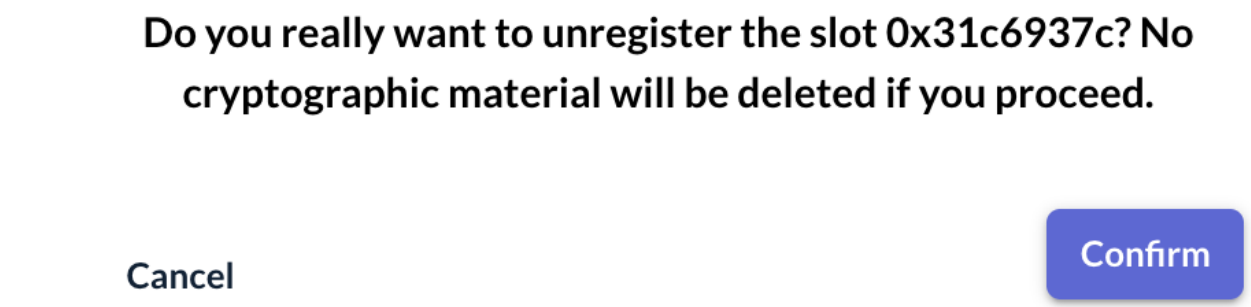
Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':



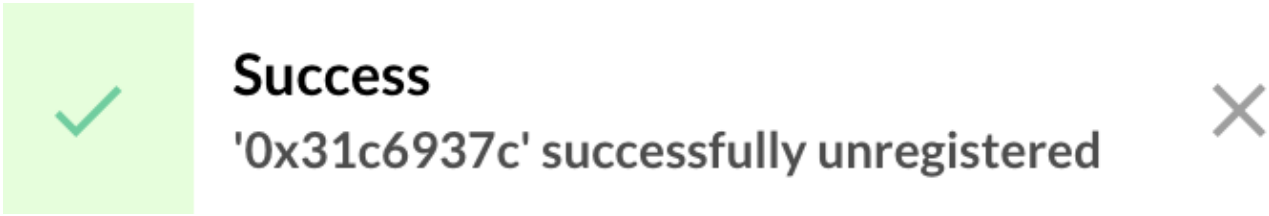
Step 3: Hit the button of the Slot you are willing to unregister:



Step 4: Hit the '**Confirm**' button:



Step 5: The Slot is successfully unregistered:



2.7.3. Managing FIPS 140-2 Level 3 Key Generation Mode

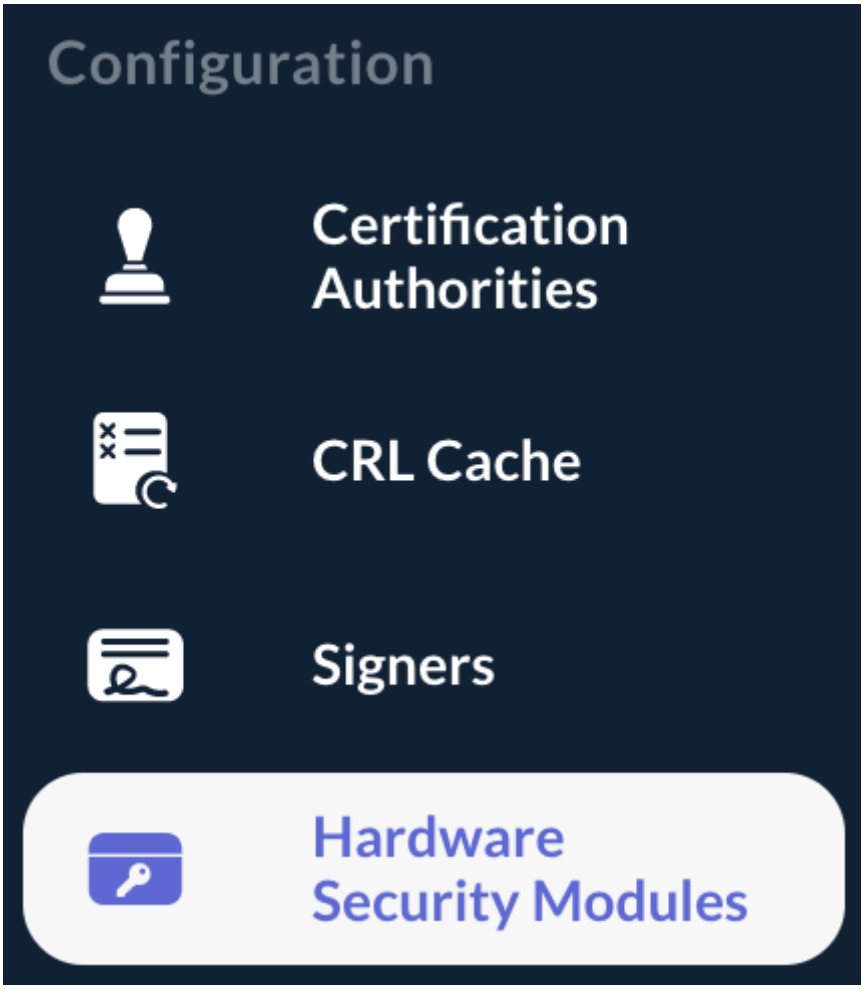
Enabling FIPS 140-2 Level 3 Key Generation Mode

Enabling 'FIPS 140-2 Level 3 Key Generation Mode' causes key to be generated using the '**CKM_RSA_X9_31_KEY_PAIR_GEN**' mechanism within the HSM. Do not enable this mode unless:

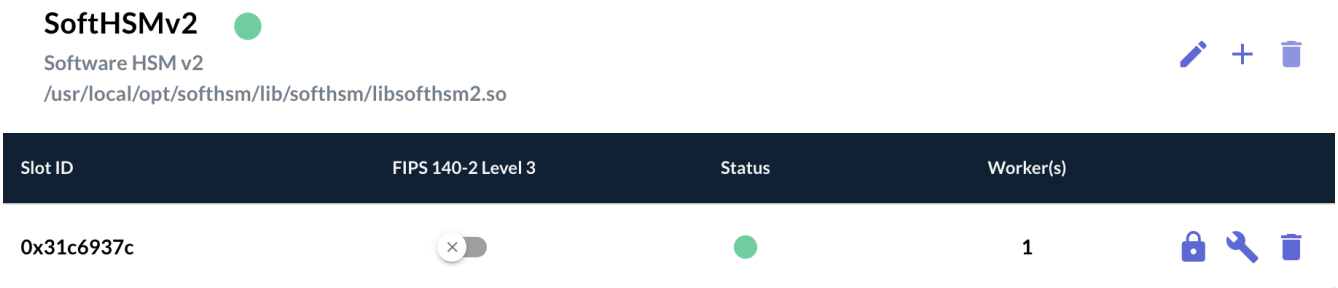
- The Hardware Security Module supports this key generation mechanism;
- Issuing the key pair using the key mechanism is mandatory.

Step 1: Access the OCSPd Web Management Console;

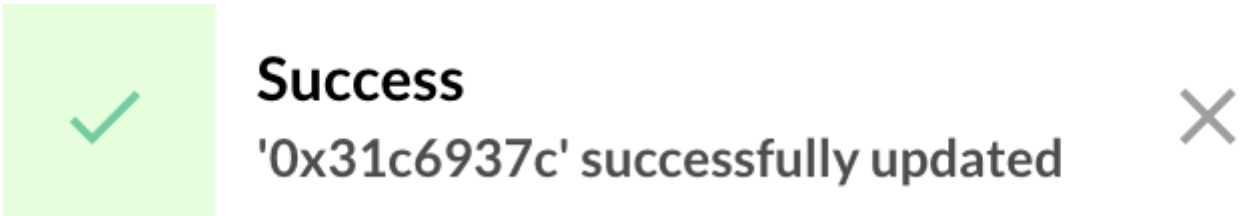
Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':



Step 3: Hit the button of the Slot for which you are willing to enable FIPS 140-2 Level 3 Key Generation Mode:



Step 4: FIPS 140-2 Level 3 is now enabled. New keypair will be generated using the '**CKM_RSA_X9_31_KEY_PAIR_GEN**' mechanism:



SoftHSMv2

Software HSM v2

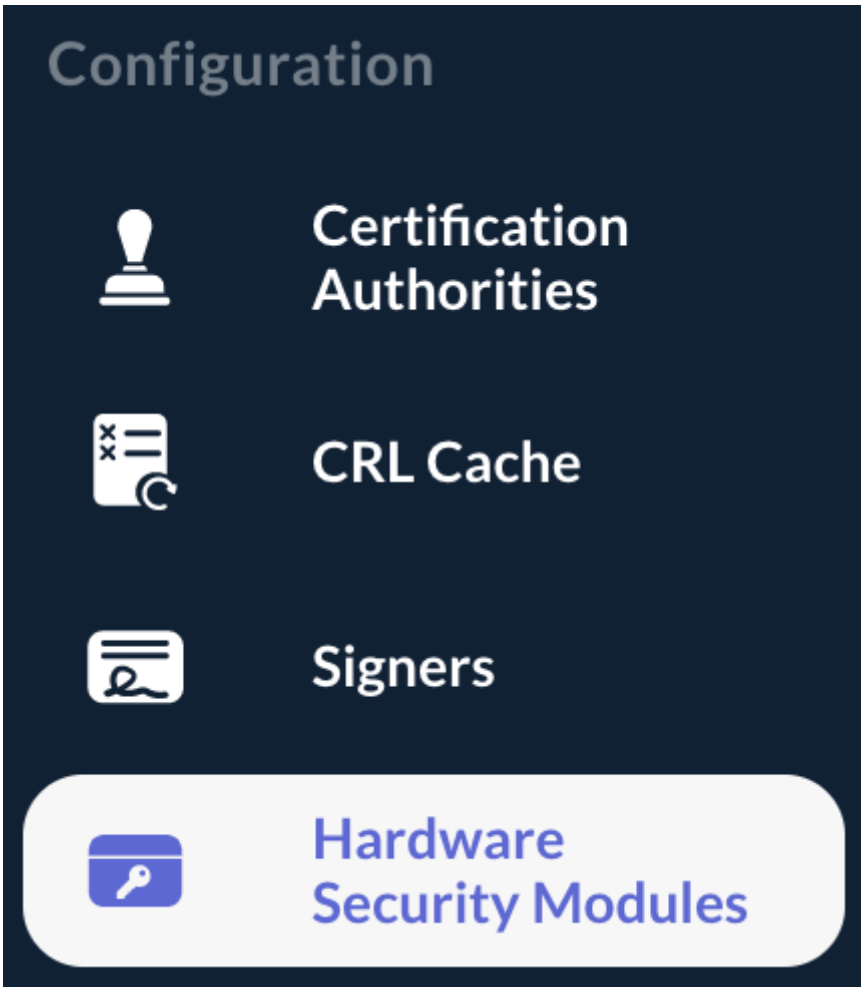
/usr/local/opt/softhsm/lib/softhsm/libsofthsm2.so

Slot ID	FIPS 140-2 Level 3	Status	Worker(s)
0x31c6937c			1

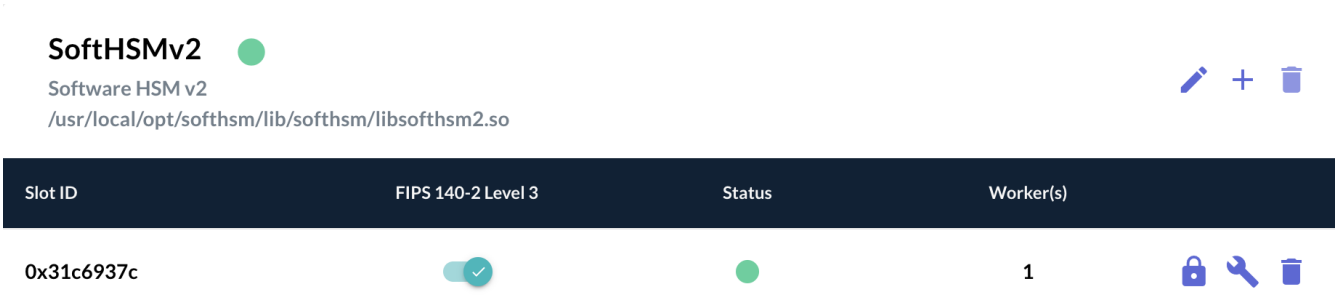
Disabling FIPS 140-2 Level 3 Key Generation Mode

Step 1: Access the OCSPd Web Management Console;

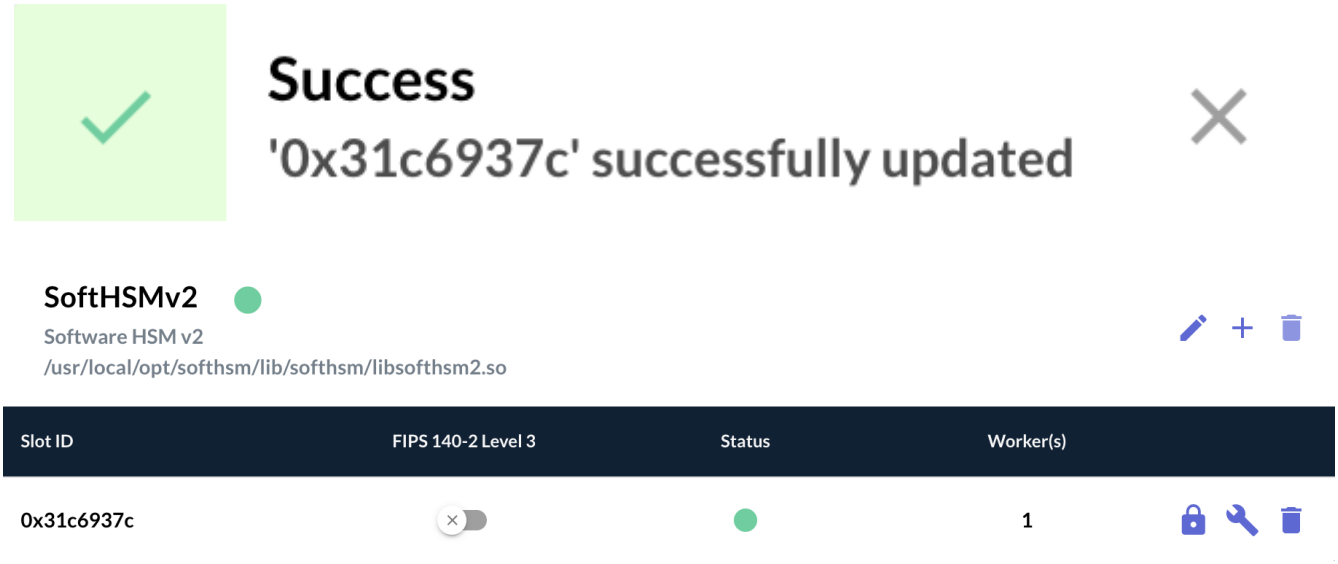
Step 2: In the '**Configuration**' left menu, select '**Hardware Security Modules**':



Step 3: Hit the button of the Slot for which you are willing to disable FIPS 140-2 Level 3 Key Generation Mode:



Step 4: FIPS 140-2 Level 3 is now disabled. New keypair will be generated using the '**CKM_RSA_PKCS_KEY_PAIR_GEN**' mechanism:



2.7.4. HSM specifics

nCipher nShield Connect

To integrate the nCipher nShield Connect HSM, the **cknfastrc** configuration file must be updated with the following configuration entry:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=Y
```

Utimaco CryptoServer

To integrate the Utimaco CryptoServer, the ocspd configuration file (**/etc/default/ocspd**) must be modified and the following lines lust be added at the beginning of the configuration file:

```
# Utimaco specific export
export CS_PKCS11_R2_CFG=[CS_PKCS11_R2]
```

Where [CS_PKCS11_R2] is the absolute path of the cs_pkcs11_R2.cfg configuration file.

The [CS_PKCS11_R2] configuration file must be updated as well to enable a session keep alive:

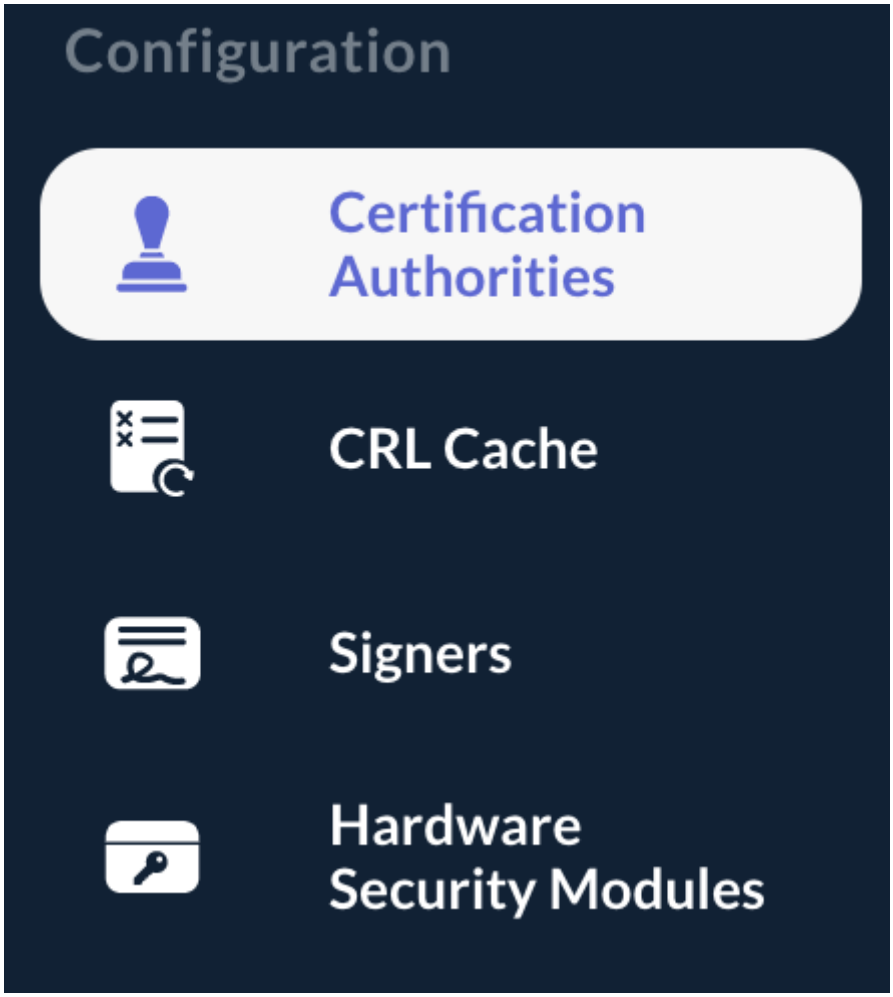
```
# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true
```

2.8. Managing Certificate Authorities

2.8.1. Importing a Certificate Authority

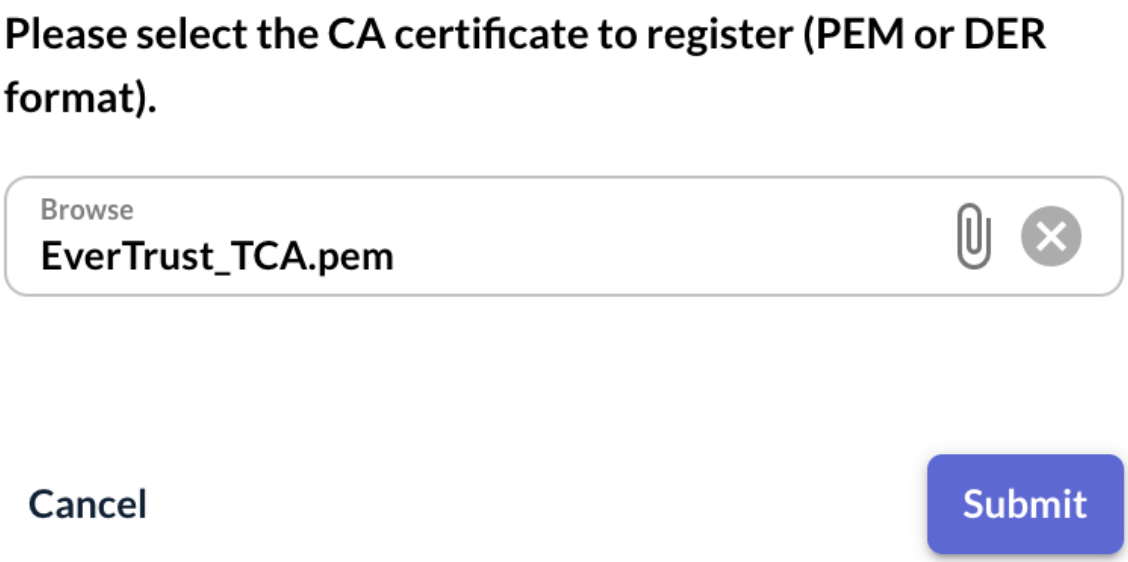
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':

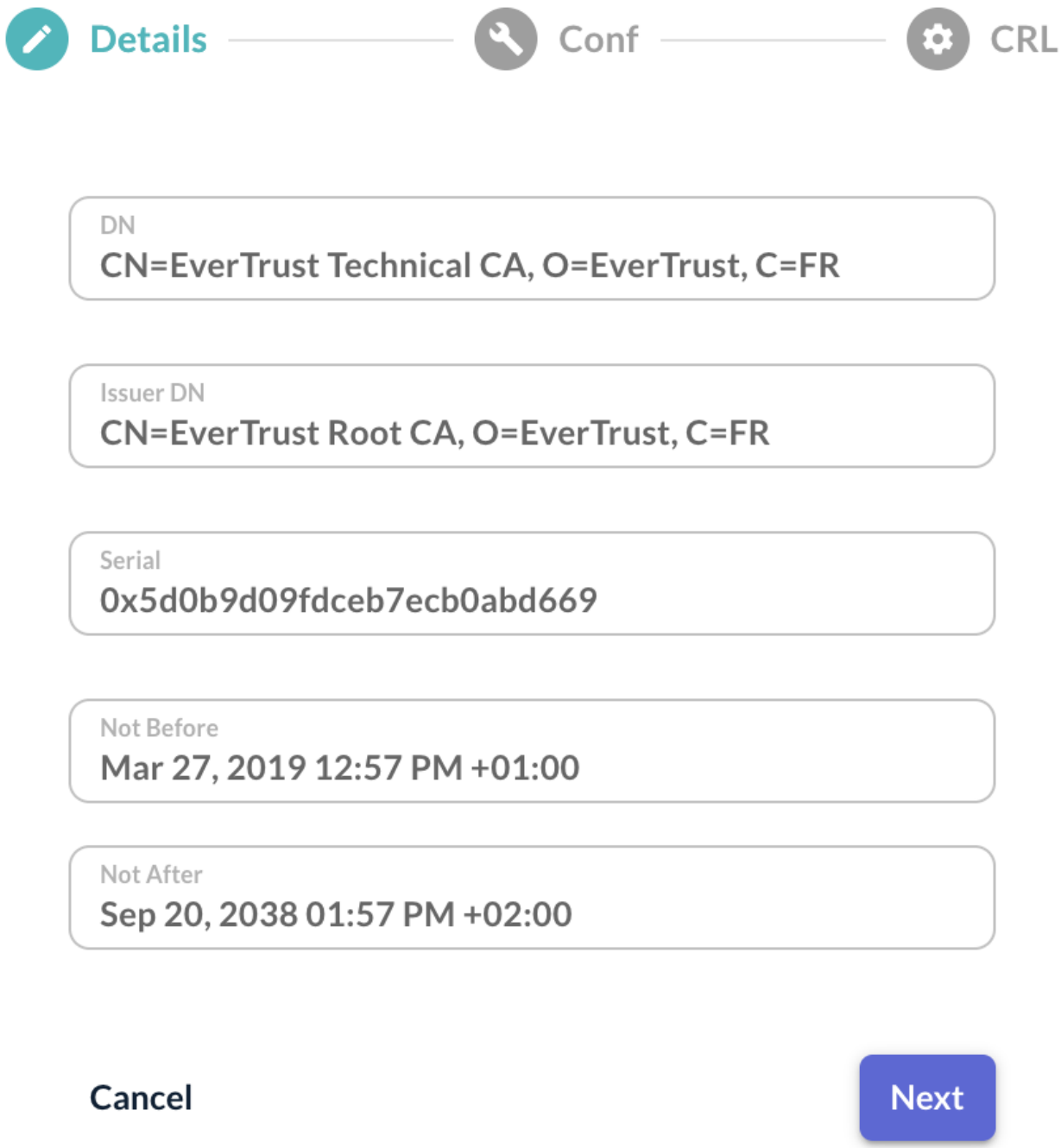


Step 3: In the Certificate Authorities page, hit the '+' button at the bottom of the page:

Step 4: Browse for the certificate of the Certificate Authority you are willing to load (PEM or DER) and hit the '**Submit**' button:



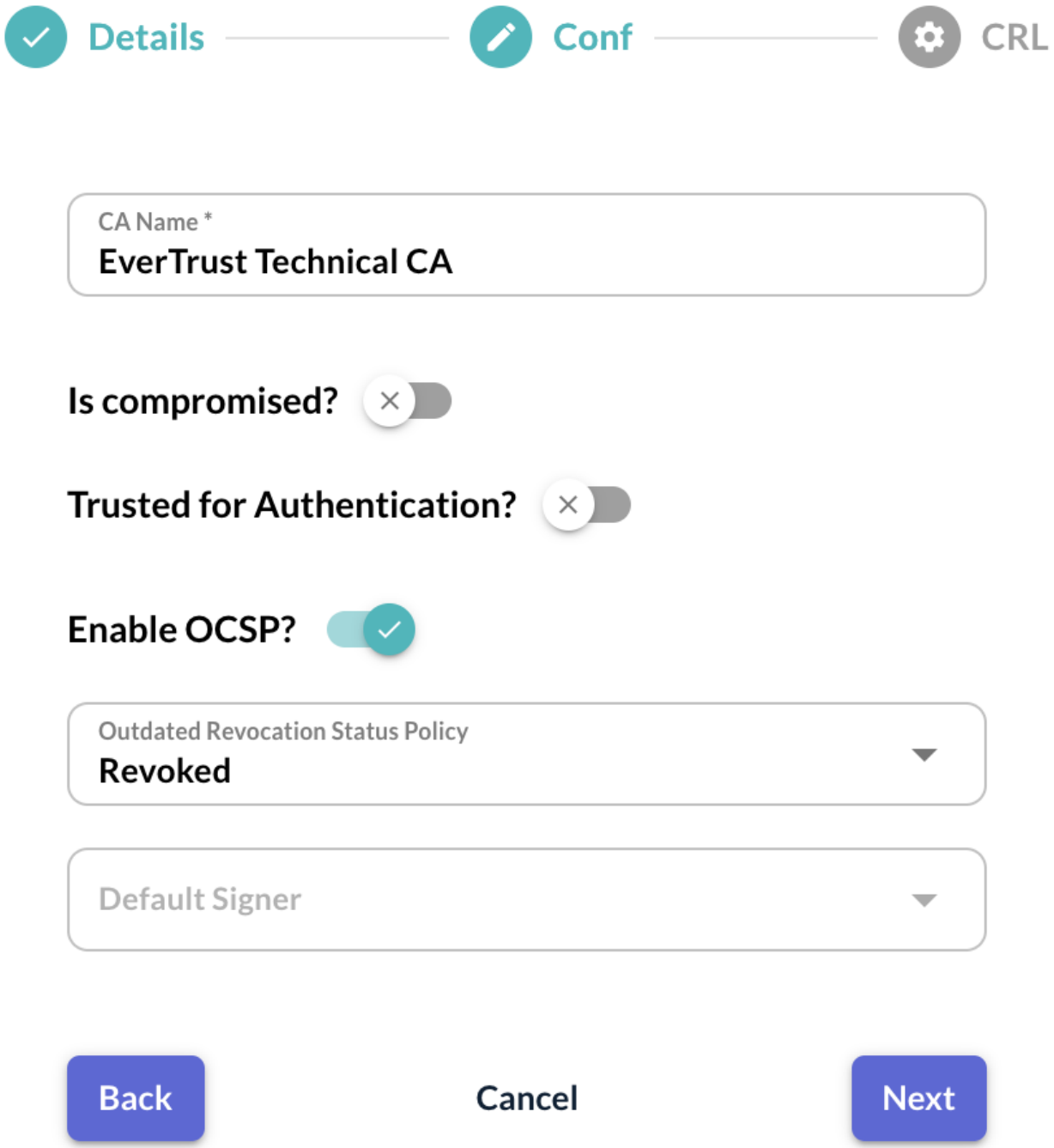
Step 5: The Certificate Authority is loaded and the details of the CA are displayed:



Step 6: Click on 'Next' and specify the following configuration information:

- '**Name**': This is the name of the Certificate Authority within OCSPd;
- '**Is compromised?**': If this parameter is checked, any OCSP request targeting tis Certificate Authority will trigger a '**revoked**' response and the revocation date will be set as the request date;
- '**Trusted for Authentication?**': If this parameter is checked, this Certification Authority is trusted for client certificate authentication on the OCSPd Web Management Console;
- '**Enable OCSP?**': This parameter indicates if OCSPd should serve OCSP responses for this particular Certificate Authority;

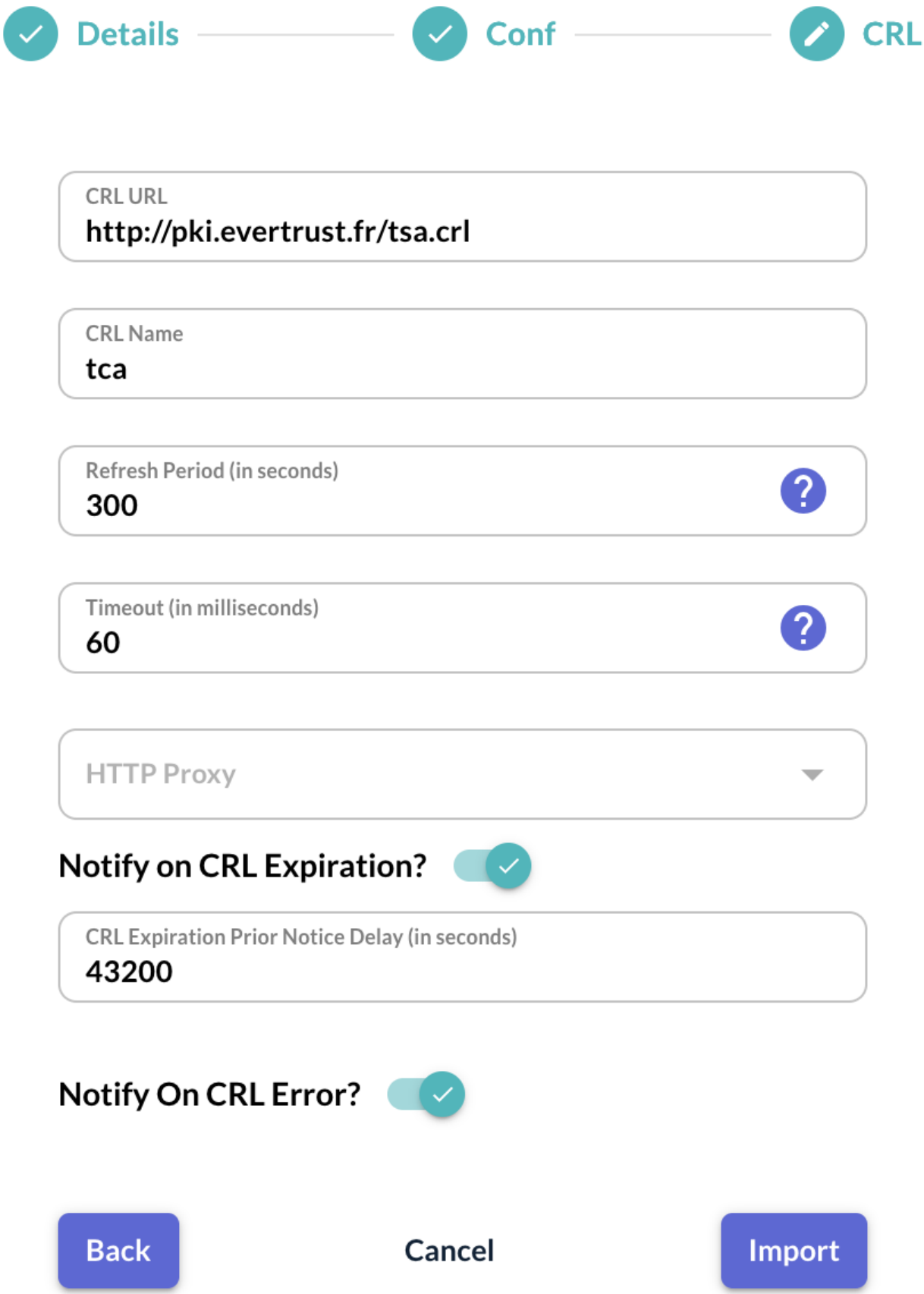
- '**Outdated Revocation Status Policy**': This defines the behavior of the OCSP responder when the revocation status is unavailable (CRL is expired or cannot be downloaded). OCSPd implements 3 policies:
  - '***Revoked***': any OCSP request will trigger a '**revoked** response (RFC 5019 compliant);
  - '***Unknown***': any OCSP request will trigger an '**unknown**' response;
  - '***Last available status***': the OCSP responder will determine the status based on the last information available (this policy is not compliant with the RFC 5019, but it allows avoiding denial of services when CRL is unavailable or expired);
- '**Default Signer**': This parameter indicates which signer should be used to sign the OCSP responses for this particular CA when the responder to use is not defined in the URL.



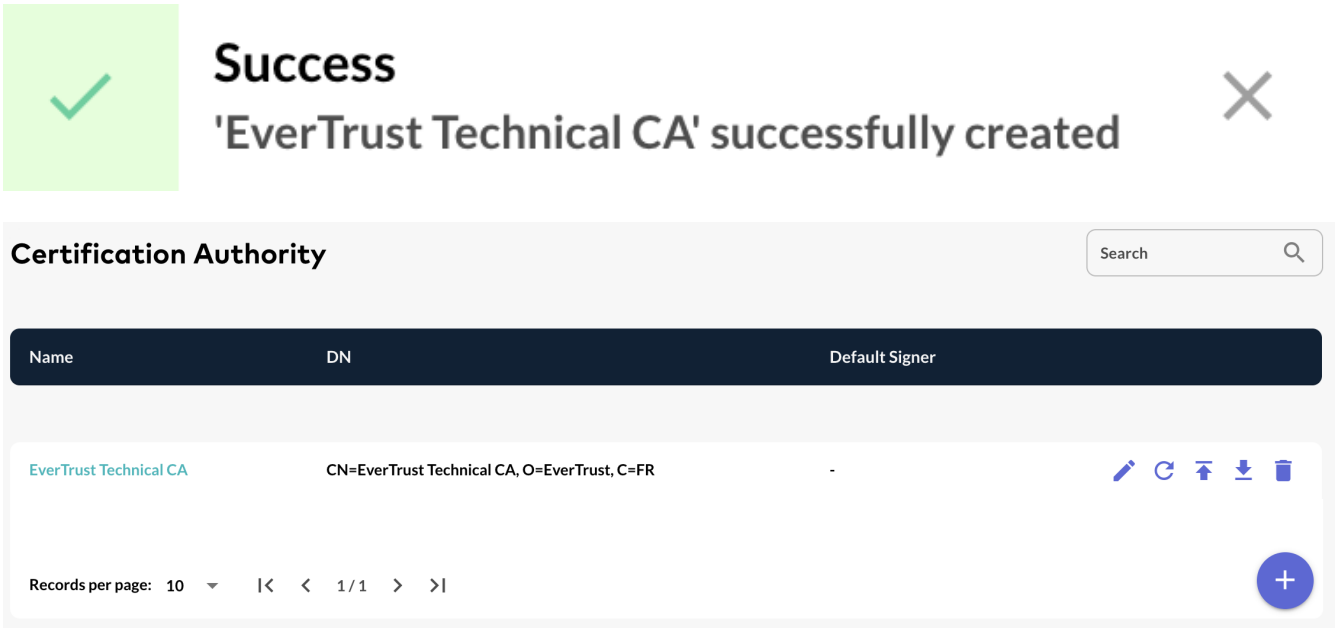
Step 7: Click on 'Next' and specify the following CRL configuration information:

- '**CRL URL**': This is the URL where the CRL can be downloaded from. OCSPd currently supports **HTTP and LDAP only**;
- '**CRL Name**': This parameter specifies how the CRL should be named when available through HTTP on the OCSPd component. For example, if the CRL name is configured as '**acsa**', then, the CRL will be available under http://[EverTrustOCSP IP or DNS NAME]/acsa.crl (DER format) and http://[EverTrustOCSP IP or DNS NAME]/acsa.pem (PEM format). If the CRL Name parameter is not defined, the CRL will be name after the CA Name;
- '**Refresh Period**': This parameter defines the CRL refresh period in seconds. For example, for a value of 300, OCSPd will attempt to download the CRL every 300 seconds, i.e. 5 minutes. **If this parameter is set to '0', the CRL will not be downloaded at all**;
- '**Timeout**': This parameter defines the CRL timeout in milliseconds. **If this parameter is set to '0', no timeout will be set**;
- '**Proxy**': This parameter defines the proxy to use to download the CRL. Proxies are declared in the '**Proxies**' page;
- '**Notify on CRL expiration?**': If this parameter is checked, an email will be sent to the Administrator when the CRL is expired;
- '**CRL Expiration Prior Notice Delay (in seconds)**': This parameter defines the CRL expiration delay prior to notify the Administrator. For example, for a value of 43200, OCSPd will send an email to the Administrator 12 hours before the expiration of this Certification Authority CRL and each time the CRL is refreshed (defined by '**Refresh Period**' parameter);
- '**Notify on CRL error?**': If this parameter is checked, an email will be sent to the Administrator when the CRL retrieving of this Certification Authority will fail and each time the CRL is refreshed (defined by '**Refresh Period**' parameter).

Step 8: Hit the '**Import**' button:



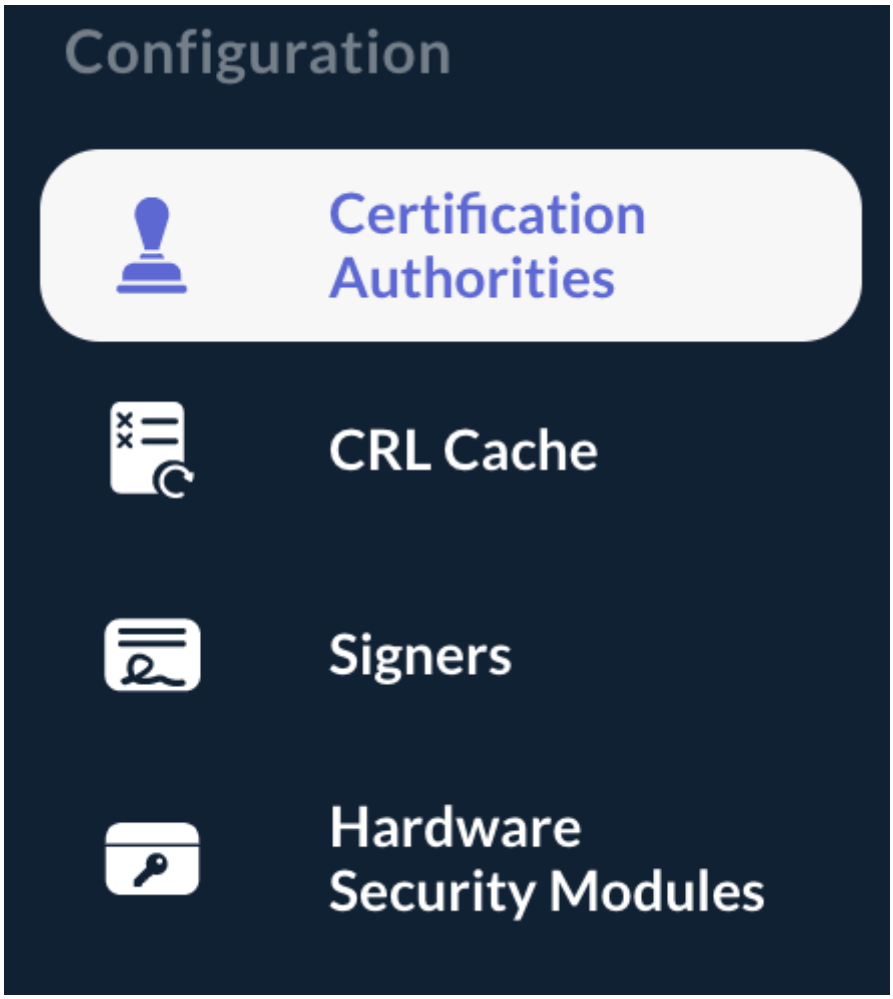
Step 9: The Certificate Authority is successfully imported:



2.8.2. Editing a Certificate Authority

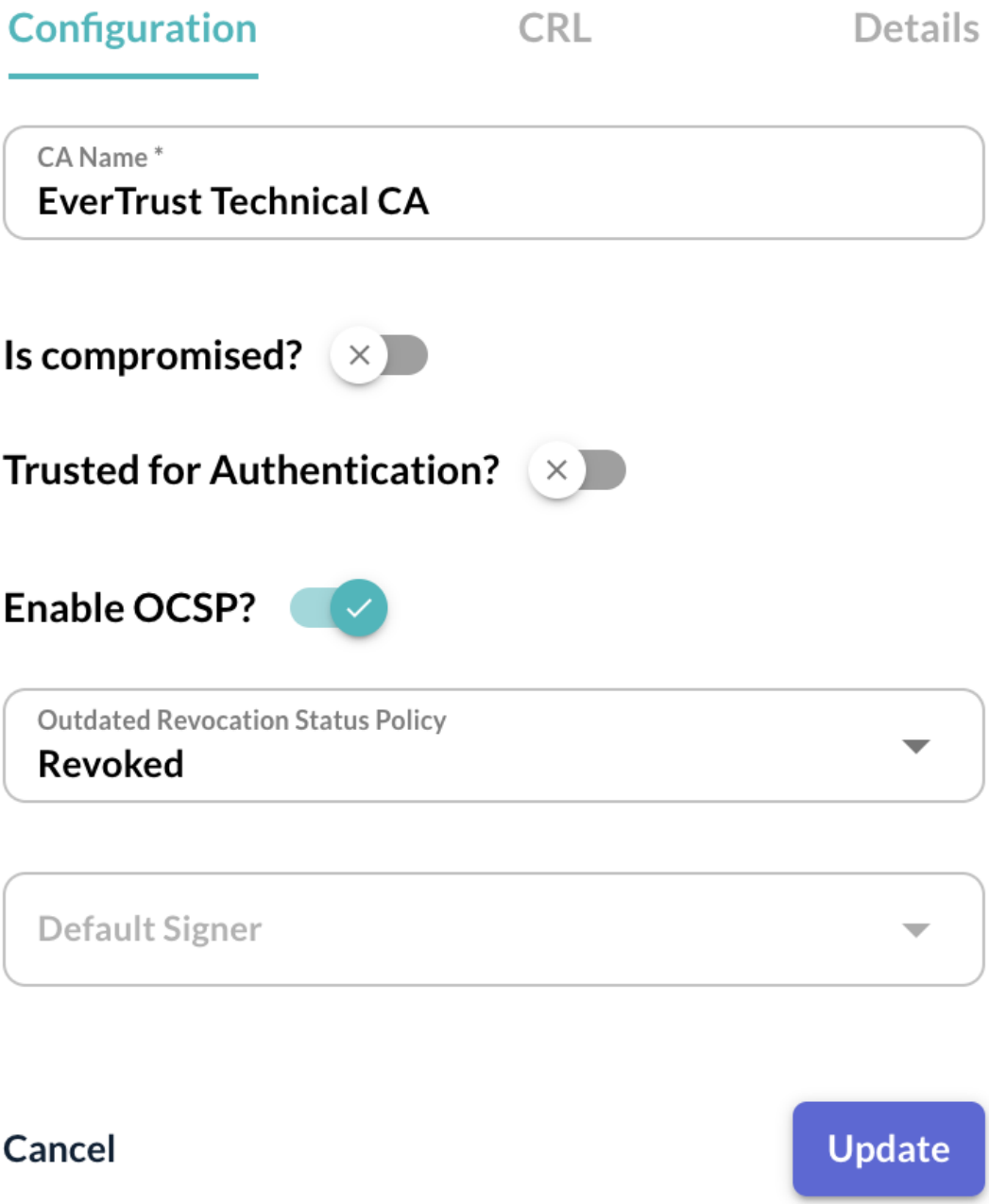
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':



Step 3: Click on the Certificate Authority's name you are willing to edit or hit the ✎ button:

Step 4: Update all the Certificate Authority attributes and hit the '**Update**' button:



Step 5: The Certificate Authority is successfully updated:

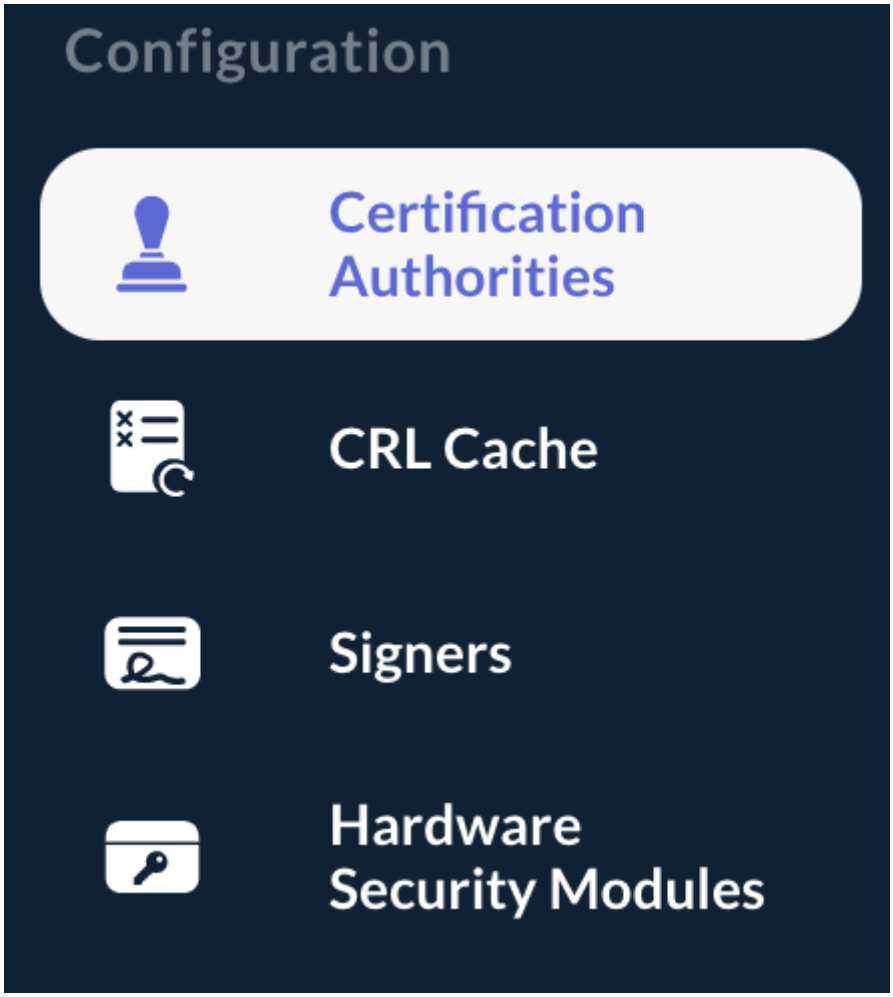
2.8.3. CRL management

Forcing a CRL Refresh

This option is available only if a 'CRL URL' has been set in the Certificate Authority configuration.

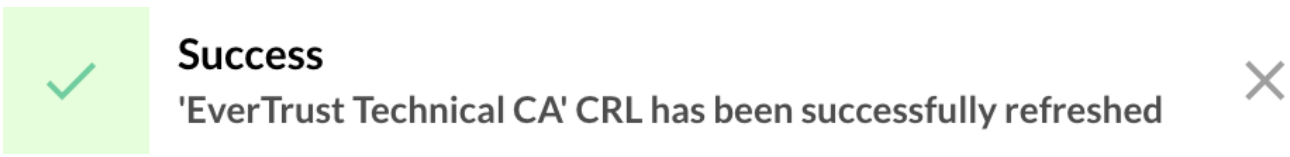
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':



Step 3: Hit the  button of the Certificate Authority you are willing to refresh the CRL:

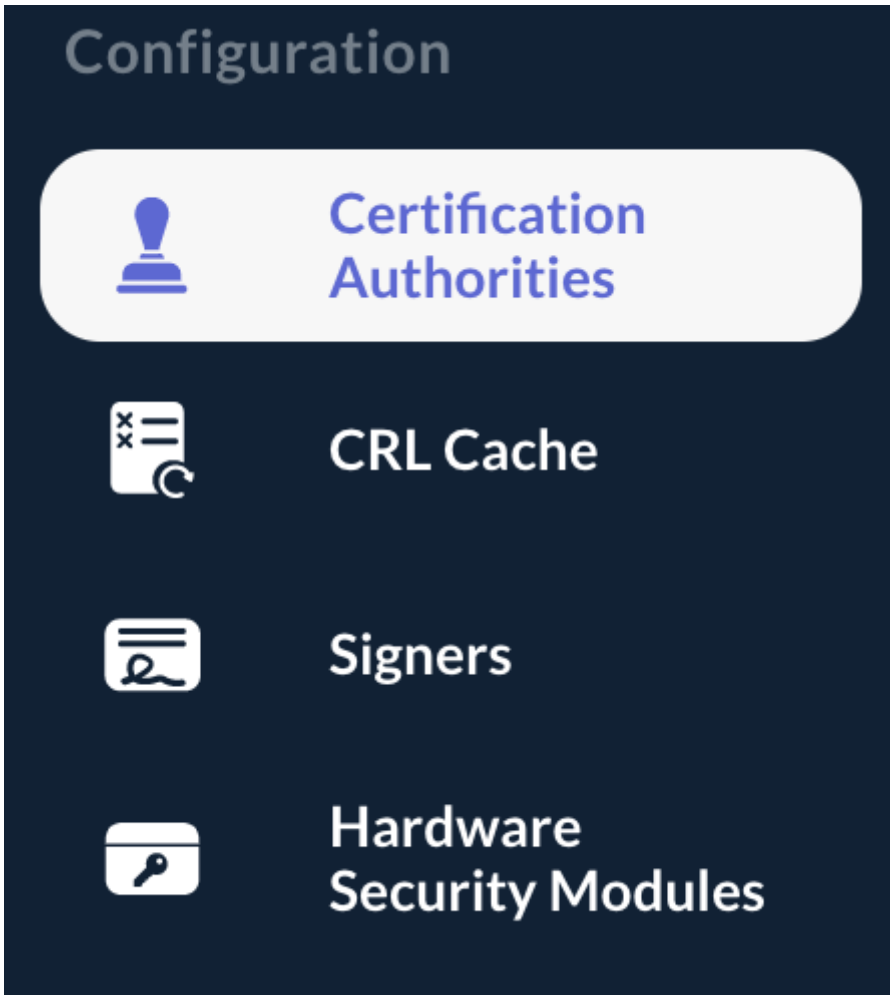
Step 4: The Certificate Authority CRL is successfully refreshed:



Uploading a CRL manually

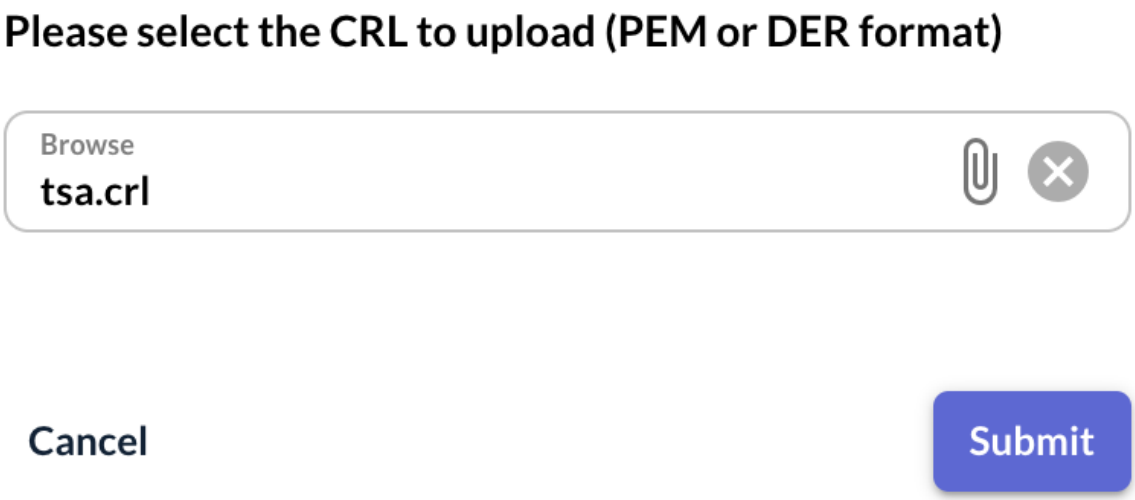
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':

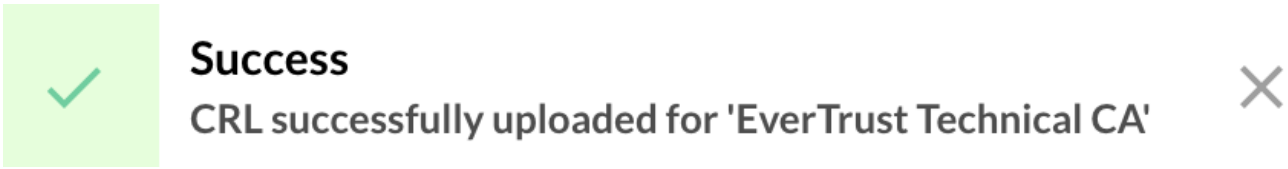


Step 3: Hit the ⤒ button of the Certificate Authority you are willing to upload a CRL:

Step 4: Browse for the CRL (PEM or DER) and hit the '**Submit**' button:



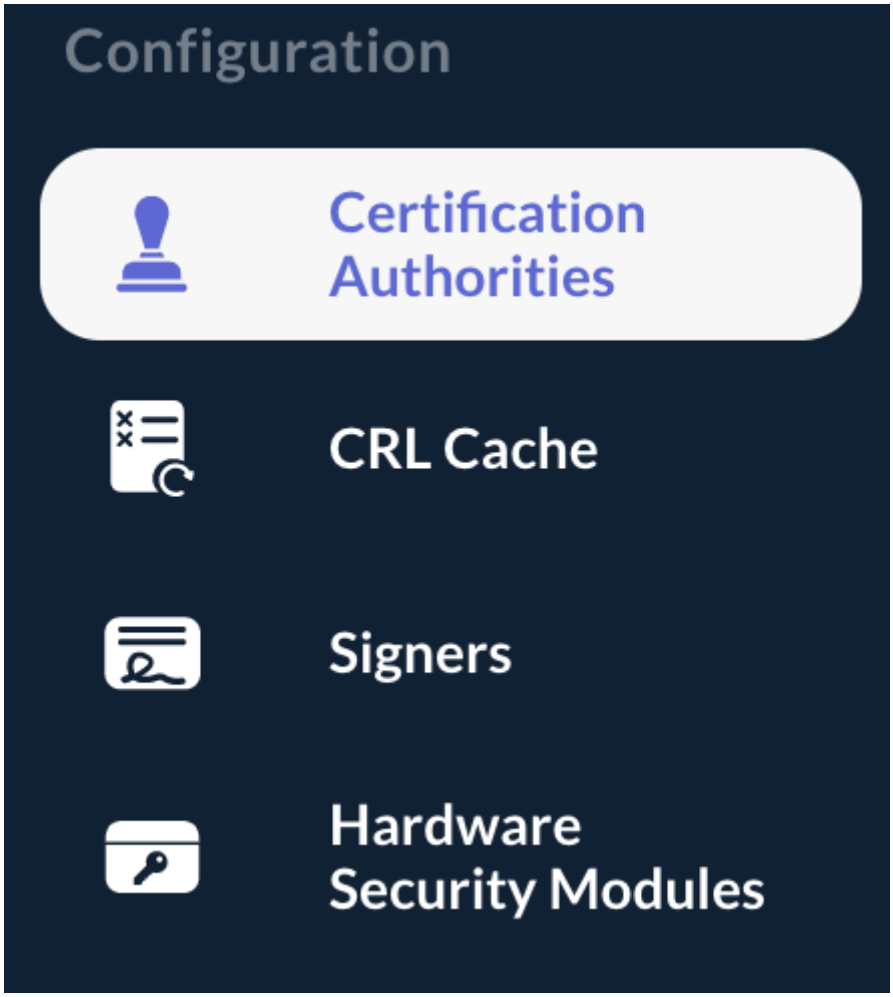
Step 5: The CRL is successfully uploaded:



2.8.4. Downloading the CA certificate

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':



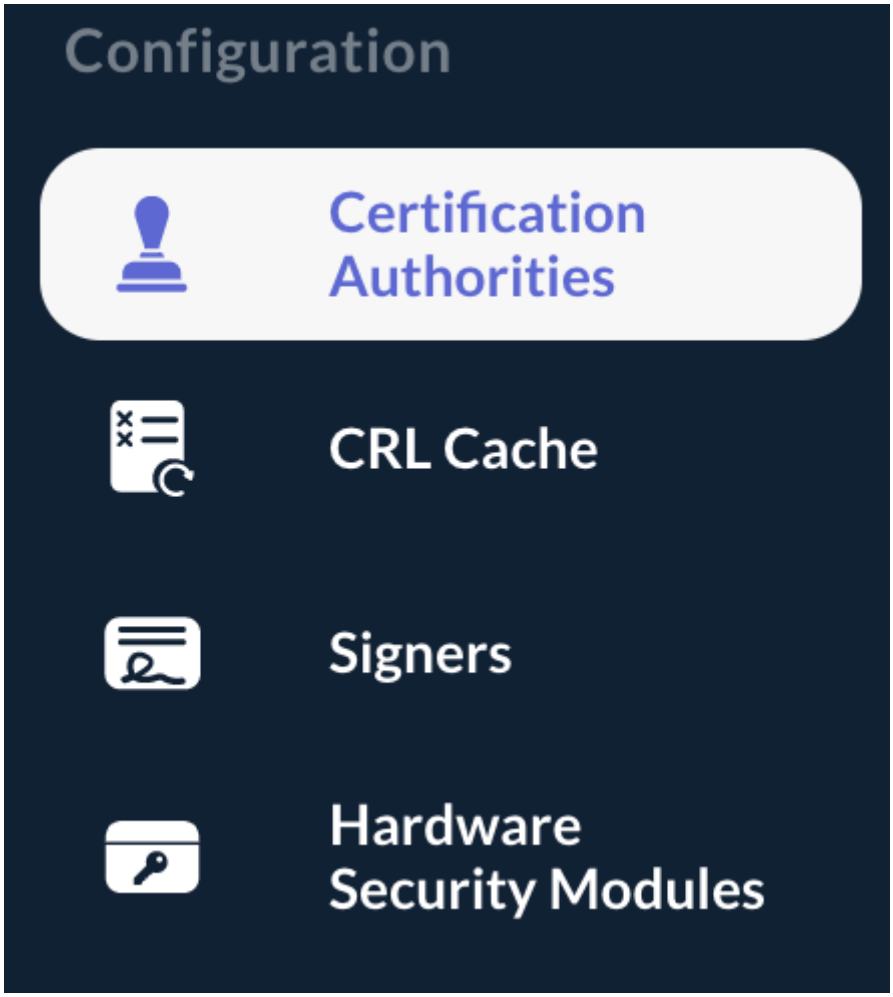
Step 3: Hit the button of the Certificate Authority you are willing to download the certificate (in PEM format):

Step 4: The Certificate Authority's certificate is downloaded in PEM format.

2.8.5. Deleting a Certificate Authority

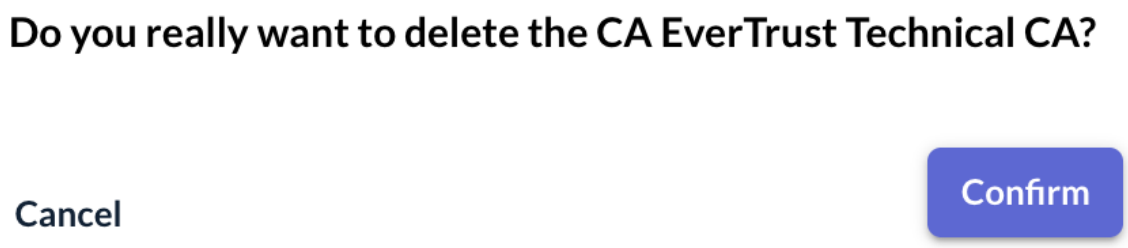
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Certificate Authorities**':

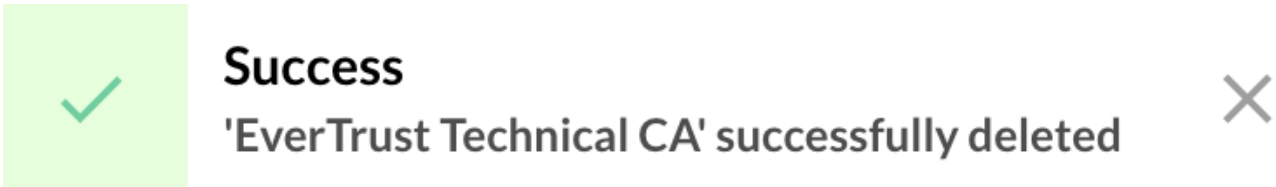


Step 3: Hit the button of the Certificate Authority you are willing to delete:

Step 4: Hit the '**Confirm**' button:

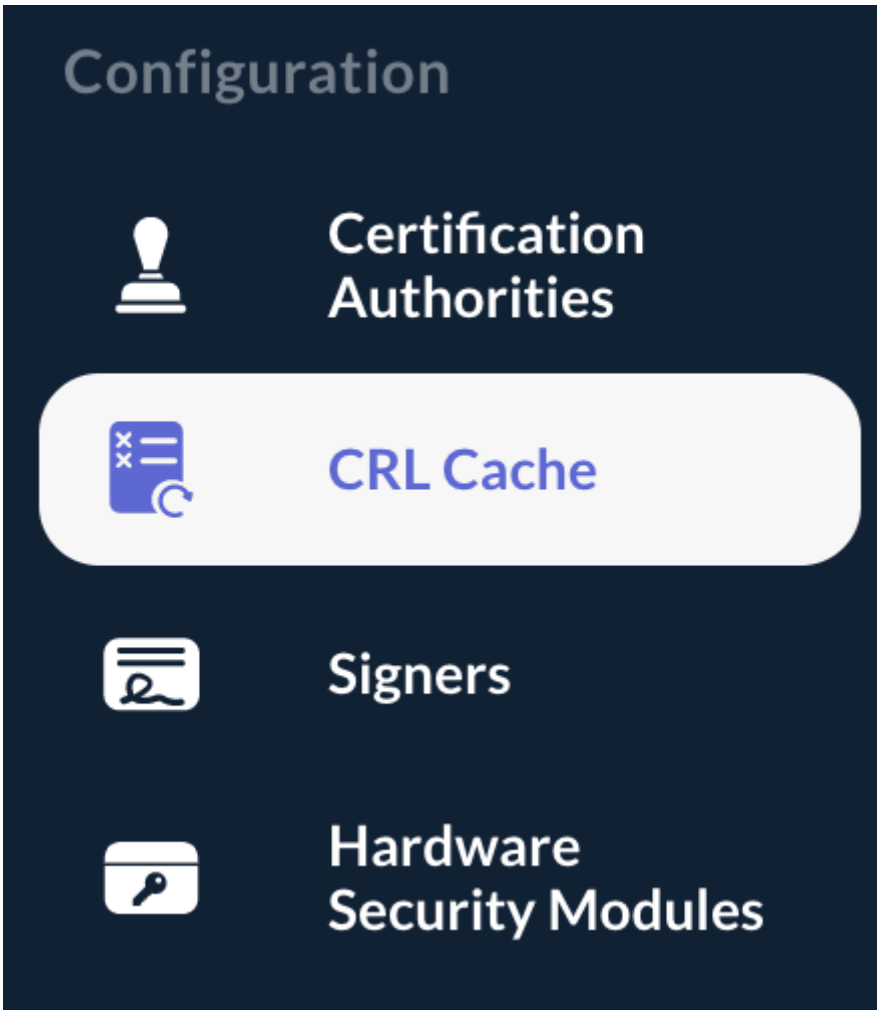


Step 5: The Certificate Authority is successfully deleted:



2.8.6. Understanding the Cache Management

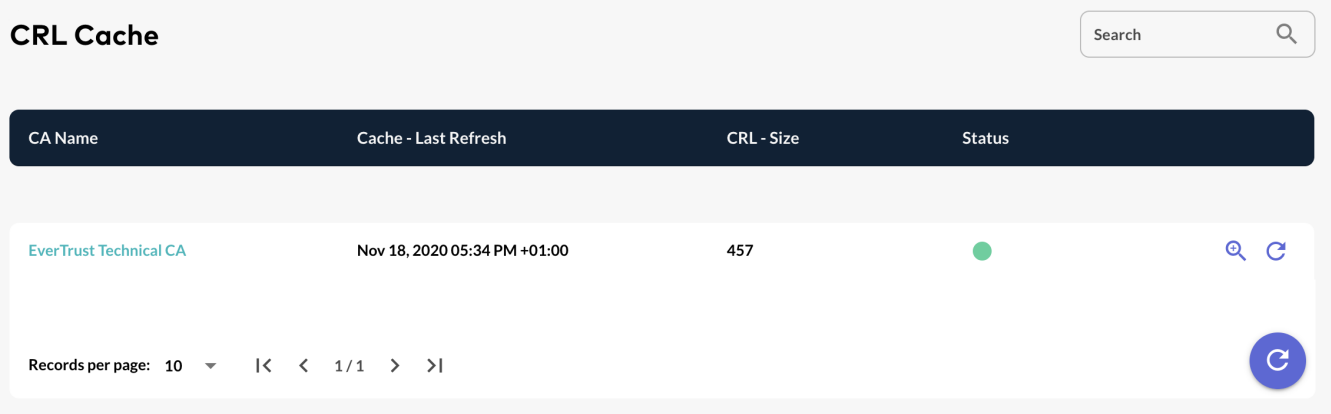
When CRL are downloaded, they are cached using an in-memory caching system (EHCache). The status of the cache is available in the '**CRL Cache**' entry of the '**Configuration**' left menu:



Basically, when a new CRL is downloaded or uploaded, the CRL is parsed and each revocation entry is inserted / updated in the cache. Addressing the cache being faster than querying the CRL object, it results in a great performance enhancement, particularly for big CRL.

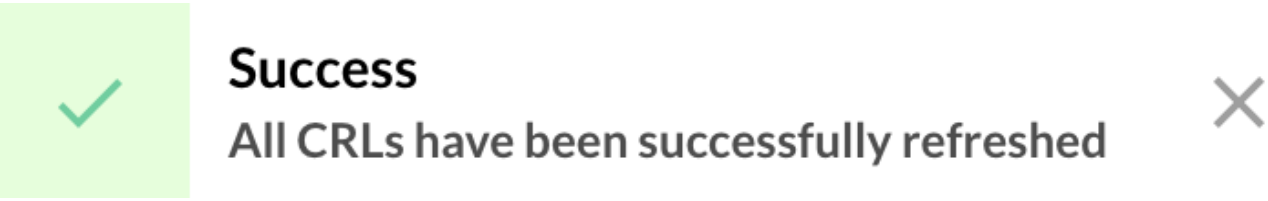
The cache status details for each Certificate Authority:

- The Certificate Authority Name ('**CA Name**');
- The last time of cache refresh for the CRL ('**Cache - Last Refresh**');
- The number of revoked entries in the cache for the considered Certificate Authority ('**CRL - Size**');
- The current cache status for the considered Certificate Authority: 'Valid', 'Warning', 'Expired', 'Error' ('**Status**').
- The following CRL info are available when mouseover the button:
  - The issuance date of the last downloaded CRL for the considered Certificate Authority;
  - The expiration date of the last downloaded CRL for the considered Certificate Authority.
  - The CRL serial number of the last downloaded CRL for the considered Certificate Authority.



You can retrieve information about the cache 'error' or 'warning' by hovering on the '**Status**'.

The cache status can be refreshed by hitting the '**Refresh**' button:



The cache cannot be purged. To purge the cache, restart the OCSPd service.

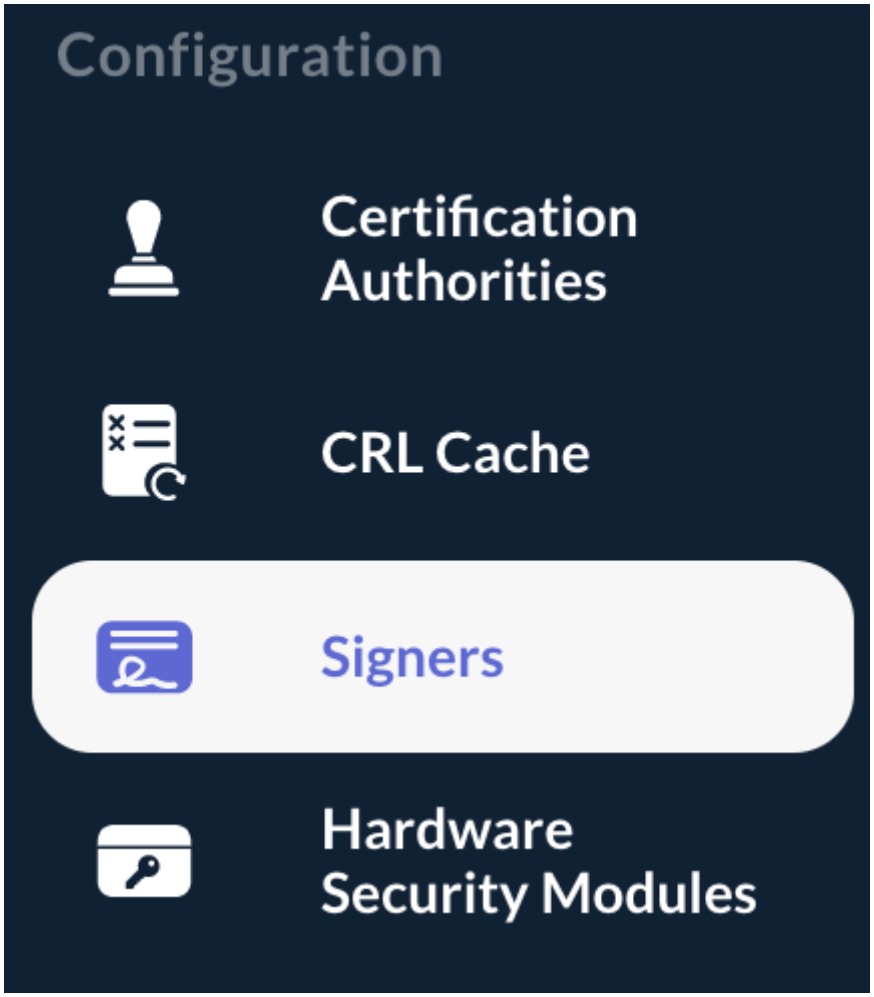
The number of cache entries in the cache does not reflect the number of entries in the CRL. Expired entries will be removed from the CRL, but not from the cache. Therefore, the cache contains at least as many entries as in the CRL, but can contain more. It contains all the revoked entries parsed in the different CRL since the OCSPd service was started.

2.9. Managing OCSP Signers

2.9.1. Creating a Signer

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':

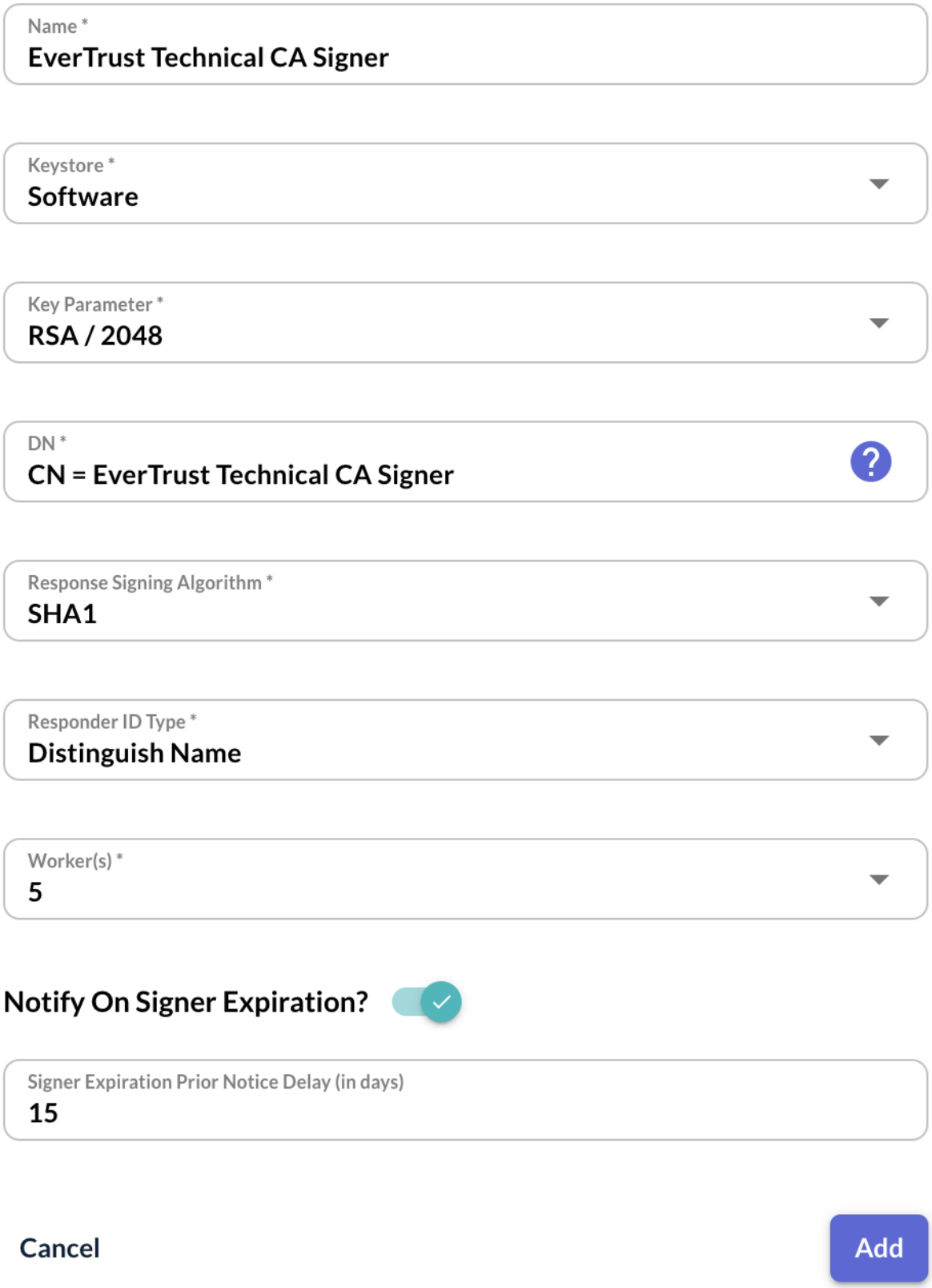


Step 3: In the Signers page, hit the '+' button at the bottom of the page:

Step 4: Specify:

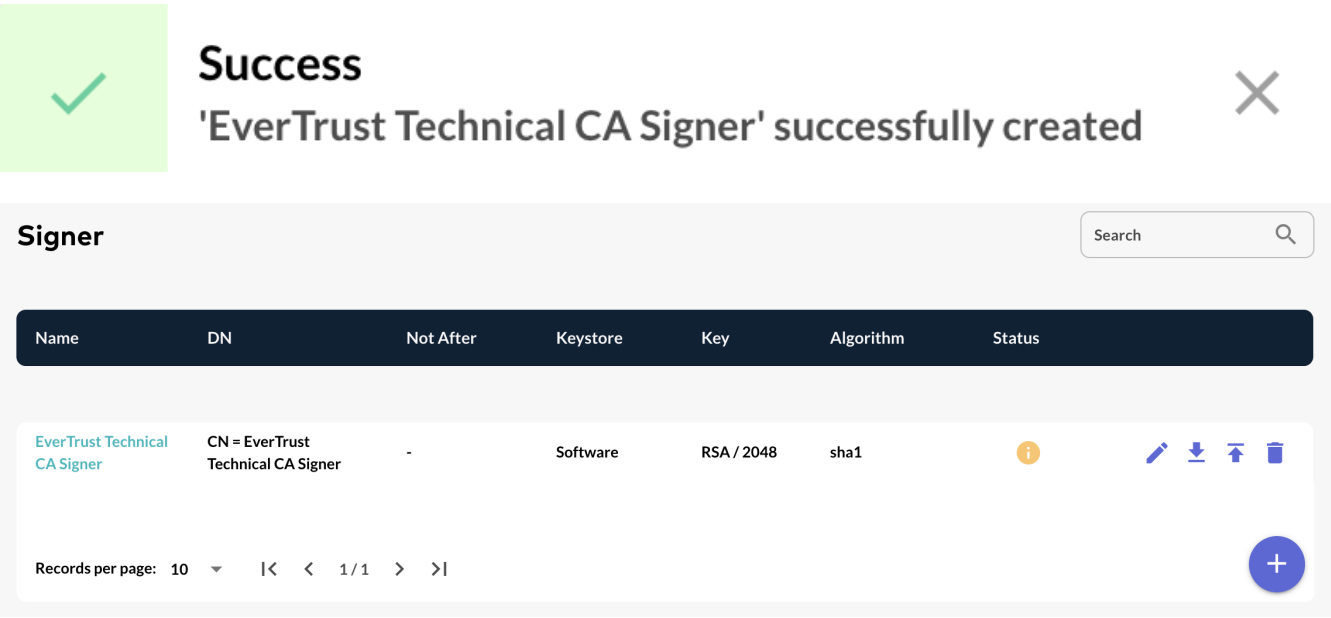
- '**Name**': the name of the Signer;
- '**KeyStore**': the keystore for the Signer Private Key. It can be:
  - '***Software***': the private key is stored in the OCSPd database;
  - '***Hardware***': the private key is stored in any defined HSM Slot;
- '**Key Parameter**': the type and size of the keypair (RSA and ECDSA are supported);
- '**DN**': the Distinguished Name of the Signer certificate.

And hit the '**Add**' button:



The other attributes are irrelevant until the Signer certificate is issued and installed.

Step 5: The Signer is successfully created:

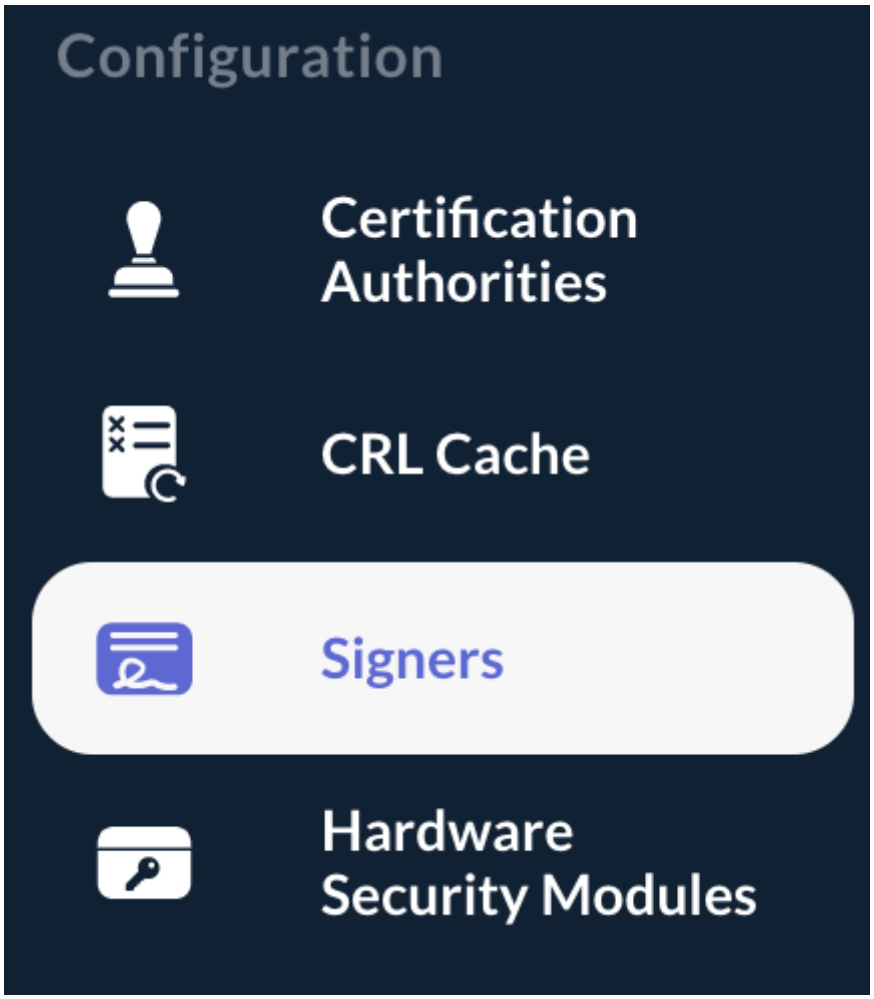


2.9.2. Managing Signer Certificate Requests

Editing a Signer prior Certificate Request

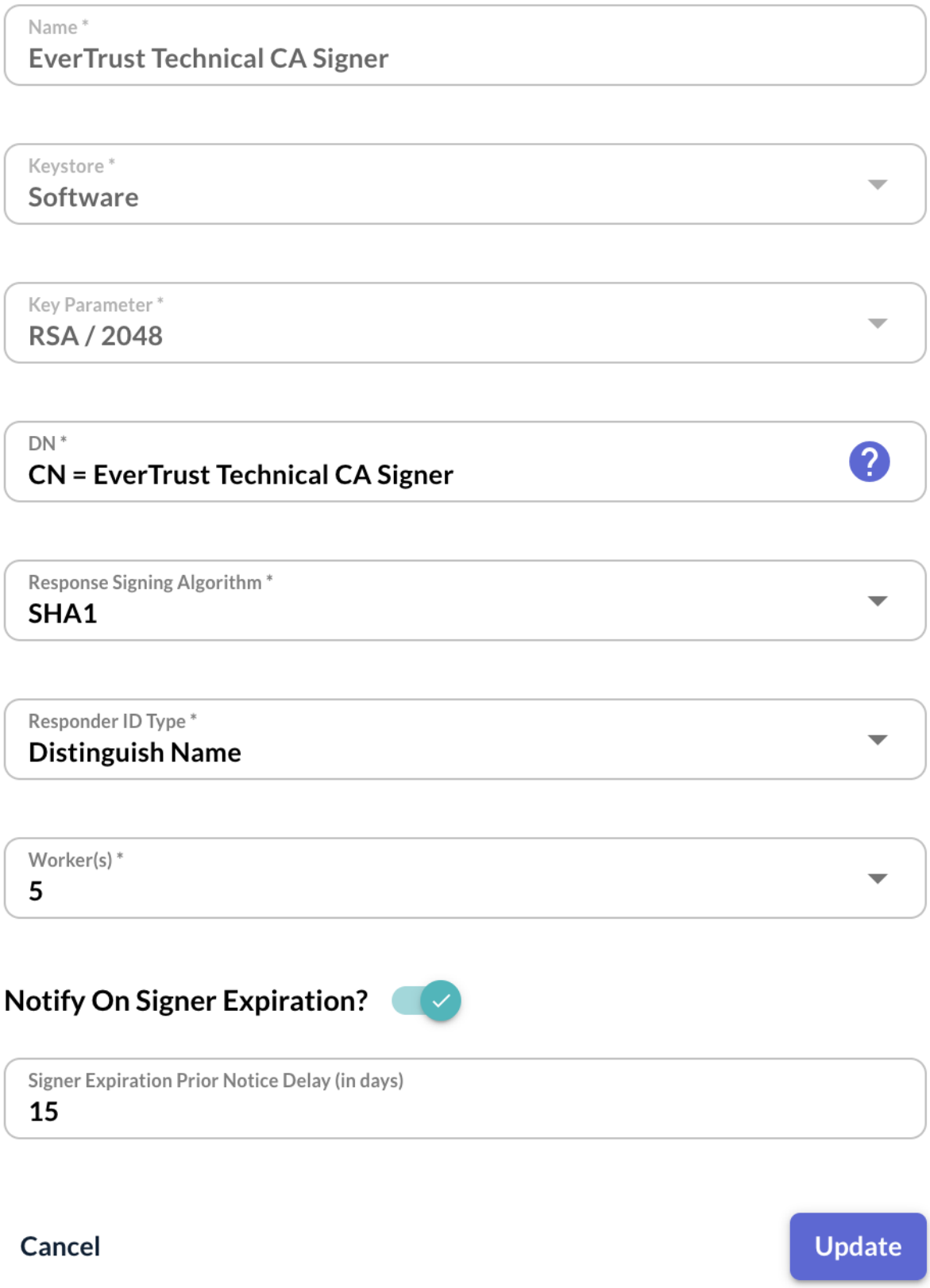
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Click on the Signer's name you are willing to edit or hit the ✎ button:

Step 4: Modify the Signer Distinguish Name and hit the '**Update**' button:

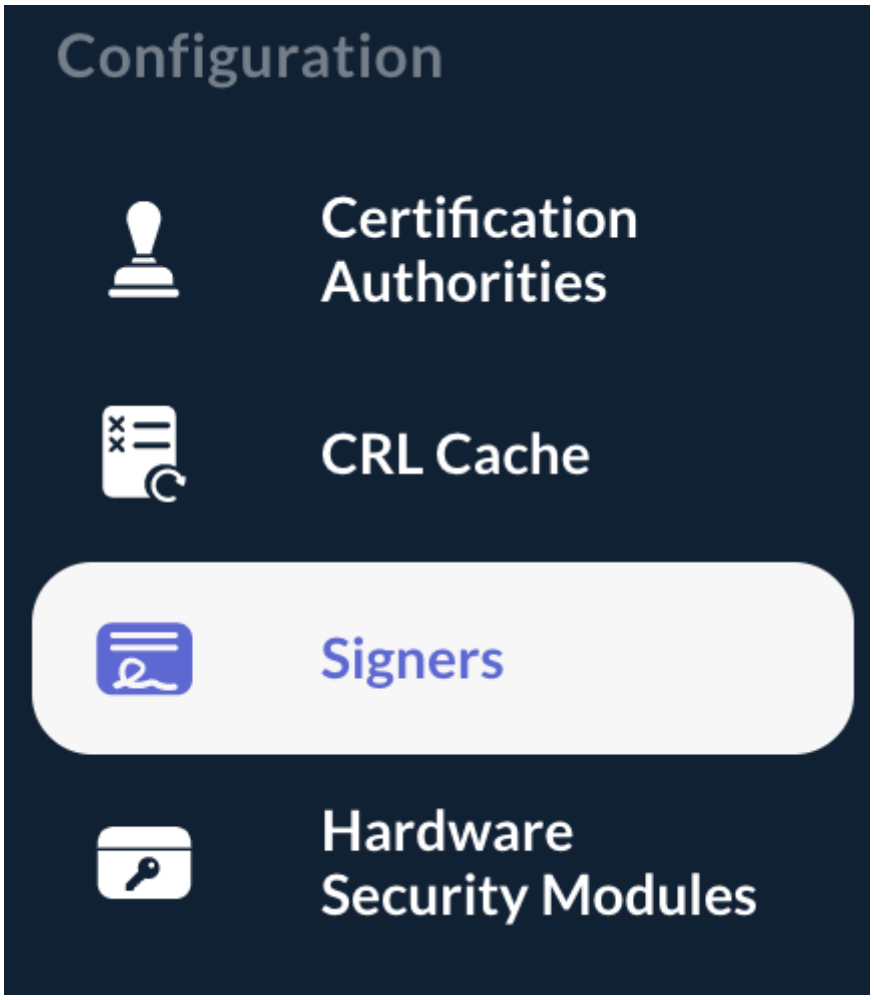


Step 5: The Signer is successfully updated:

Generating a Signer Certificate Request

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the ⬇ button of the Signer you are willing to generate a Certificate Request (PKCS#10):

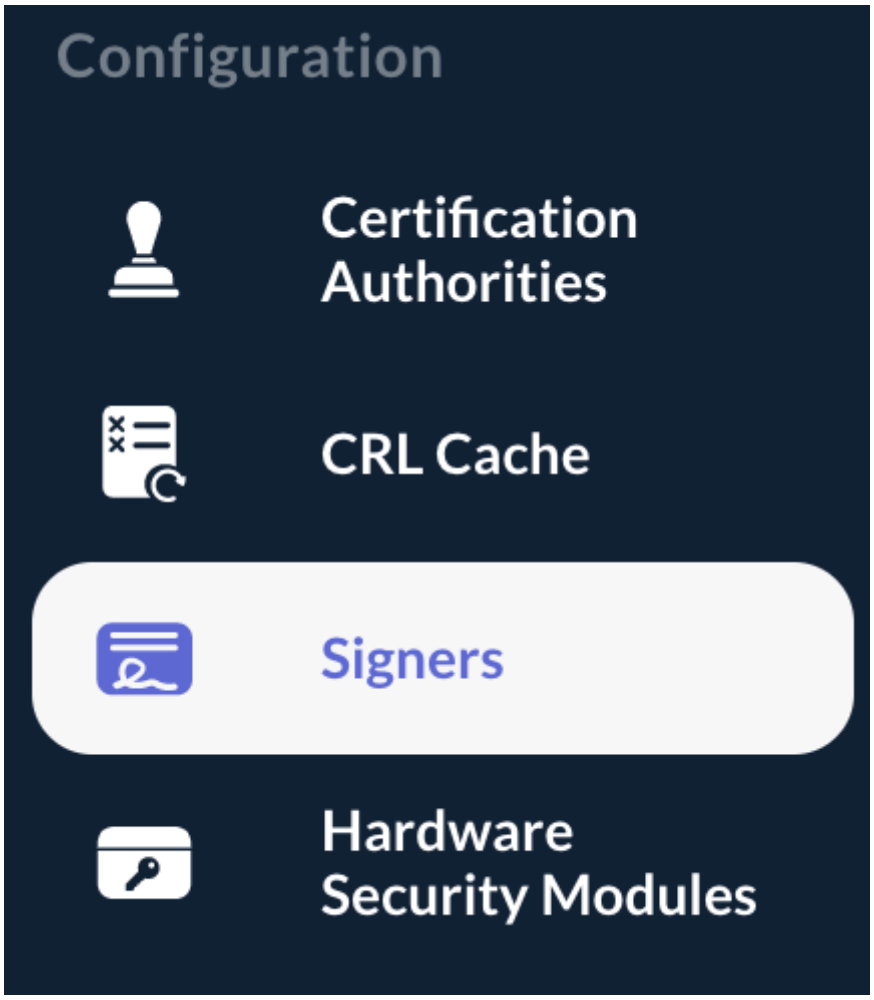
Step 4: The PKCS#10 certificate is generated.

The request needs to be signed using your corporate PKI.

Installing a Signer Certificate

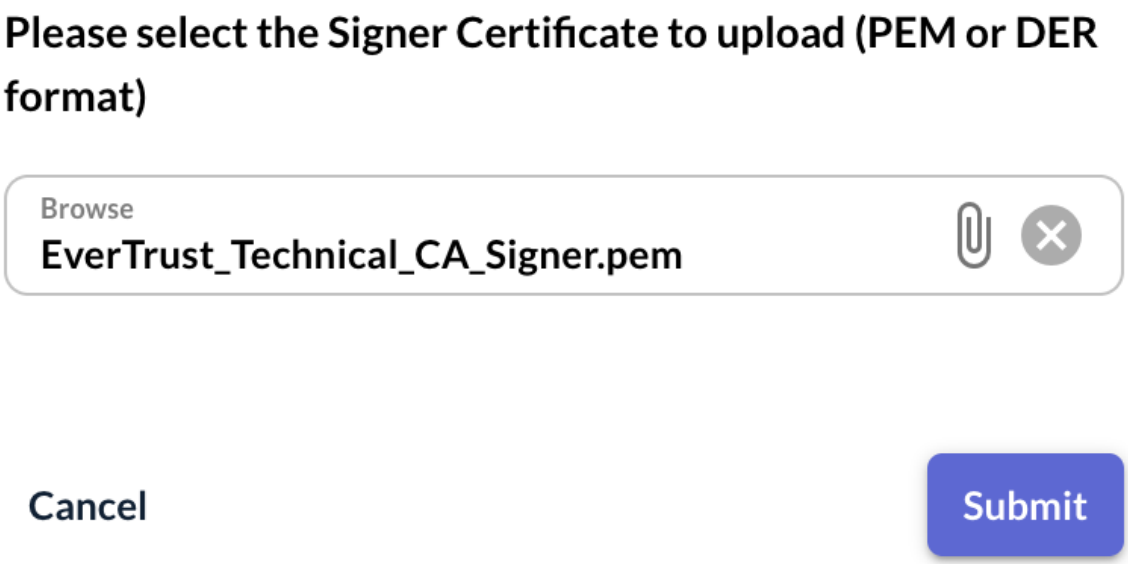
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the ⬆ button of the Signer you are willing to install the certificate for:

Step 4: Browse for the Signer certificate (PEM or DER) and hit the '**Submit**' button:



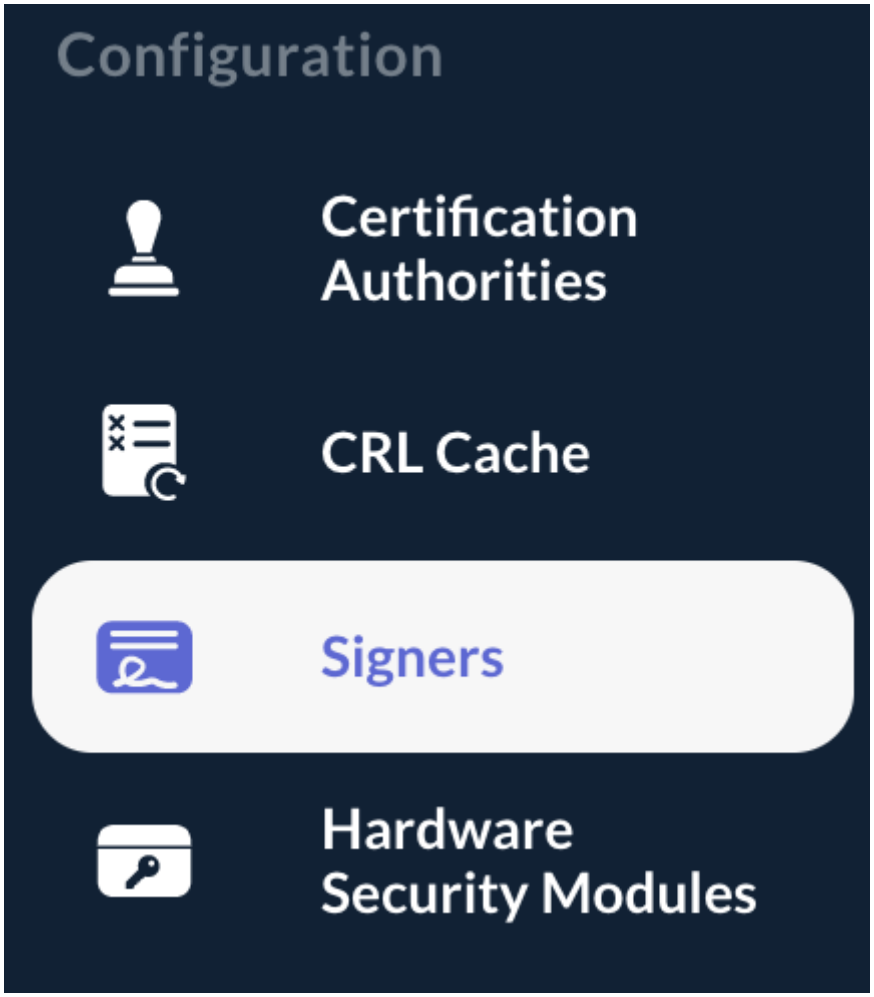
Step 5: The Signer certificate is successfully installed:

2.9.3. Managing Signers

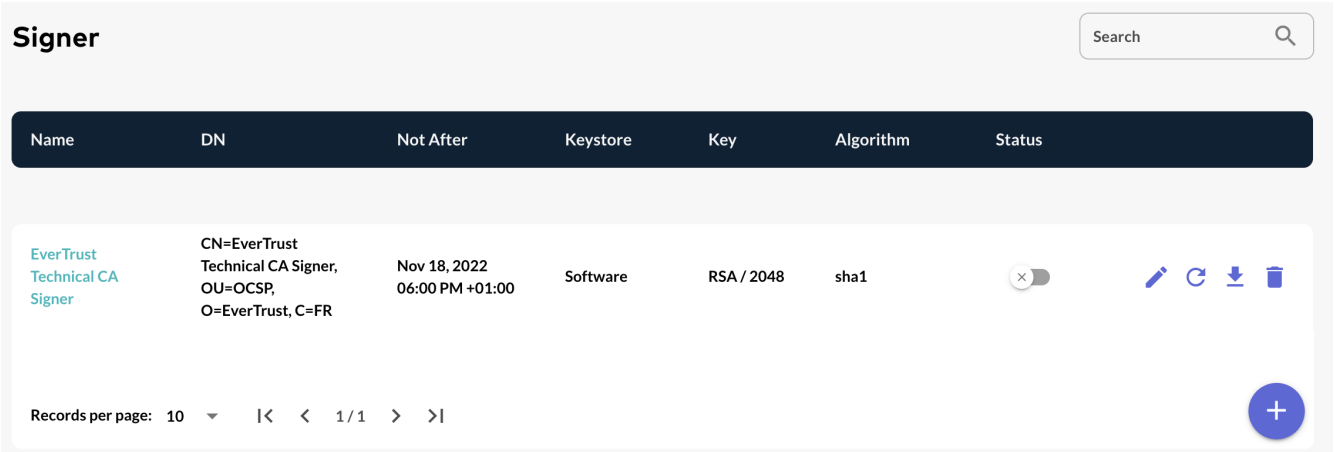
Editing a Signer

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Select the Signer you are willing to edit or hit the ✎ button:



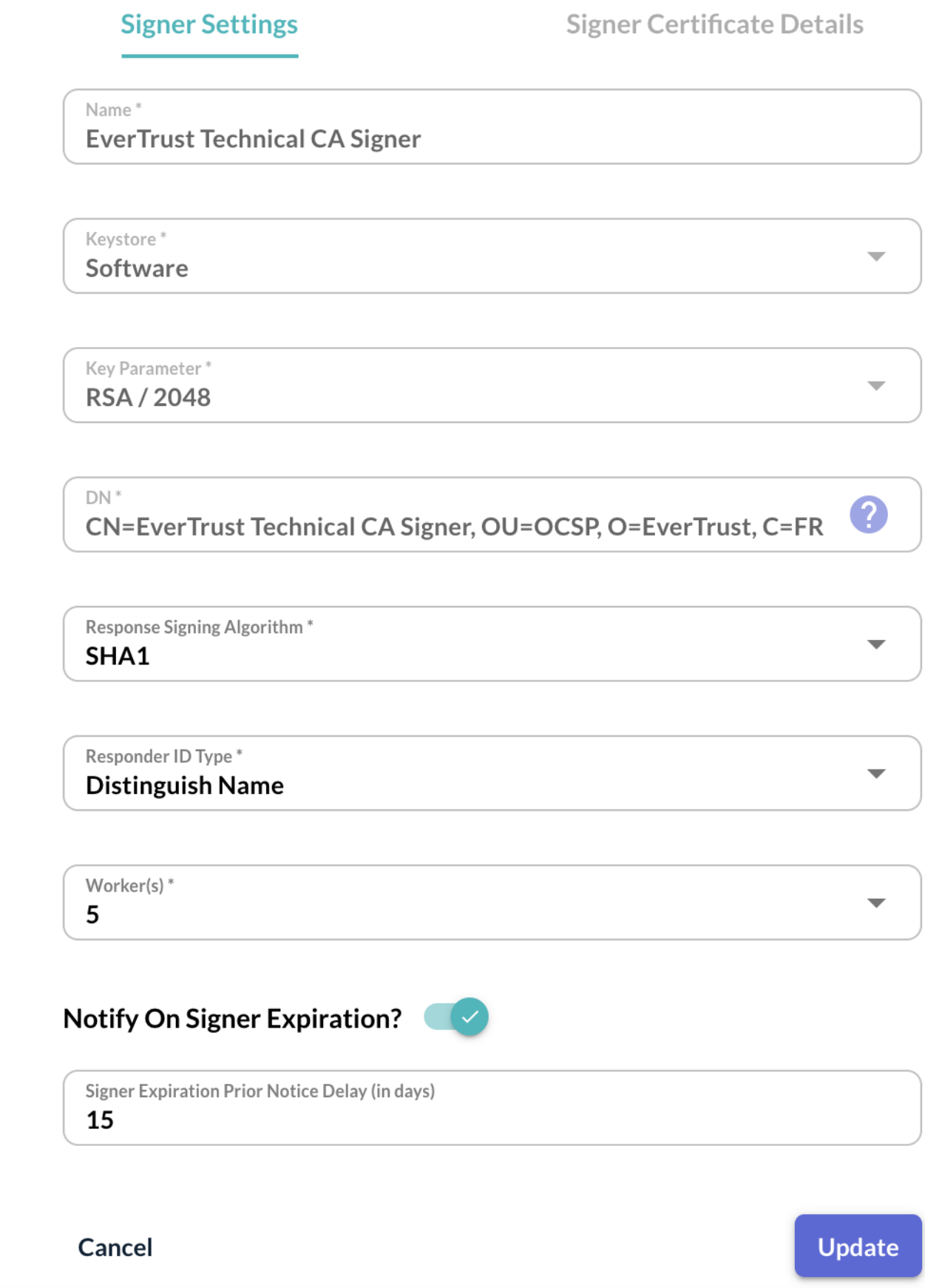
Step 4: Modify the following attributes:

- '**Response Signing Algorithm**': this attribute defines the signing algorithm used by the signer to sign the OCSP responses (SHA1, SHA2 and SHA3 hash algorithms are supported);
- '**Responder ID Type**': this attribute defines the format of the Responder ID included in the OCSP response (Certificate ID or Certificate DN);
- '**Worker(s)**': the number of concurrent signing for the signer (by default, the maximum number of workers is set to 5 but this can be tweaked in the configuration);
- '**Notify on signer expiration**': if this attribute is checked, an email will be sent to the

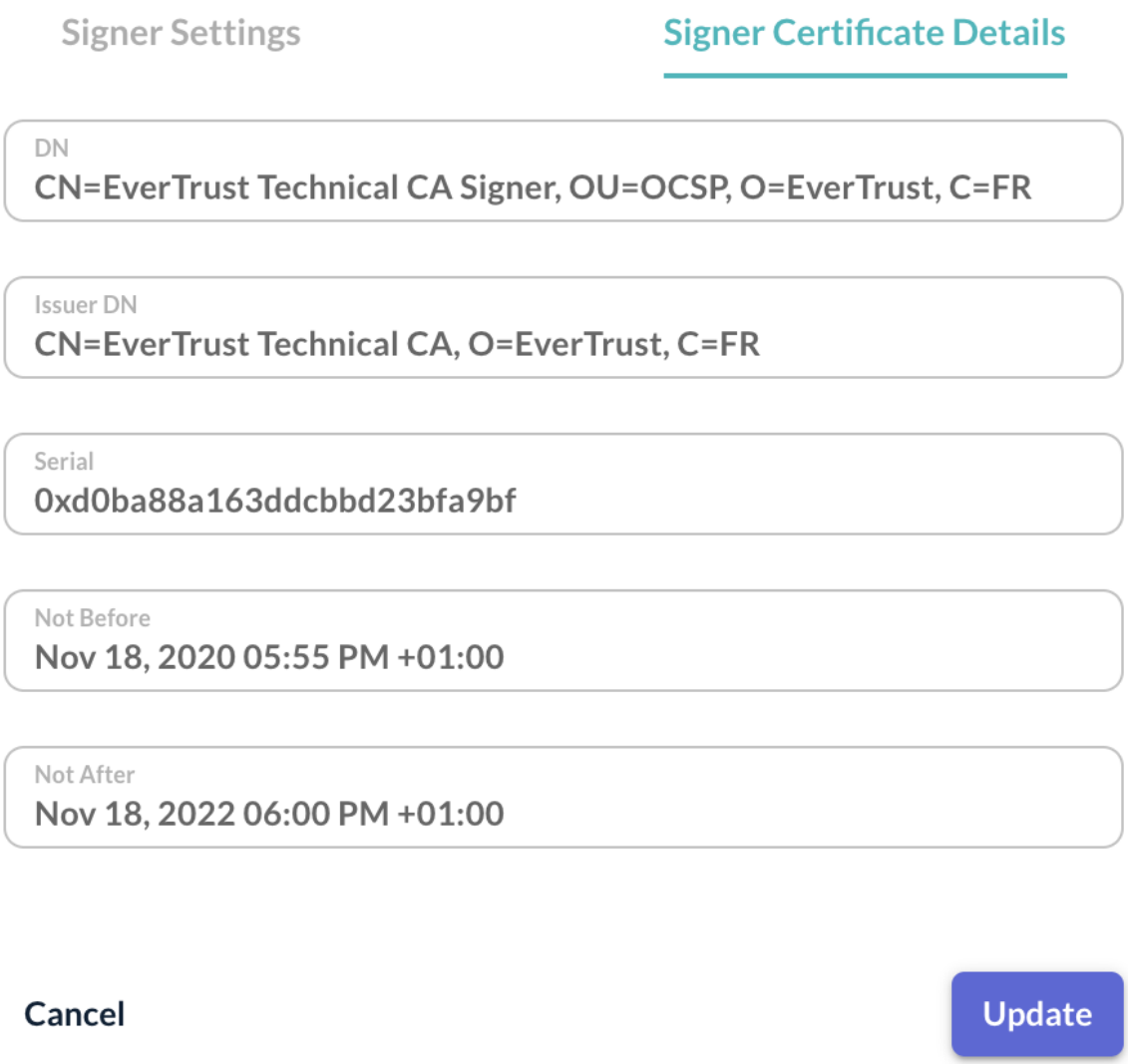
Administrator when the certificate of this Signer is expired. This notification is sent daily at 00:00;

- '**Signer Expiration Prior Notice Delay (in days)**': this attribute defines how many days before this signer certificate expires an email should be sent to the administrator.

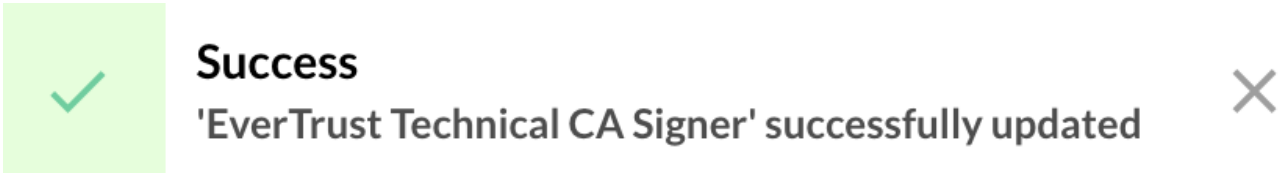
And hit the '**Update**' button:



Signer's certificate information is available under the tab named '**Signer Certificate Details**':



Step 5: The Signer is successfully updated:

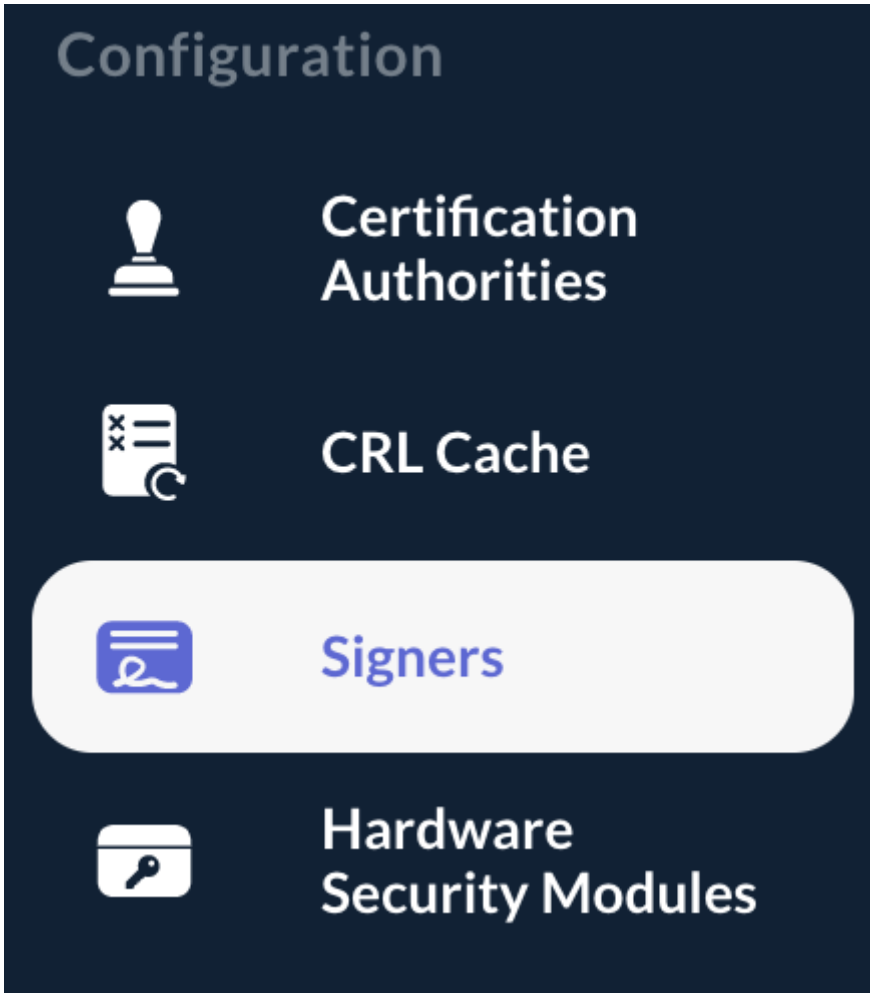


Deleting a Signer

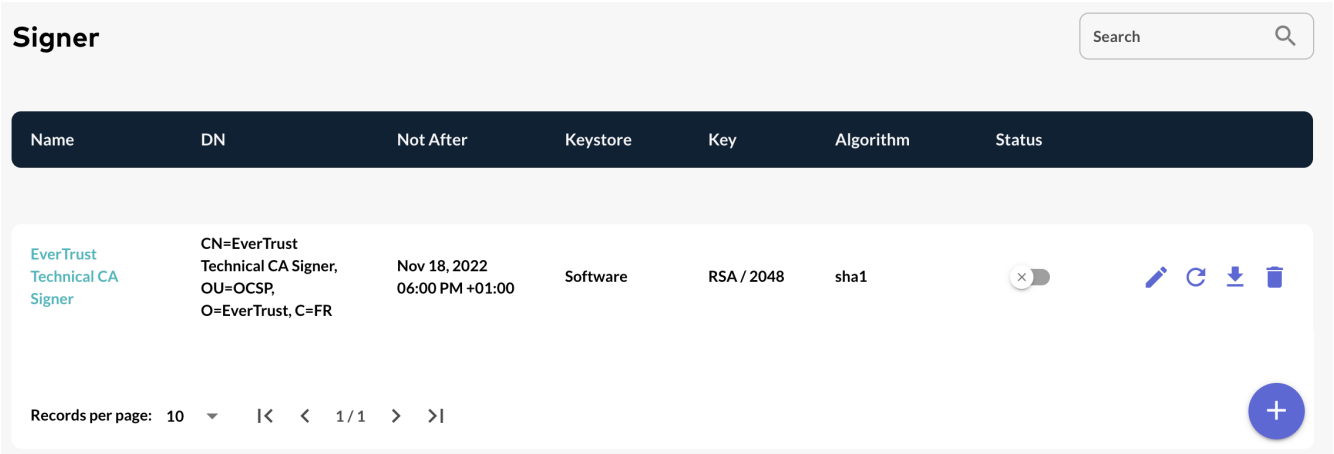
A Signer cannot be deleted if it is enabled. You **MUST** disable it prior to be able to delete it.

Step 1: Access the OCSPd Web Management Console;

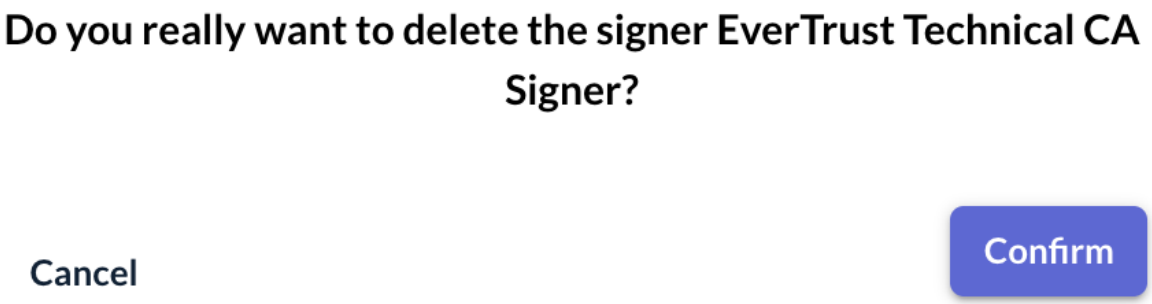
Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the button of the Signer you are willing to delete:



Step 4: Hit the '**Confirm**' button:

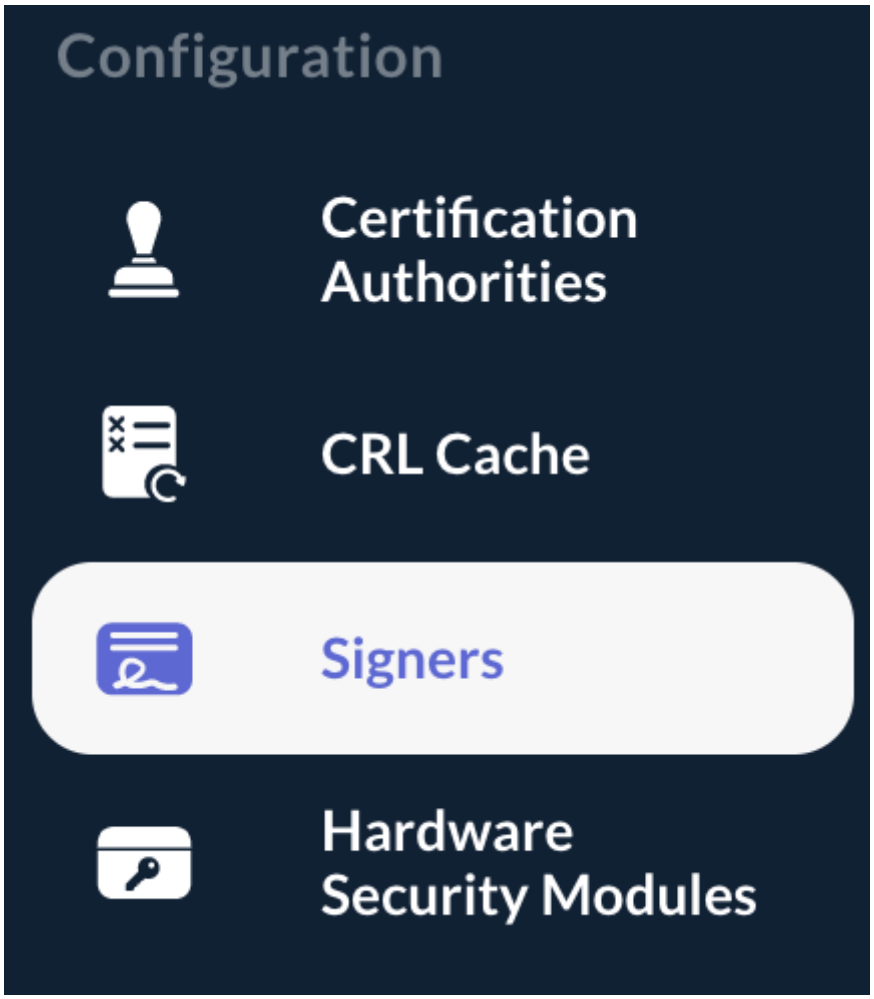


Step 5: The Signer is successfully deleted:

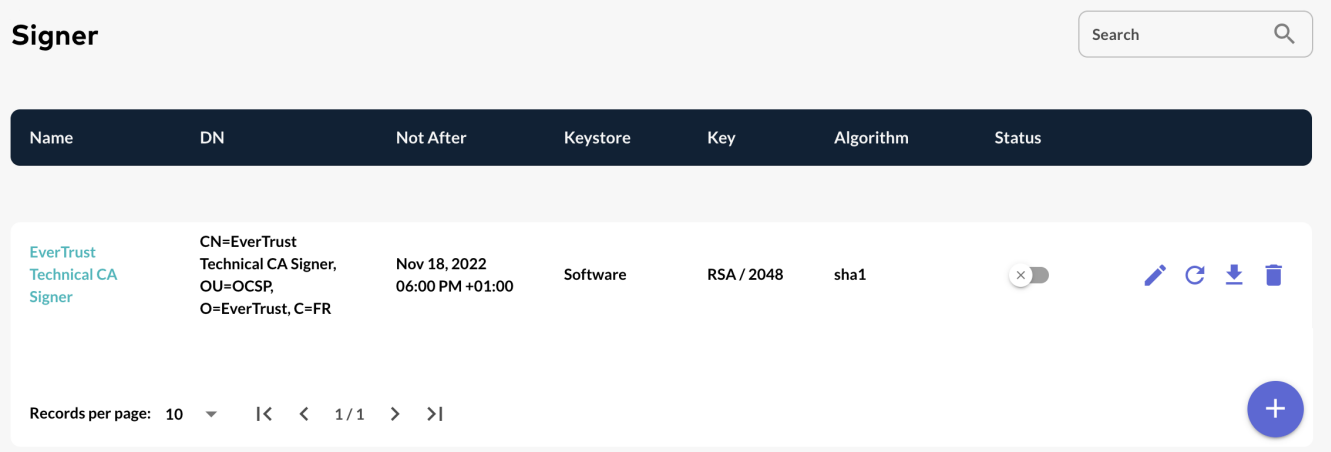
2.9.4. Downloading a Signer Certificate

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the ⬇ button of the Signer you are willing to download the certificate:



Step 4: The Signer certificate is downloaded in **PEM format**.

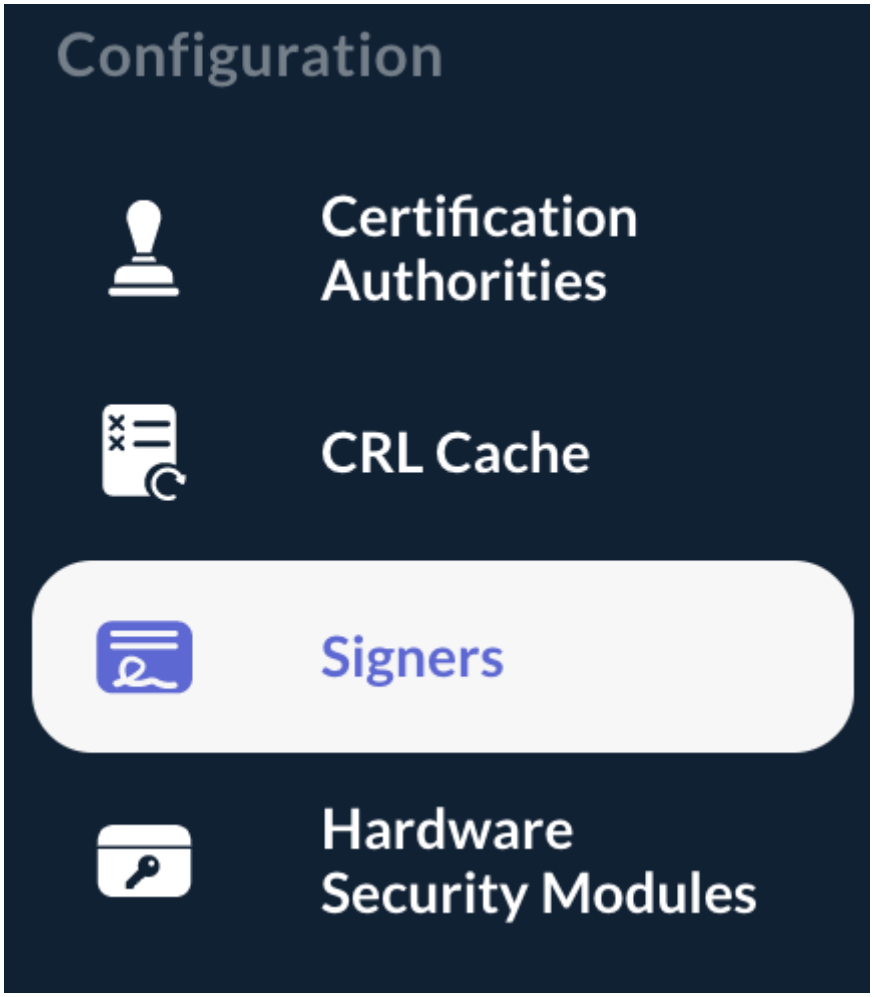
2.9.5. Enabling or Disabling Signers

Enabling a Signer

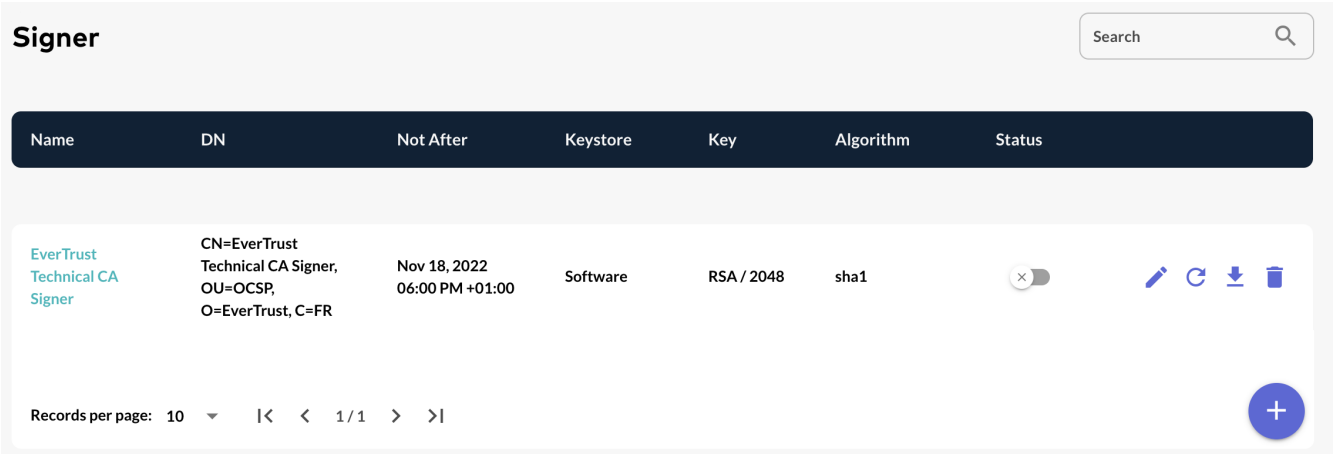
ℹ A signer cannot be consumed until it is enabled.

Step 1: Access the OCSPd Web Management Console;

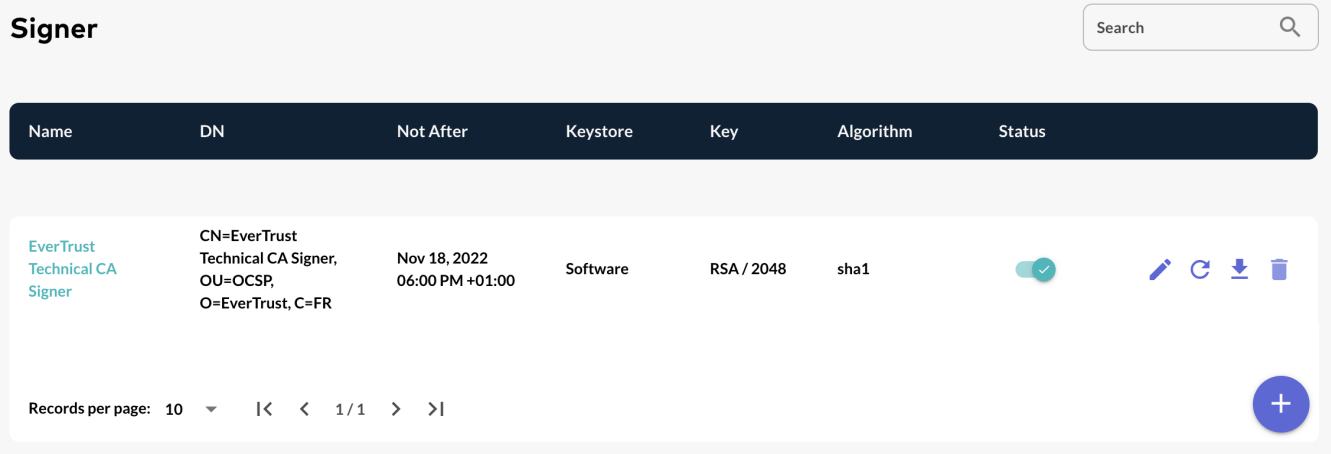
Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the button of the Signer you are willing to enable:



Step 4: The Signer is successfully enabled:



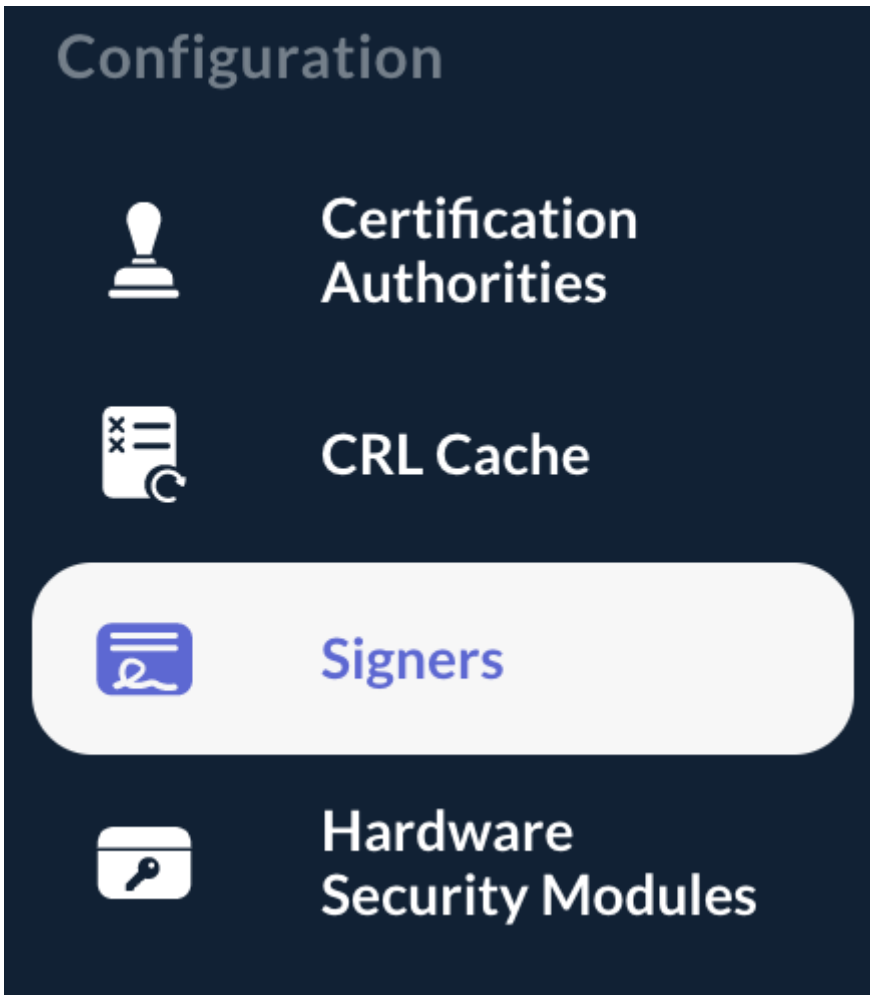
The Signer can now be set as a default Signer in the Certificate Authority configurations.

Disabling a Signer

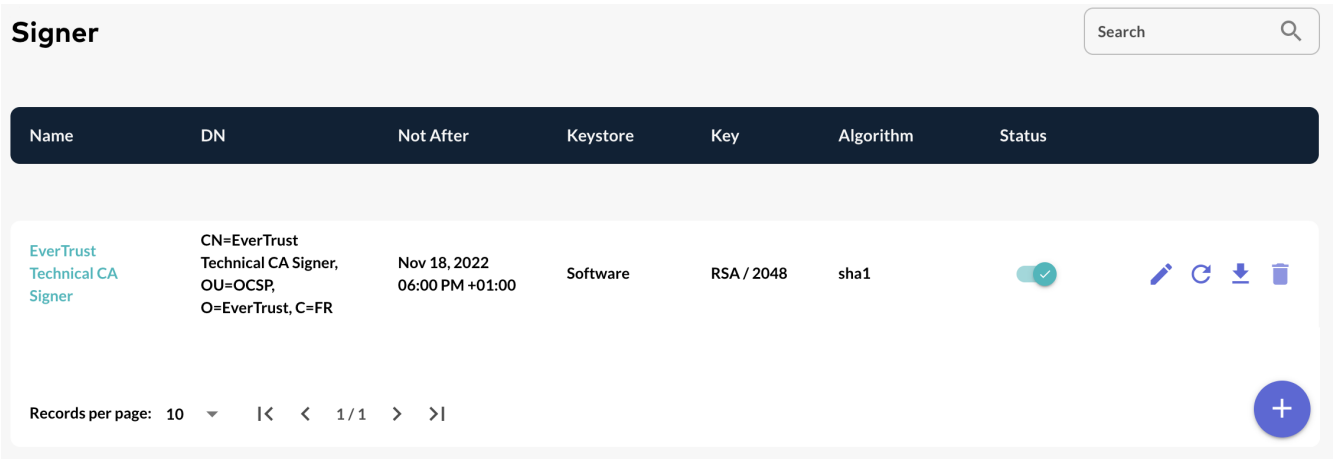
A Signer cannot be disabled if it is defined as a Default Signer in a Certificate Authority. You **MUST** modify this configuration prior to be able to disable it.

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**Configuration**' left menu, select '**Signers**':



Step 3: Hit the button of the Signer you are willing to disable:



Step 4: The Signer is successfully disabled:

2.10. Managing Services

Starting the OCSPd services

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Start the ocspd service with the following command:

```
# /etc/init.d/ocspd start
```

Step 3: Start the nginx service with the following command:

```
# /etc/init.d/nginx start
```

Stopping the OCSPd services

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Stop the ocspd service with the following command:

```
# /etc/init.d/ocspd stop
```

Step 3: Stop the nginx service with the following command:

```
# /etc/init.d/nginx stop
```

2.11. Backup and Restore

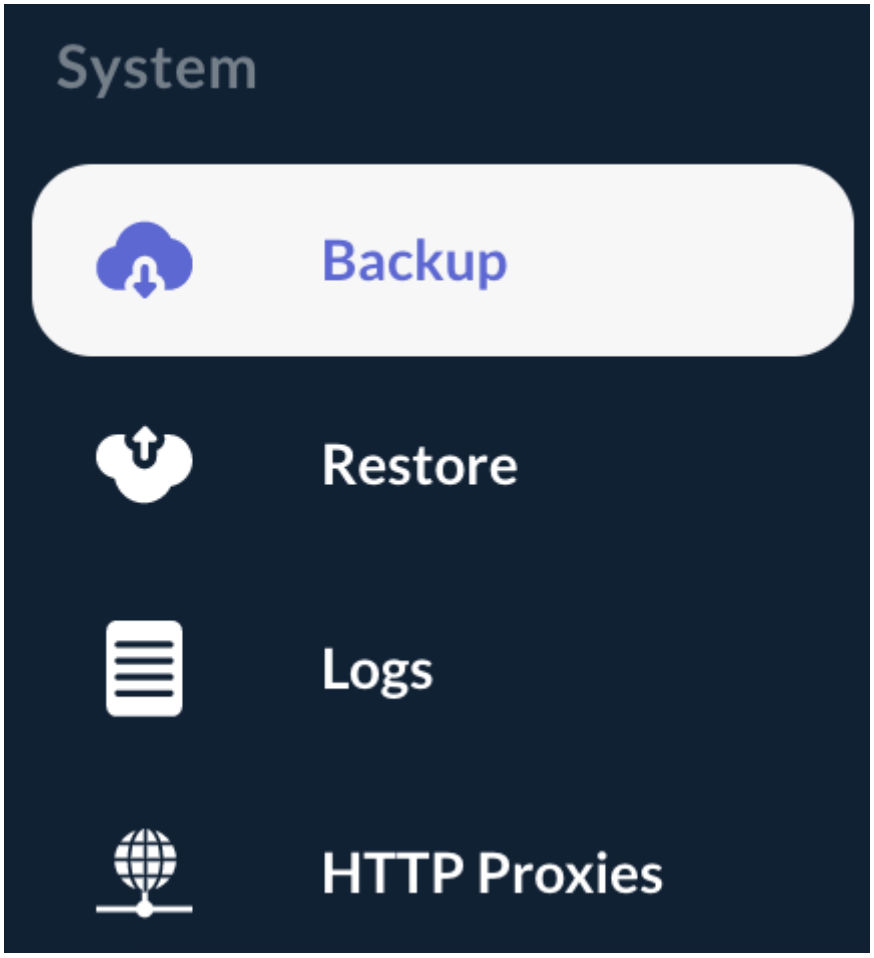
Backup

The following backup procedure does not detail how to back up the Hardware Security Module. Please refer to the HSM provider documentation and **ensure to perform an HSM backup** when using an hardware keystore.

A backup should be performed after each OCSPd configuration modification.

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**System**' left menu, select '**Backup**':



Step 3: Click on '**Generate**' to retrieve a JSON backup file. Keep this file in a safe place.

Click on the following button to generate a JSON backup of the OCSP.

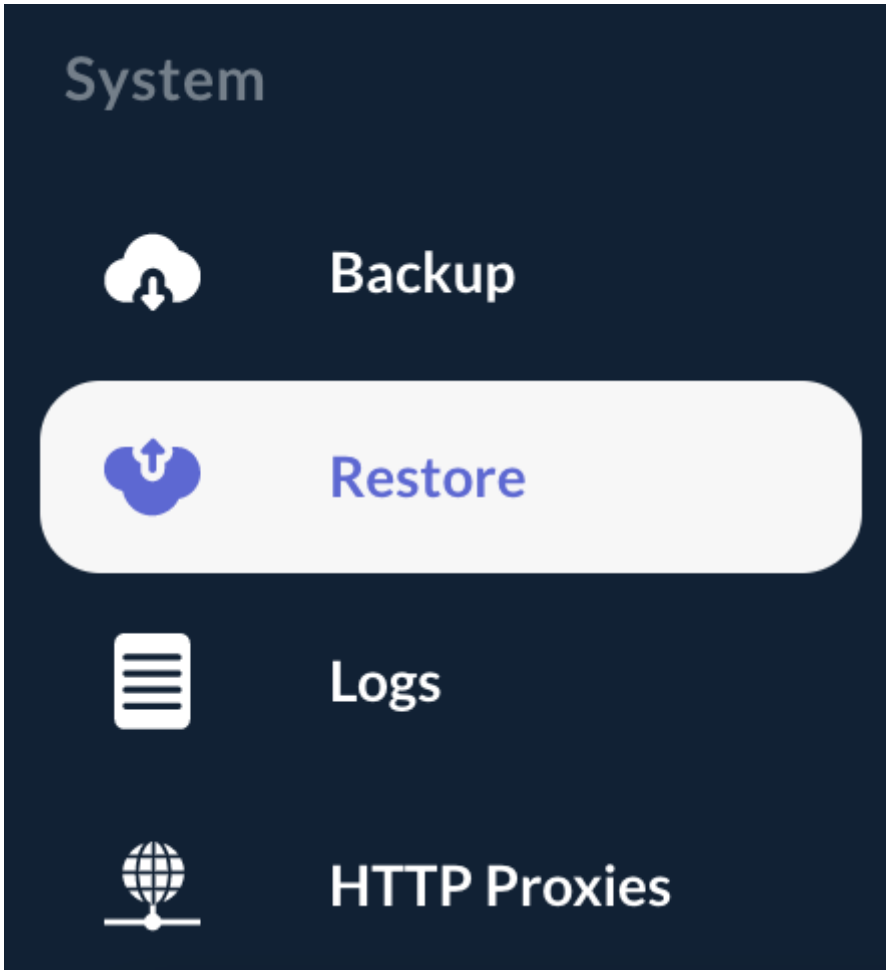
Generate

Restore

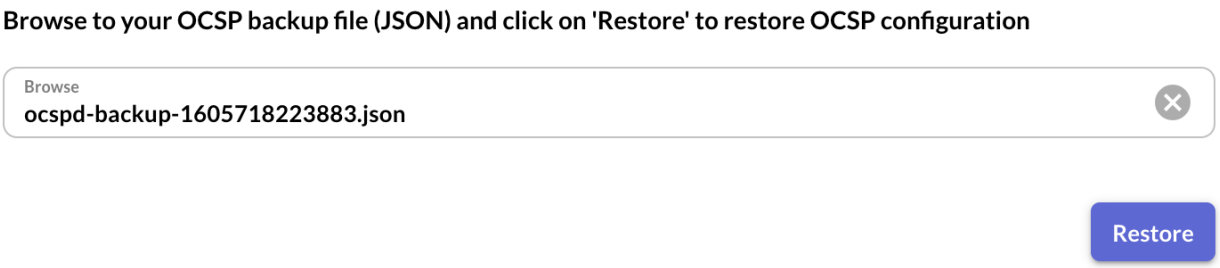
The following restore procedure does not detail how to restore the content of an HSM. Please refer to the HSM provider documentation for restoring HSM secrets.

Step 1: Access the OCSPd Web Management Console;

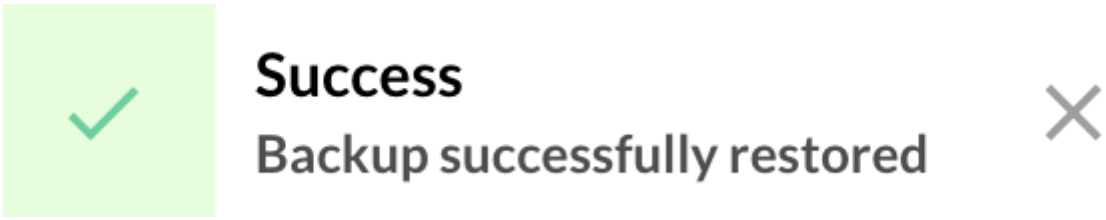
Step 2: In the '**System**' left menu, select '**Restore**':



Step 3: Browse for the OCSPd backup JSON file you want to restore and hit the '**Restore**' button:



Step 5: The Backup is successfully restored:



2.12. Logs & Monitoring

Logs location

Logs are located under '***/opt/ocspd/var/log***' with the following distinction:

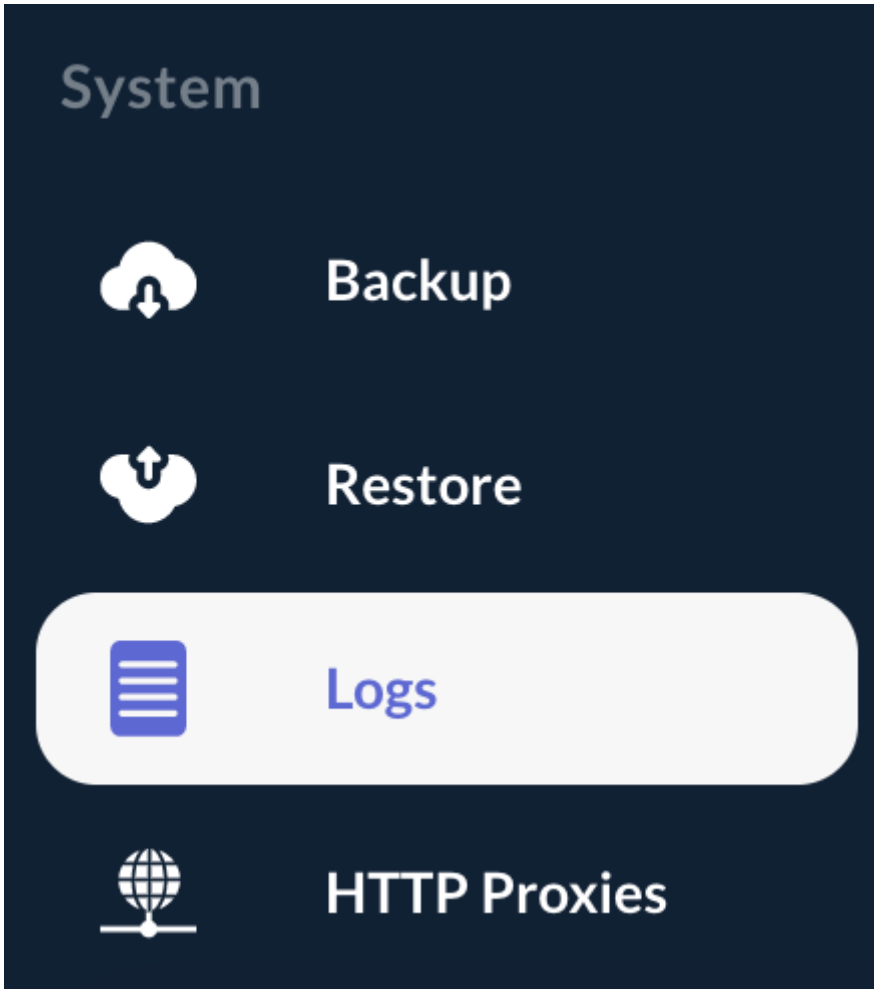
- Application logs are spooled to '***ocspd.log***';
- Administration logs are spooled to '***ocspd-admin.log***' and the log file can be signed upon rotation.

> These log files are rotated daily.

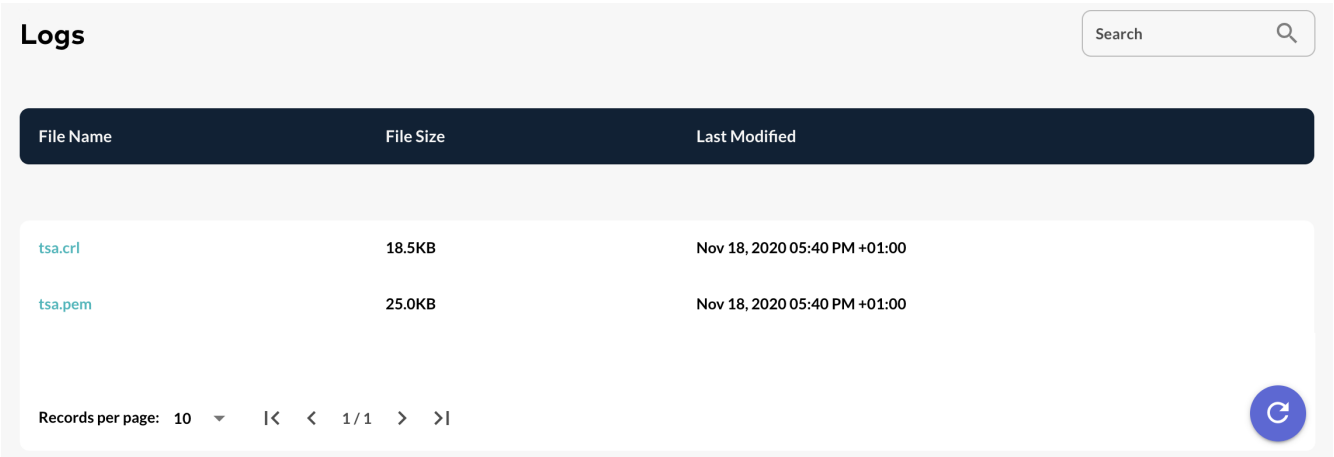
Logs download from the Web Management Console

Step 1: Access the OCSPd Web Management Console;

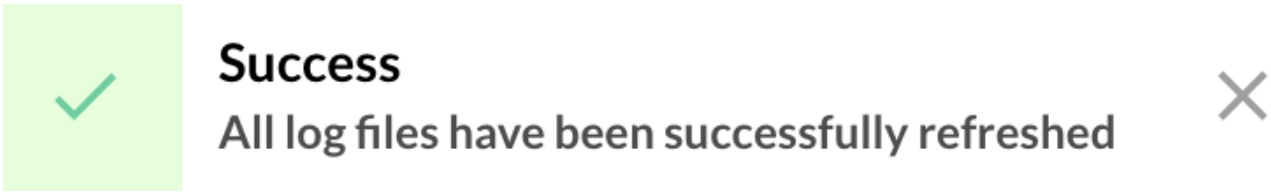
Step 2: In the '**System**' left menu, select '**Logs**':



Step 3: All the logs files under '***/opt/ocspd/var/log***' can be downloaded:



Step 3: All the logs files can be refreshed by hitting the '**Refresh**' button:



Managing the OCSPd Log Level

3 Log Levels are available within OCSPd:

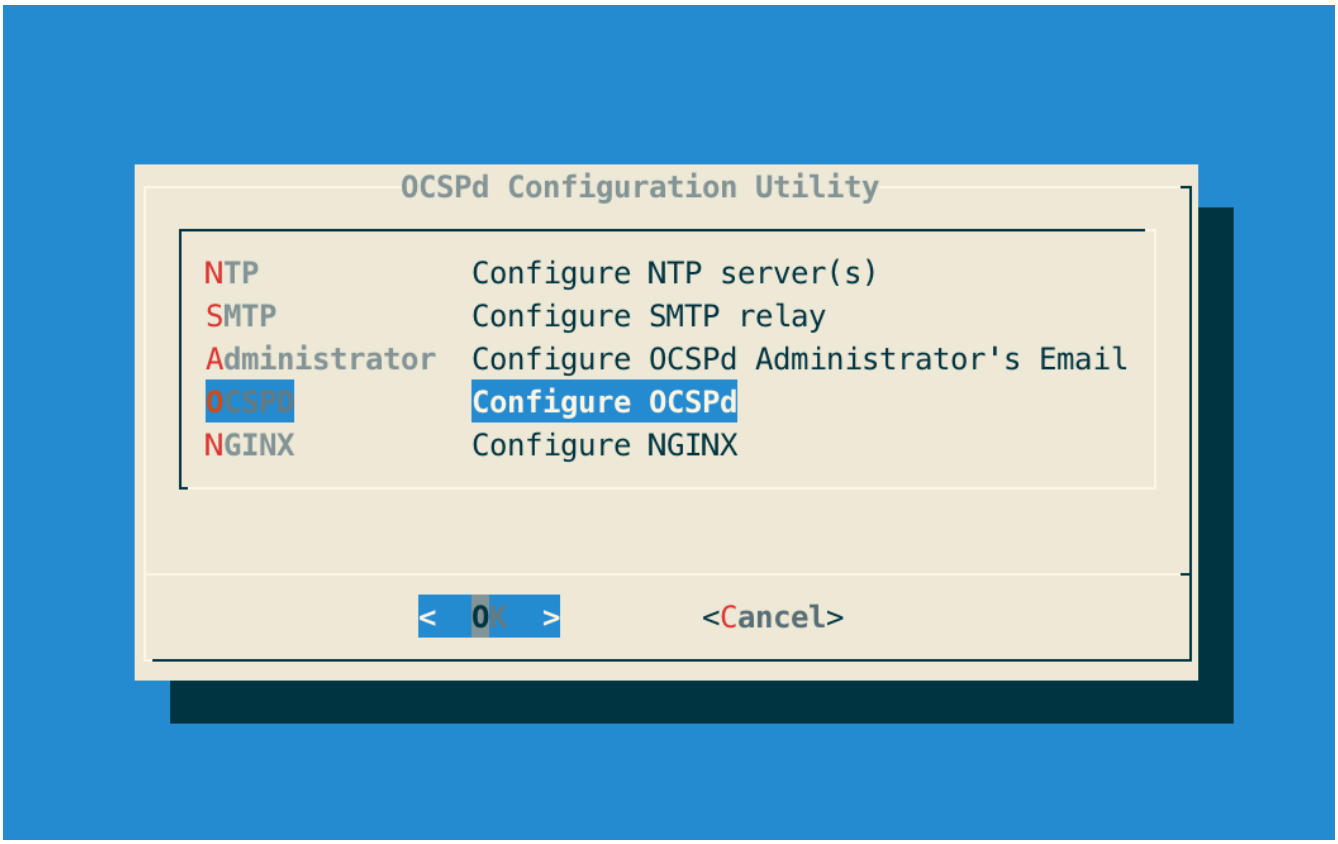
- '***DEBUG***': this mode is very verbose and provides debug information. It should not be turned on in production except for debugging purpose;
- '***INFO***': this is the default mode. It provides error information along with OCSP request information;
- '***ERROR***': this mode only logs errors.

Step 1: Access the server through SSH with an account with administrative privileges;

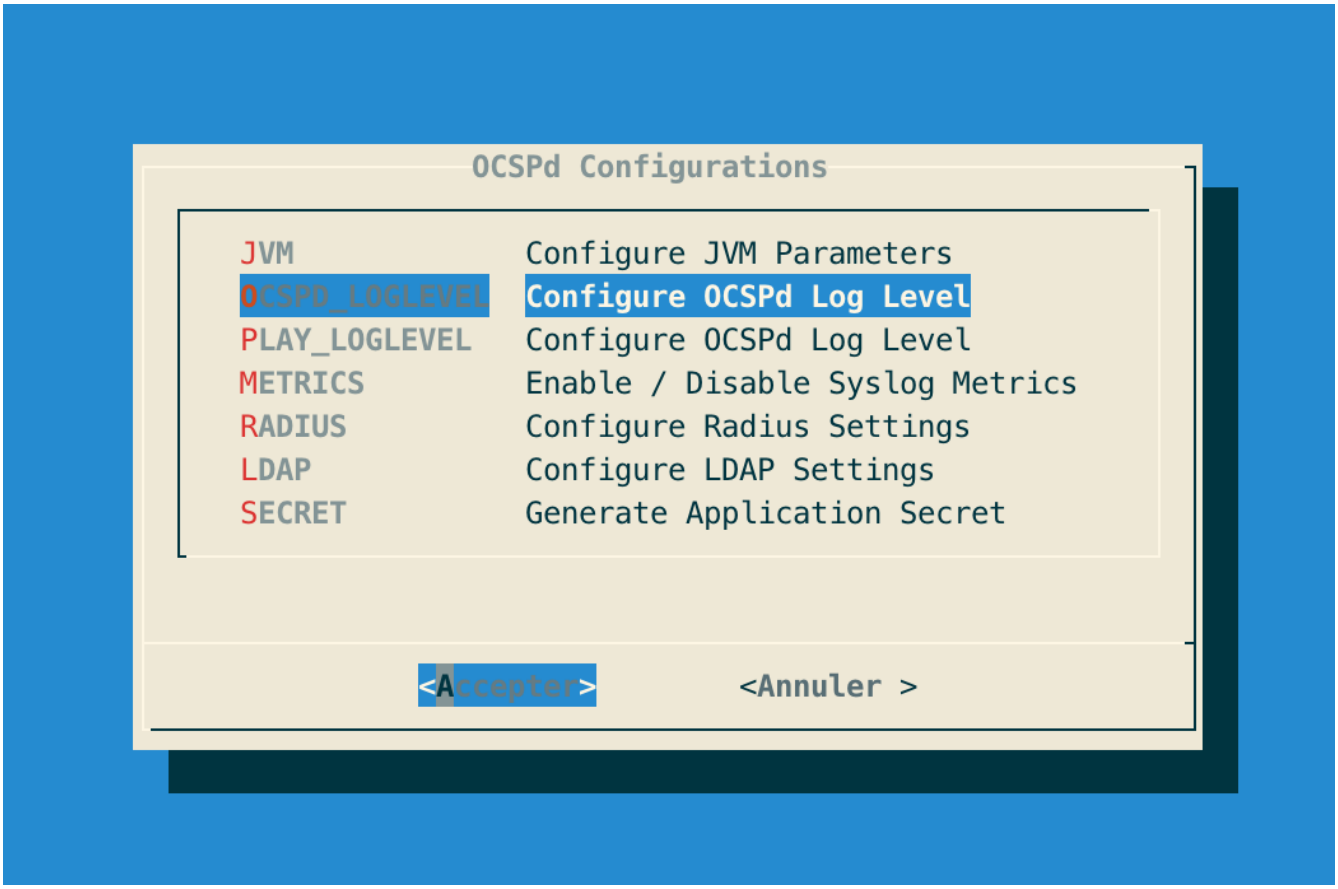
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

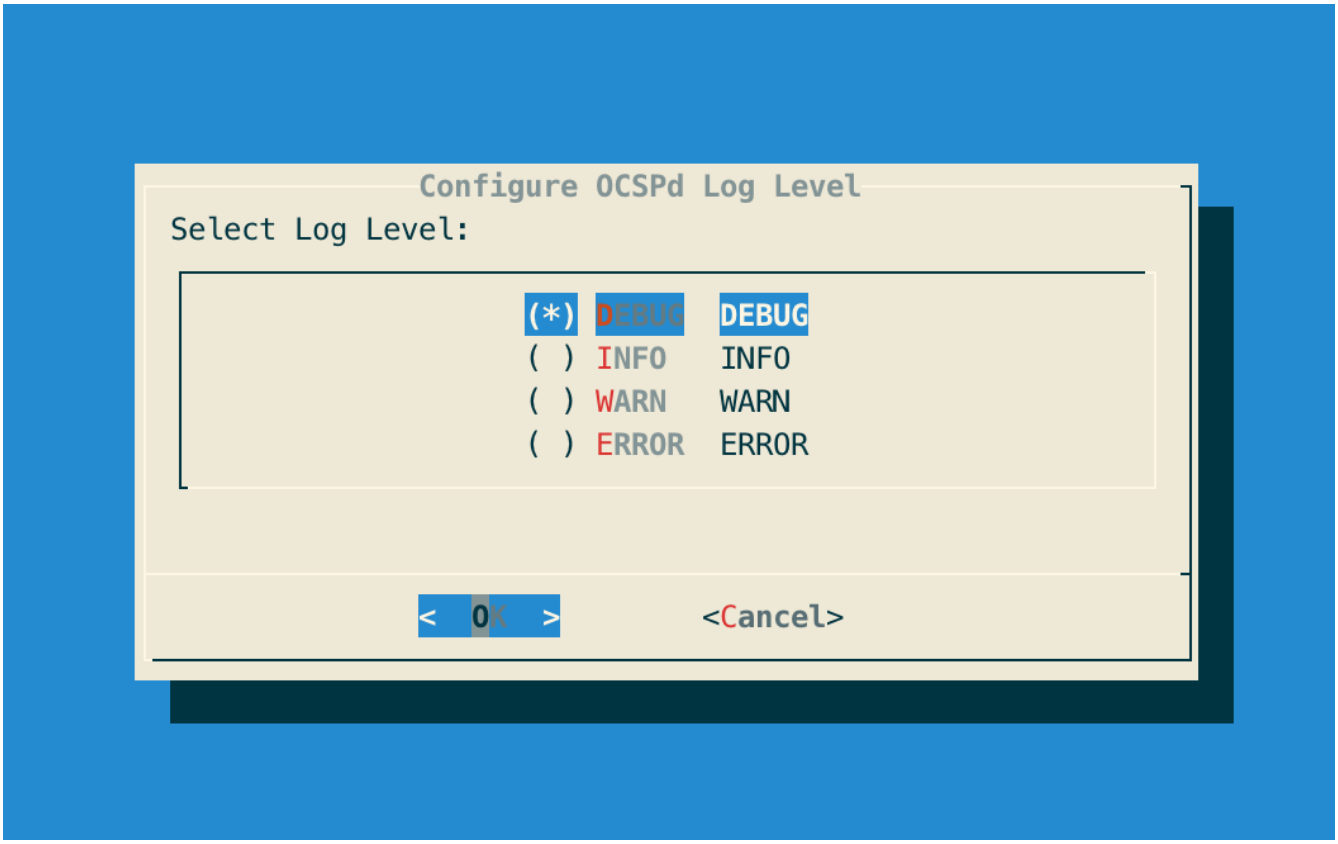
Step 3: In the main menu, select '**OCSPd**':



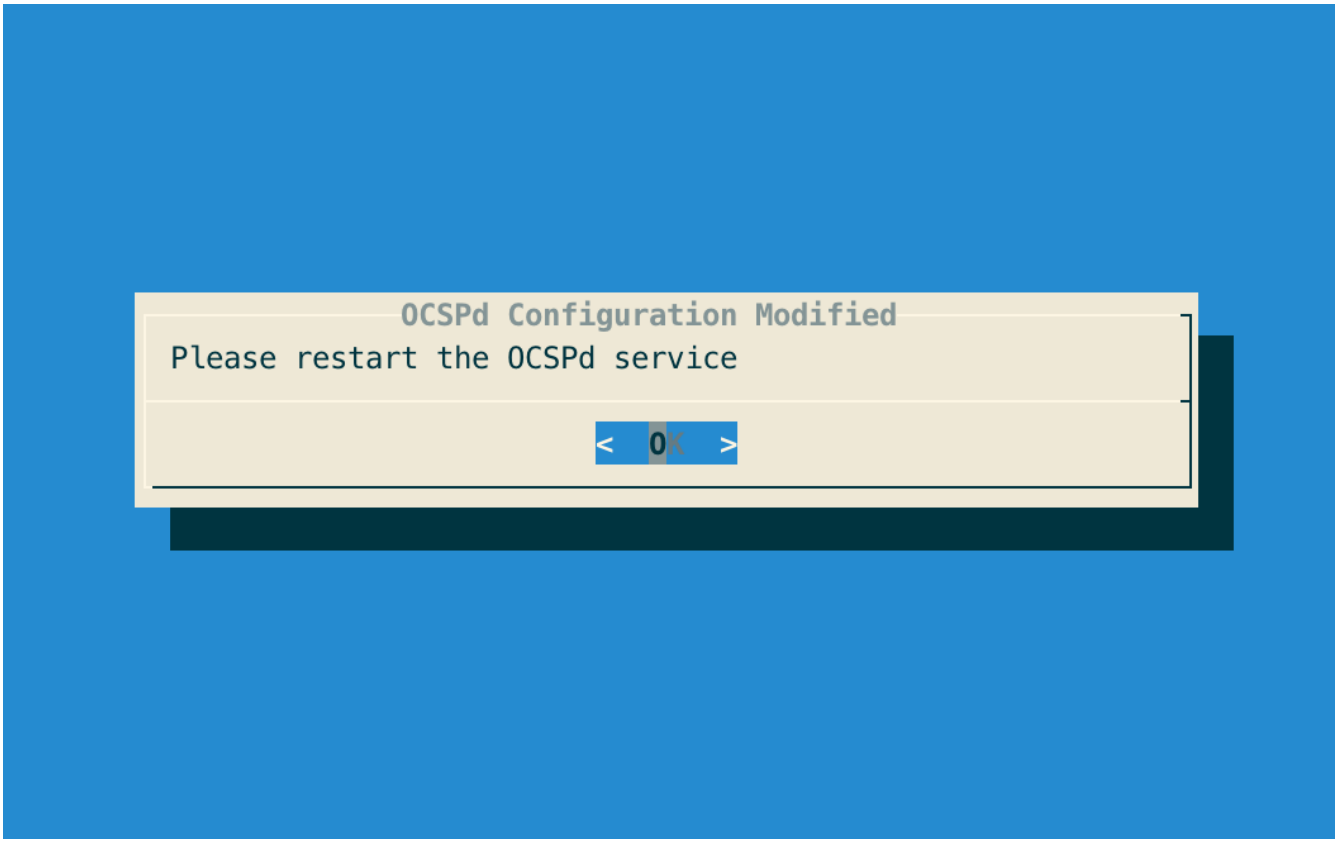
Step 4: In the OCSPD menu, select '**OCSP_LOGLEVEL**':



Step 5: Select the Log Level and validate:



Step 6: The OCSPd configuration is updated:



Step 7: Exit the OCSPd Configuration Utility and restart the OCSPd service with the following command:

```
# /etc/init.d/ocspd restart
```

Monitoring

As of now, OCSPd does not offer any specific monitoring capability. Monitoring must be performed directly by the monitoring system.

Here are the elements to monitor:

- CRL Download through HTTP under '/';
- OCSP request through HTTP under '***/ocsp***';
- Administration interface through HTTPS.

2.13. HTTP Proxies

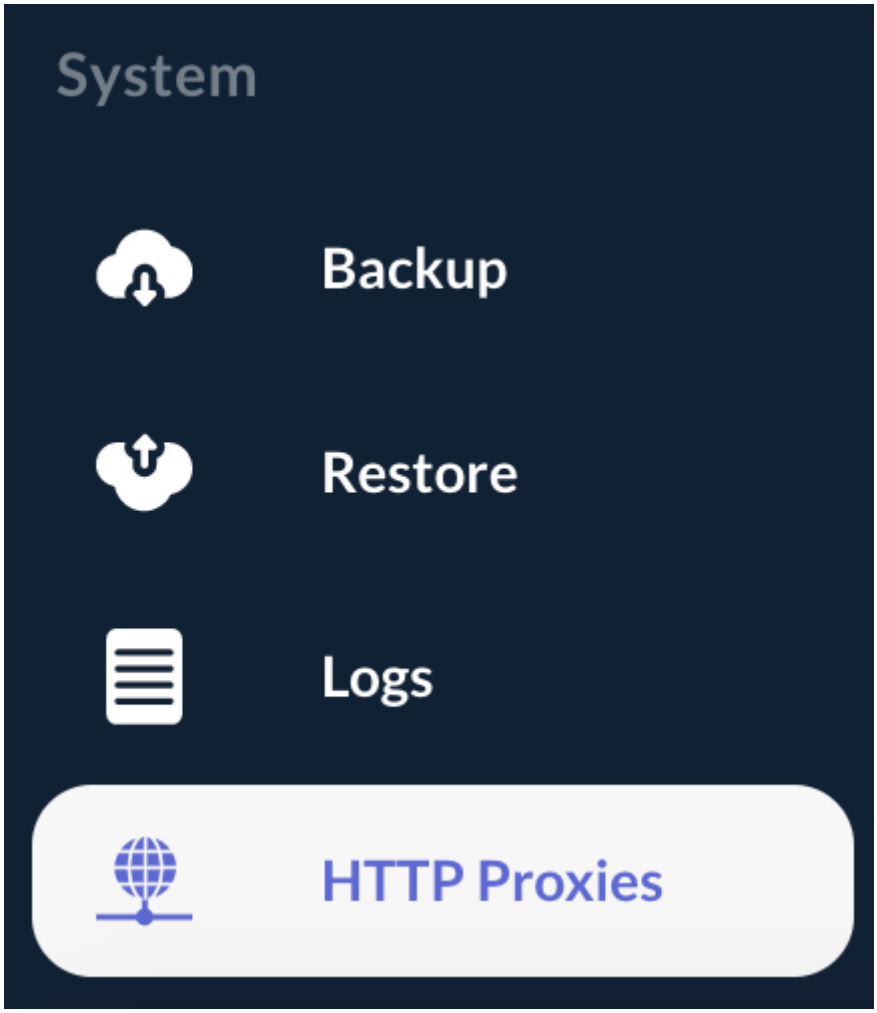
This section details how to manage OCSPd HTTP Proxies.

An HTTP Proxy can be bind to a Certification Authority when the CRL must be downloaded through a proxy.

Creating an HTTP Proxy

Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**System**' left menu, select '**Proxies**':



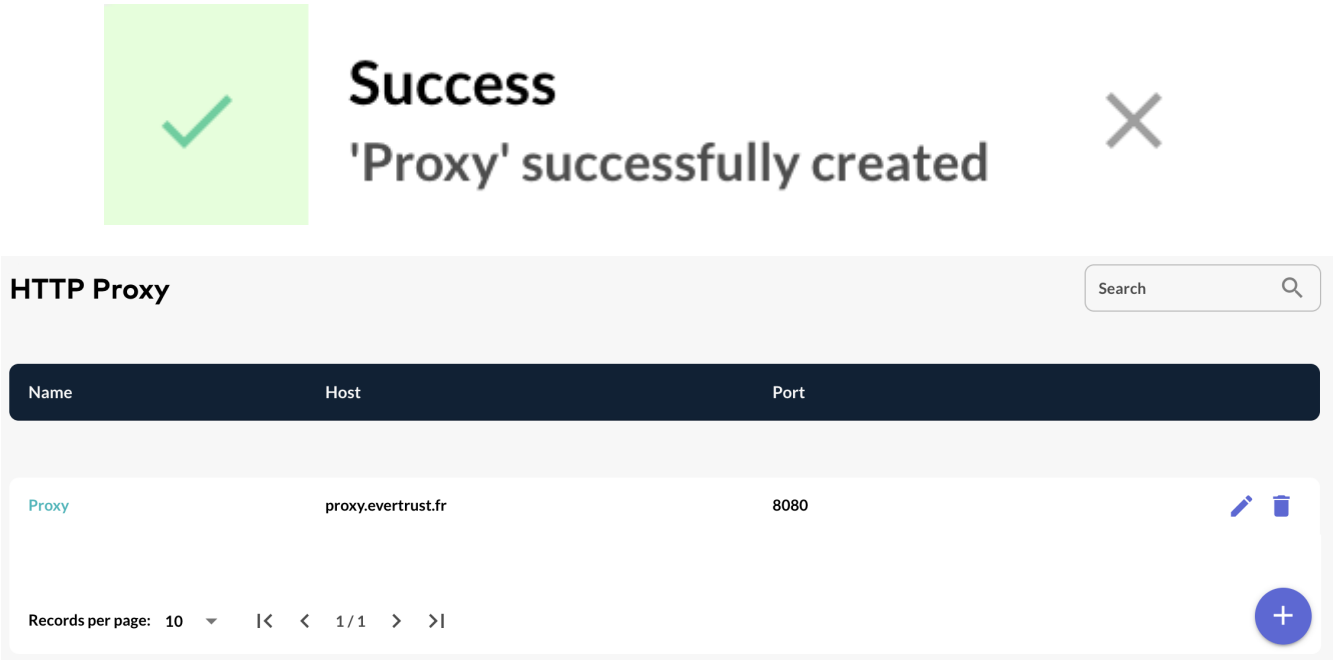
Step 3: In the HTTP Proxies page, hit the '+' button at the bottom of the page:

Step 4: Specify the following elements:

- '**Name**': name of the proxy;
- '**Host**': host of the proxy (can be DNS name or IP address);
- '**Port**': port of the proxy.

And hit the '**Add**' button:

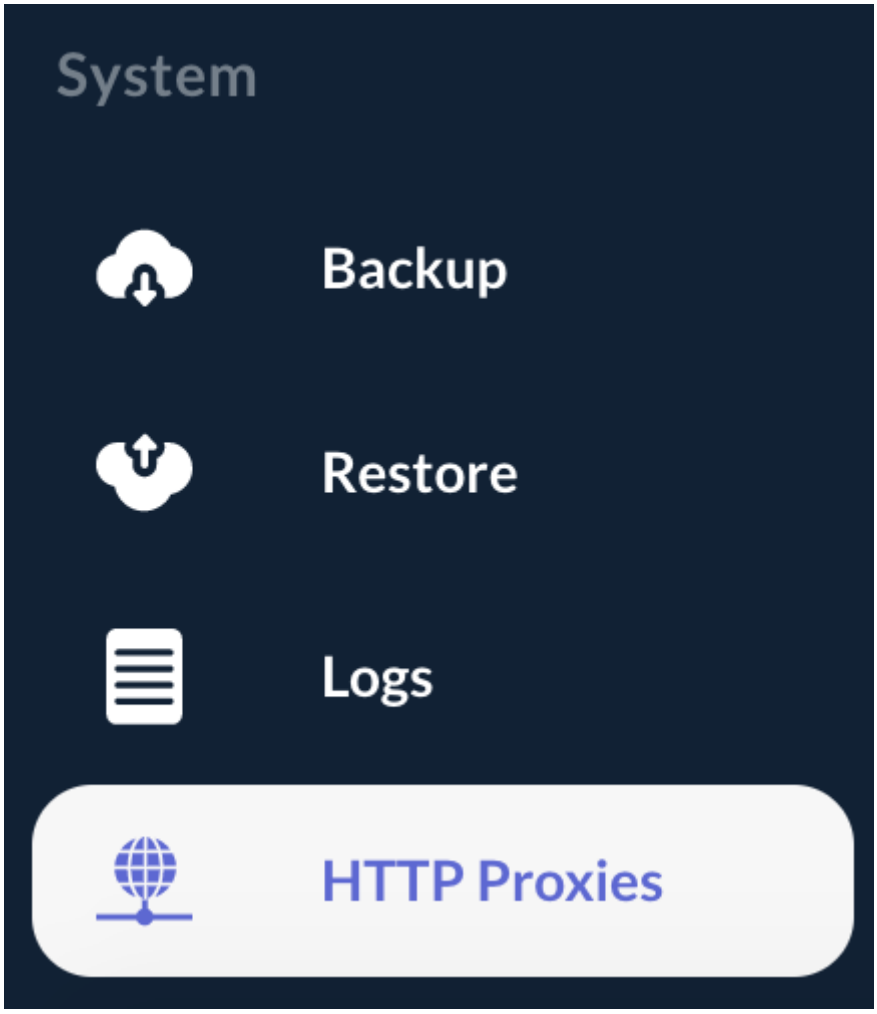
Step 5: The HTTP Proxy is successfully created:



Editing an HTTP Proxy

Step 1: Access the OCSPd Web Management Console;

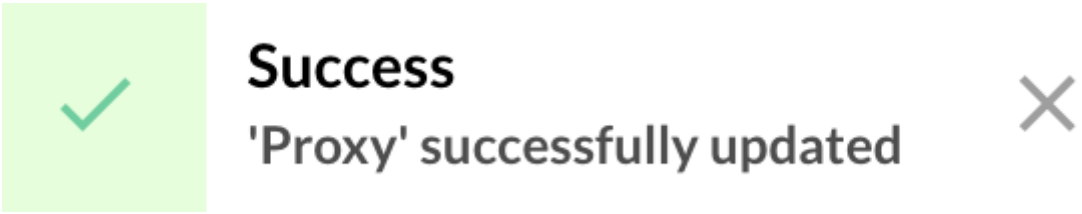
Step 2: In the '**System**' left menu, select '**Proxies**':



Step 3: Click on the HTTP Proxy's name you are willing to edit or hit the button:

Step 4: Modify the HTTP Proxy attributes and hit the '**Update**' button:

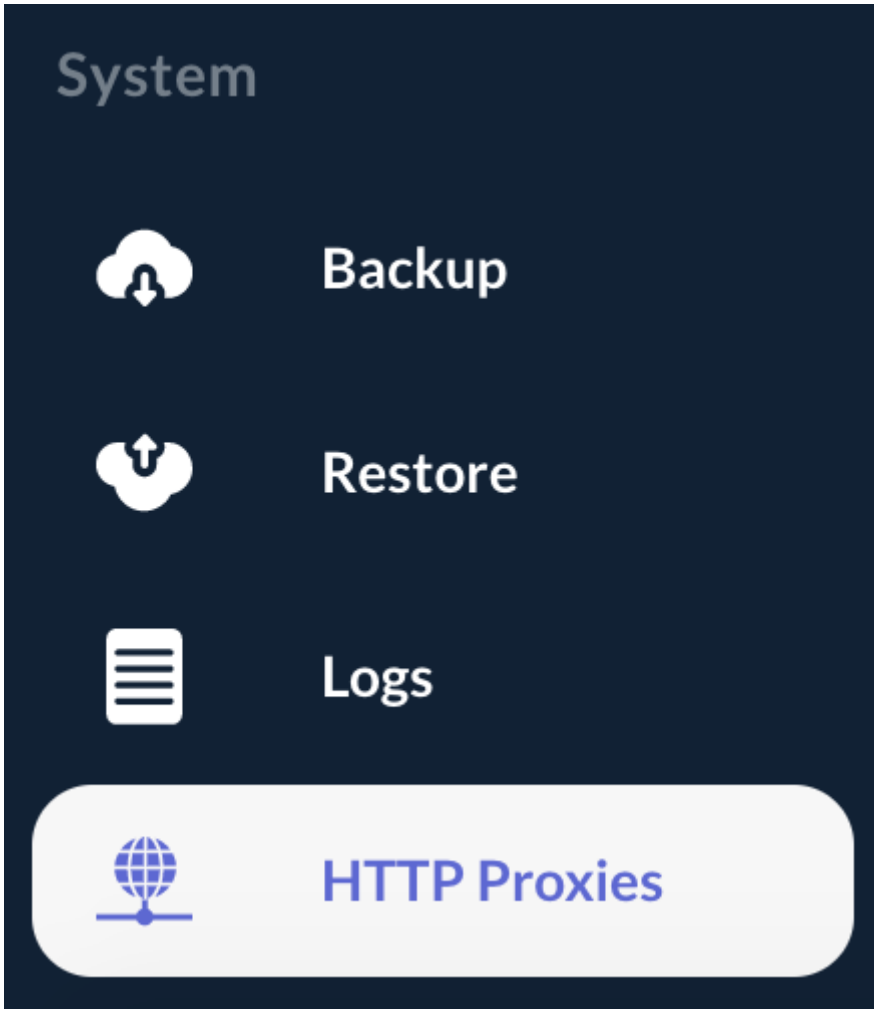
Step 5: The HTTP Proxy is successfully updated:



Deleting an HTTP Proxy

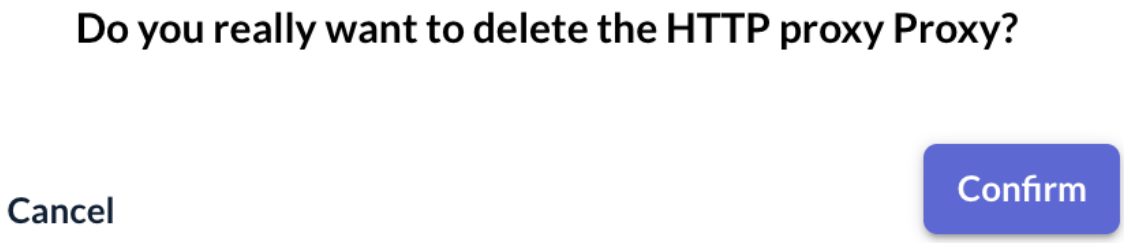
Step 1: Access the OCSPd Web Management Console;

Step 2: In the '**System**' left menu, select '**Proxies**':

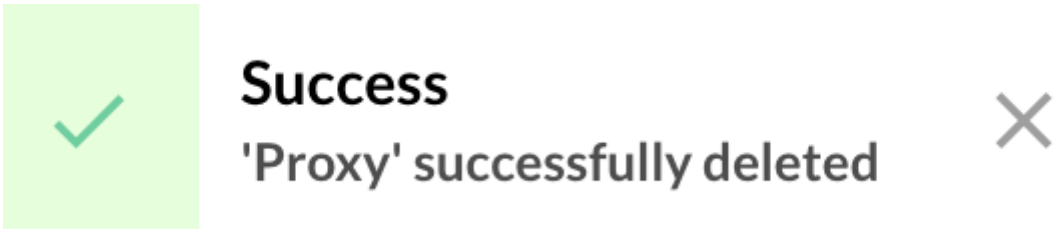


Step 3: Hit the button of the HTTP Proxy you are willing to delete:

Step 4: Hit the '**Confirm**' button:



Step 5: The HTTP Proxy is successfully deleted:



2.14. Key Performance Indicator(s)

OCSPd is able to send syslog event upon OCSP request. It allows to generate performance metrics within tools such as ELK or Splunk.

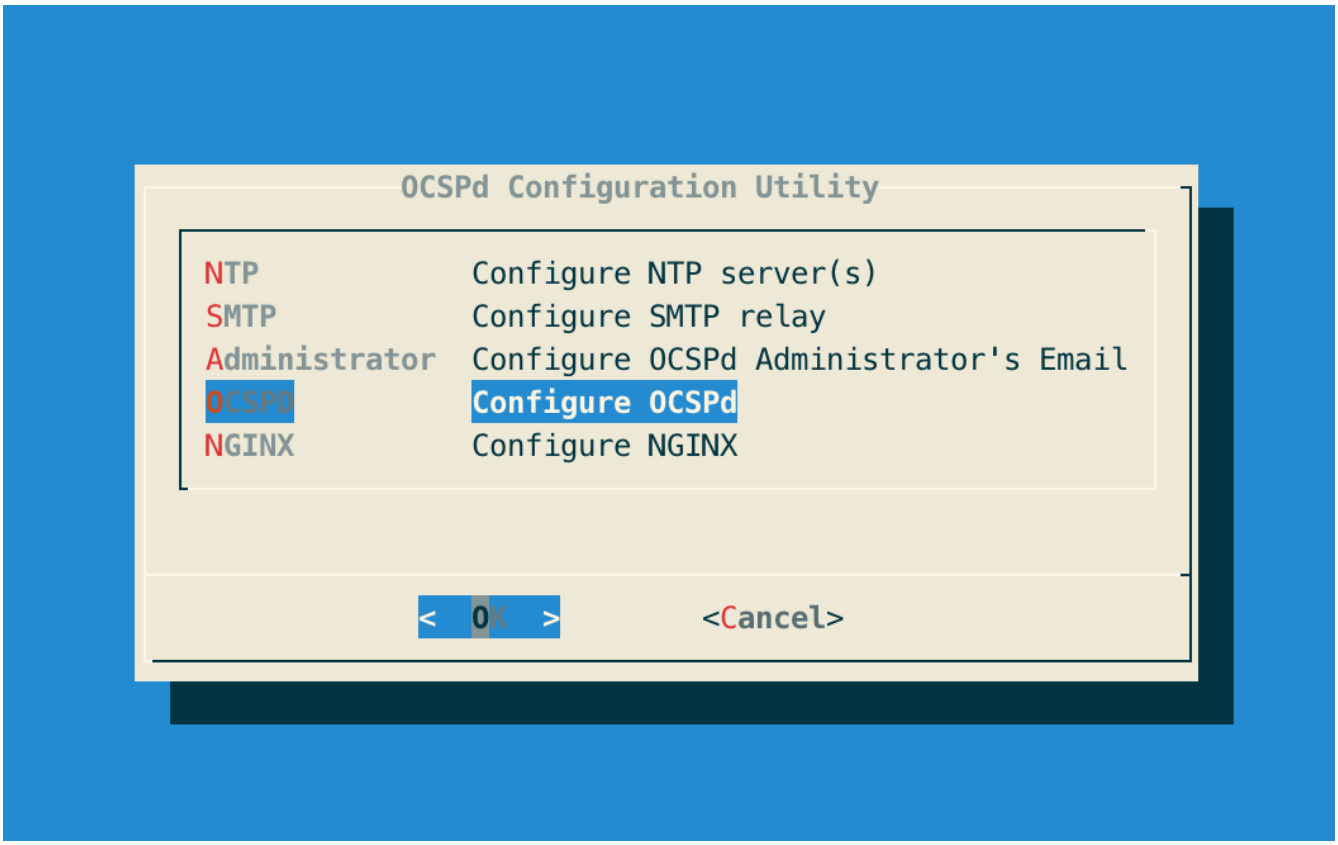
The following KPI configuration procedure does not detail how to aggregate metrics logs. Please refer to the **OCSPd KPI Integration Guide** documentation for more information.

Step 1: Access the server through SSH with an account with administrative privileges;

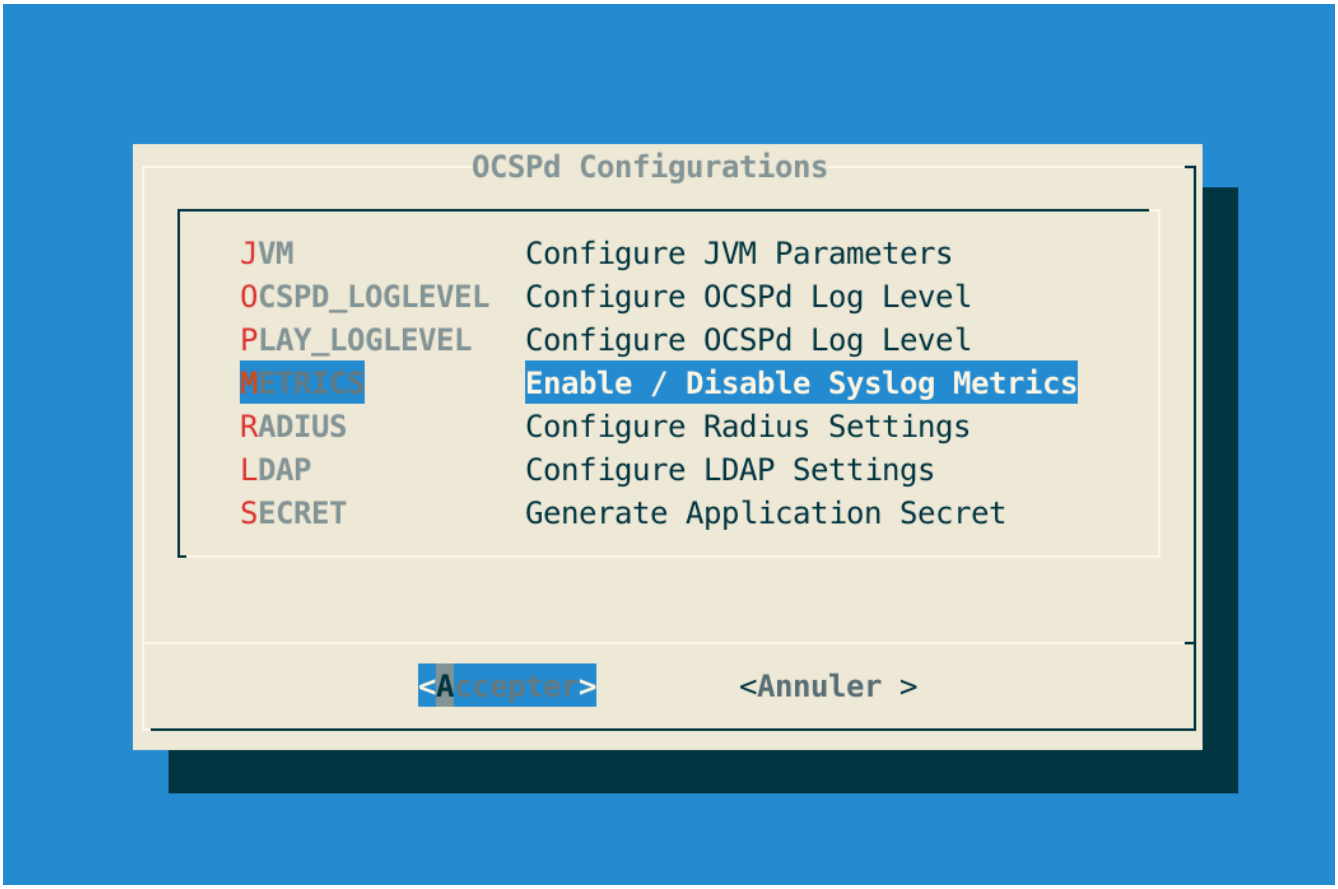
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

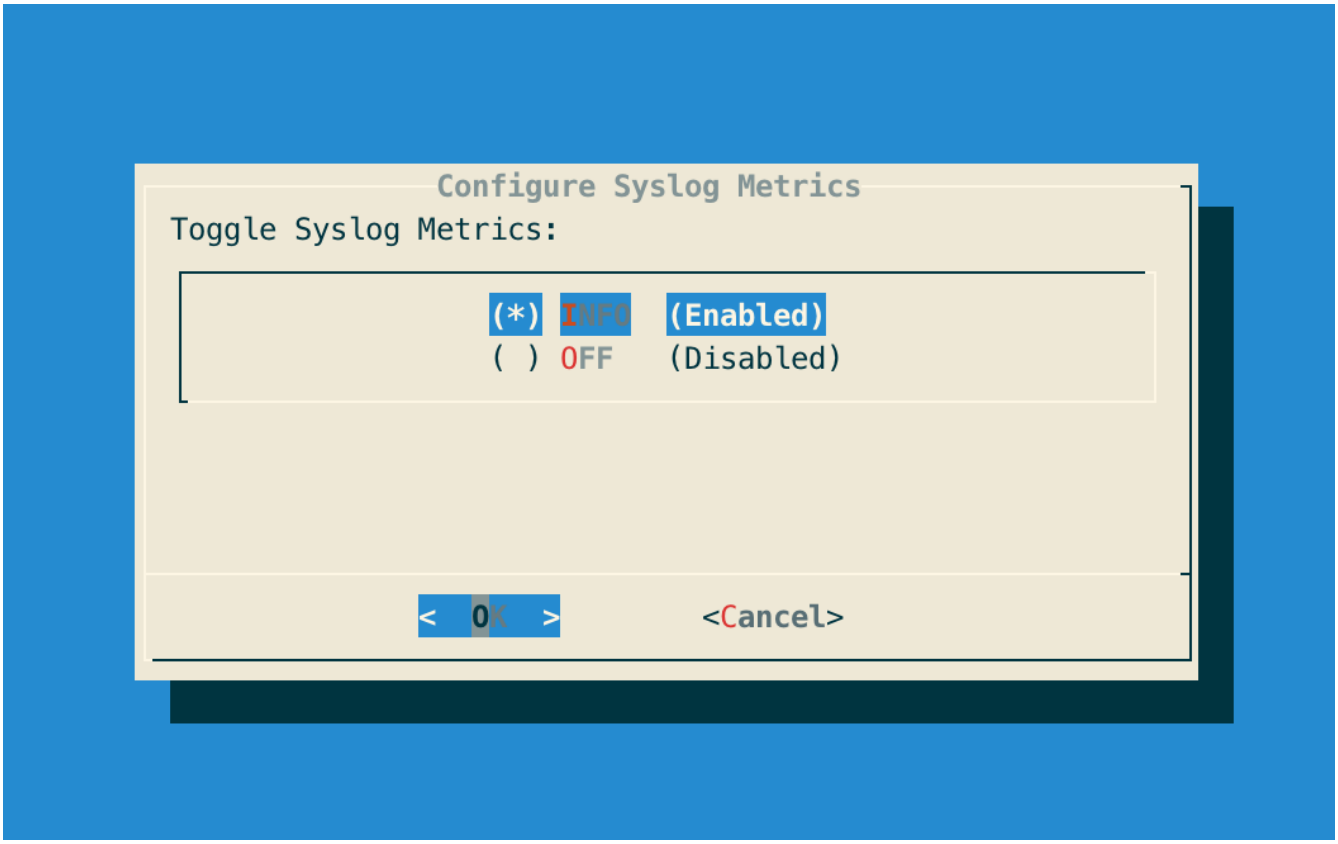
Step 3: In the main menu, select '**OCSPd**':



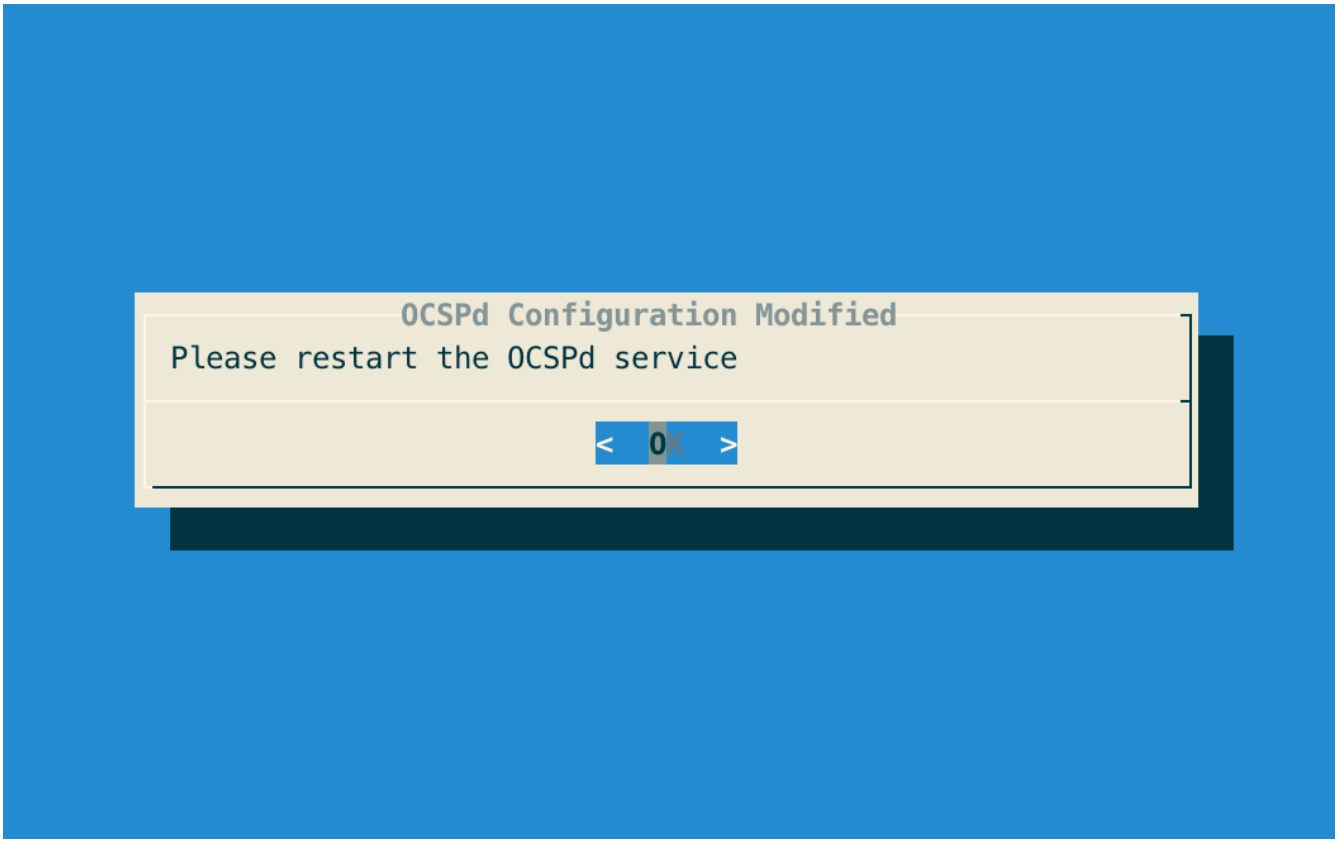
Step 4: In the OCSPD menu, select '**METRICS**':



Step 5: Select the '**INFO**' level to enable Syslog Metrics and validate:



Step 6: The OCSPd configuration is updated:



Step 7: Exit the OCSPd Configuration Utility and restart the OCSPd service with the following command:

```
# /etc/init.d/ocspd restart
```

Step 8: Create an '**ocspd.conf**' syslog configuration file in '**/etc/rsyslog.d**' with the following content to retrieve syslog events from OCSPd and store them into '**/var/log/ocspd/metrics.log**':

```
local6.*                                                /var/log/ocspd/metrics.log
```

You can store syslog events wherever you want, '/var/log/ocspd/metrics.log' is the standard path in UNIX environment.

Step 9: Uncomment the following lines in the '**/etc/rsyslog.conf**':

```
$ModLoad imudp
$UDPServerRun 514
```

Step 10: Restart the Rsyslog service with the following command:

```
# systemctl start rsyslog
```

2.15. Consuming the OCSP service

OCSPd is compliant with RFC:

- 6960
- 5019

Therefore, OCSP request can be realized through:

- HTTP GET (required for OCSP Stapling);
- HTTP POST (standard OCSP request).

When performing an OCSP request against OCSPd, the signer used to sign the response can be:

- Determine dynamically from the OCSP request (POST /ocsp or GET /ocsp/**ocsprequest**);
- Passed in the querystring of the URL (POST /signer/:signer_name/ocsp or GET /signer/:signer_name/ocsp/**ocsprequest**);
- Retrieve from the Certificate Authority settings thanks to the Certificate Authority's name passed in the querystring of the URL (POST /ca/:ca_name/ocsp or GET /ca/:ca_name_ocsp/**ocsprequest**).

The signer_name and ca_name have to be URL encoded. The ocsprequest is the base64 encoded OCSP request.

If the OCSP request contains several entries for several Certificate Authorities, the name of the signer must be passed in the querystring.

3. ELK integration

3.1. Introduction

ELK Description

ELK is the acronym for three open source projects:

- **E**lasticsearch: a search and analytics engine;
- **L**ogstash: a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch;
- **K**ibana: a web application to visualize data with charts and graphs in Elasticsearch.

EverTrust built a powerful monitoring and investigation dashboard for an EverTrust OCSP infrastructure using the complete ELK stack.

This project is powered up by:

- Elastic

This document is specific to ELK version **7.6**.

Scope

This document is an Administration Guide and details how to:

- Deploy and configure log agents on each EverTrust OCSP node;
- Configure the Logstash pipeline;
- Import and manage Kibana indexes, visualizations and dashboards;

Out of Scope

This document does not detail how to install the ELK stack.

3.2. ELK for EverTrust OCSP description

To get a complete overview of the health and activity of an EverTrust OCSP infrastructure, several components are used. Each of them has a specific role in the complete logs processing and is described below.

Logs agents

- Metricbeat to collect System logs. Metricbeat is an ELK agent to periodically collect metrics from the operating system and from services running on the EverTrust OCSP node;
- Filebeat to collect NGINX logs. Filebeat is an ELK agent to monitor the NGINX log files;
- Syslog to collect EverTrust OCSP events. EverTrust OCSP supports the Syslog standard to spool event regarding the application activity.

Logs collector, aggregator and transformer

- Logstash is used as a centralized point of logs collection from all inputs described above. Logstash is configured to receive and transform logs inputs.

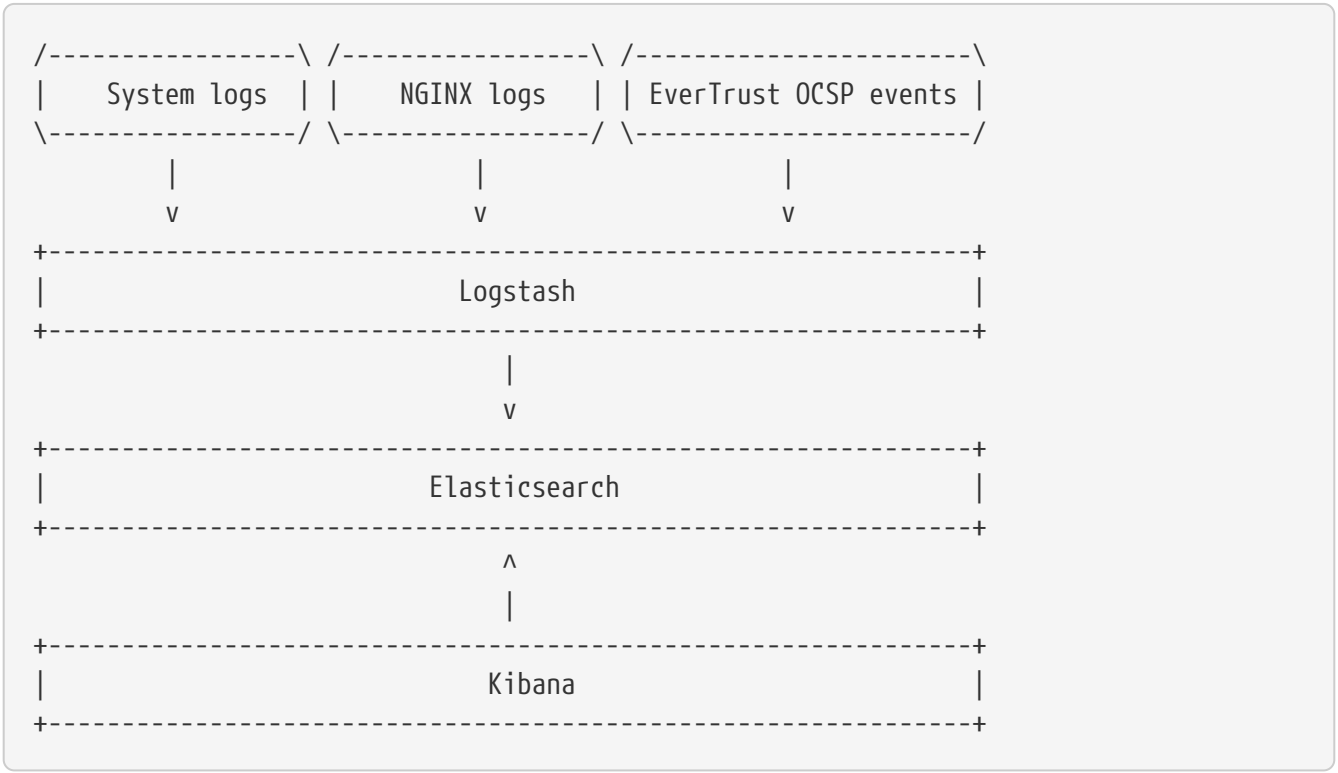
Logs storage and indexation

- Elasticsearch is used as point of storage, indexation of logs received from Logstash. Elasticsearch stores all inputs from Logstash as JSON objects. It provides high capacity of research data.

Logs shaping and visualization

- Kibana is a frontend application that sits on top of ELK stack. Kibana provides search and data visualization capabilities for data indexed in Elasticsearch.

ELK for EverTrust OCSP Overview



Metricbeat and Filebeat are additional and optional components. They are used to provide a complete overview of an EverTrust OCSP infrastructure. The support, maintenance and evolution of this component is **not provided by EverTrust**.

3.3. Logs agents' configuration

Prerequisites

The following flows are required:

- 5044/TCP between each EverTrust OCSP node and the Logstash machine;
- 5000/UDP between each EverTrust OCSP node and the Logstash machine.

All steps described below has to be performed on each EverTrust OCSP node you are willing to monitor.

Installation of the Elastic yum repository

Step 1: Access the EverTrust OCSP server through SSH with an account with administrative privileges;

Step 2: Download and install the Elastic public signing key using the following command:

```
# sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch
```

Step 3: Create a file with a '**.repo**' extension (for example, elastic.repo) in your '**/etc/yum.repos.d/**' directory and add the following lines:

```
[elastic-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Metricbeat installation and configuration

Additional information about Metricbeat installation and operation is available here.

Step 1: Access the EverTrust OCSP server through SSH with an account with administrative privileges;

Step 2: Install the Metricbeat agent using the following command:

```
# yum install metricbeat
```

Step 3: Enable the automatic Metricbeat boot at system start using the following command:

```
# systemctl enable metricbeat
```

Step 4: Modify the configuration of Metricbeat in the following file '**/etc/metricbeat/metricbeat.yml**' to send logs to 5044/TCP port of Logstash instead of Elasticsearch:

```
[...]
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: [""]
[...]
output.logstash:
  # The Logstash hosts
  hosts: ["LOGTASH_HOSTNAME:5044"]
```

Step 5: Start the Metricbeat configuration with the following command:

```
# /etc/init.d/metricbeat start
```

Metricbeat configuration file is an YAML file. It is indentation sensitive.

Filebeat installation and configuration

Additional information about Filebeat installation and operation is available here.

Step 1: Access the EverTrust OCSP server through SSH with an account with administrative privileges;

Step 2: Install the Filebeat agent using the following command:

```
# yum install filebeat
```

Step 3: Enable the automatic Filebeat boot at system start using the following command:

```
# systemctl enable filebeat
```

Step 4: Modify the configuration of Filebeat in the following file '**/etc/filebeat/filebeat.yml**' to setup NGINX logs directory:

```
filebeat.inputs:
[...]
- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/nginx/http-access.log
  exclude_files: ['\.gz$']
  fields:
    log_source: nginx
```

Step 5: Modify the configuration of Filebeat in the following file '**/etc/filebeat/filebeat.yml**' to send logs to 5044/TCP port to Logstash instead of Elasticsearch:

```
[...]
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: [""]
[...]
output.logstash:
  # The Logstash hosts
  hosts: ["LOGTASH_HOSTNAME:5044"]
```

Step 6: Start the Filebeat configuration with the following command:

```
# /etc/init.d/filebeat start
```

Filebeat configuration file is an YAML file. It is indentation sensitive.

Syslog configuration

Please refer to Key '**Performance Indicator(s)**' part of the '**EverTrust OCSP Installation Guide**'.

Step 1: Access the EverTrust OCSP server through SSH with an account with administrative privileges;

Step 2: Modify the '**ocspd.conf**' syslog configuration file in '**/etc/rsyslog.d**' with the following content to send syslog events to 5000/UPD port of Logstash:

```
local6.*                                                @LOGTASH_HOSTNAME:5000
```

Step 3: Restart the Rsyslog service with the following command:

```
# systemctl start rsyslog
```

3.4. Logstash configuration

Prerequisites

Ensure that the following plugins are installed and enabled:

- **logstash-filter-json**;
- **logstash-filter-dns**.

All steps described below has to be performed on each EverTrust OCSP node you want to monitor.

Configuration

Step 1: Retrieve the '**ocspd-dictionary.yml**' on the Web Management Console of one of your EverTrust OCSP;

Step 2: Upload the '**ocspd-dictionary.yml**' file under '**/usr/share/logstash/config/**' on the Logstash server;

Step 3: Upload the '**ocspd-pipeline.yml**' file on the Logstash server;

Step 4: Modify the following lines of the '**ocspd-pipeline.yml**' file to specify the Elasticsearch host(s) and the authentication information:

```
elasticsearch {
                        hosts => ["ELASTICSEARCH_HOST:ELASTICSEARCH_PORT"]
                        user => "ELASTICSEARCH_USER"
                        password => "ELASTICSEARCH_PASSWORD"
                }
```

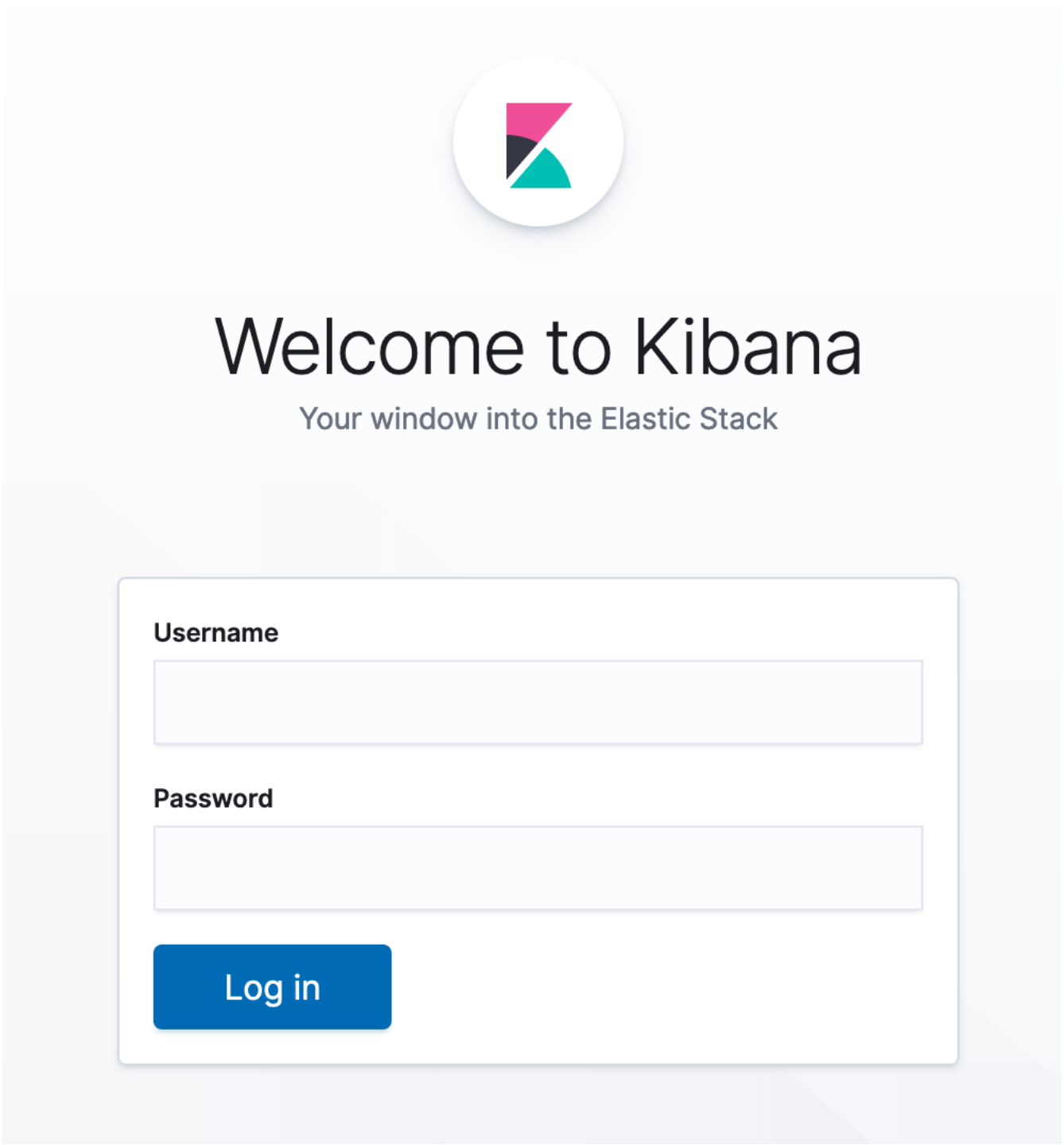
Step 4: Modify your current Logstash configuration to use the new '**ocspd-pipeline.yml**';

Step 5: Restart the Logstash service with the following command:

```
# systemctl restart logtash
```

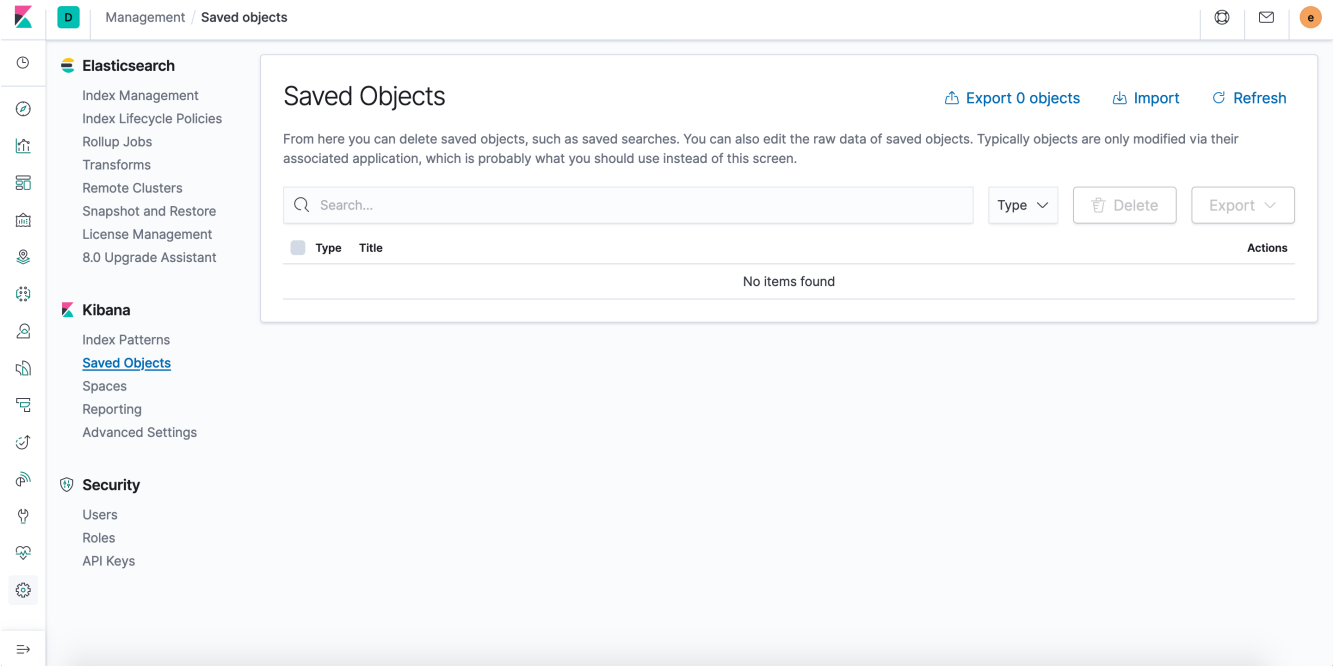
3.5. Kibana configuration

Step 1: Access to the Kibana GUI using a web browser;

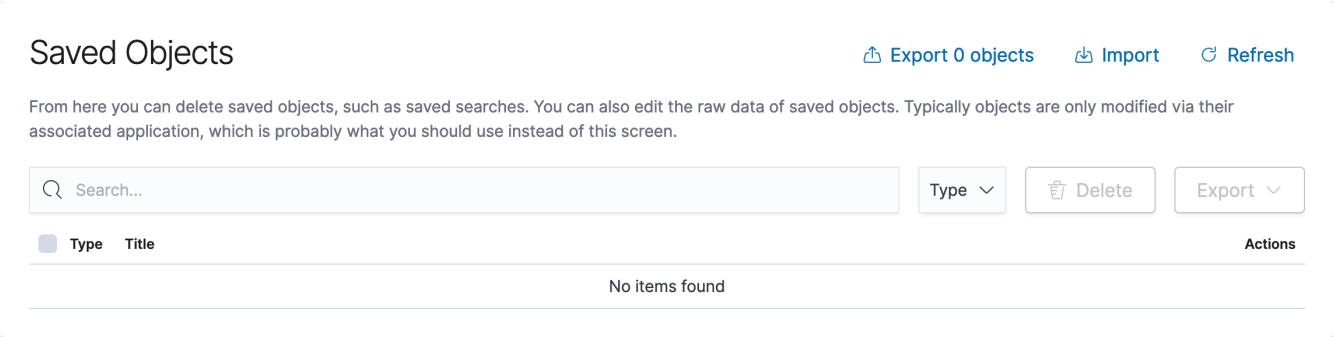


Step 2: Login with an administrator;

Step 3: Navigate to '**Management**' > '**Kibana**' > '**Saved Objects**';



Step 4: Click on '**Import**' and select the '**ocspd.ndjson**' file;



Step 5: Restart the kibana linux service on the machine;

3.6. Index details

JSON array are represented in the following table with the '.' delimiter.

NGINX index details

will find attached an example of an '**nginx-ocspd.json**' log as stored by Elasticsearch in JSON format.

Here is the explanation of this JSON file.

JSON Entry	Signification
_source.ocspd.hostname	Hostname of OCSP node where the log is from
_source.ocspd.clientname	Hostname of the Client that did the request
_source.ocspd.logtype	Type of log
_source.clienip	Requester client @IP

JSON Entry	Signification
_source.ident	HTTP remote identity
_source.auth	HTTP remote user
_source.timestap	Request timestamp
_source.verb	HTTP method
_source.request	URL of the request
_source.httpversion	HTTP version
_source.rawrequest	Complete request received
_source.response	HTTP status code
_source.bytes	Body bytes sent
_source.user_agent	User agent of the HTTP requester
_source.referrer	Address of the webpage which is linked to the resource being requested
_source.agent	Information about the Filebeat agent that send the log
_source.log	Log file name where this log is from

EverTrust OCSP index details

Inside an OCSP request, 3 situations can be found:

- Request for the status of a unique certificate for a unique Certificate Authority;
- Request for the status of multiples certificates for a unique Certificate Authority.
- Request for the status of multiples certificates for multiples Certificate Authorities.

That's why we have decided to split the EverTrust OCSP logs into two different log indexes. The first one gives information about the global OCSP request and is called '**request-ocspd**'. The second one gives details of each certificate status checked inside the request and is called '**item-ocspd**'.

EverTrust OCSP request

You will find attached an example of an '**request-ocspd.json**' log as stored by Elasticsearch in JSON format.

Here is the explanation of this JSON file.

JSON Entry	Signification
_source.ocspd.hostname	Hostname of OCSP node where the log is from
_source.ocspd.clientname	Hostname of the Client that did the request
_source.ocspd.logid	Identifier of log

JSON Entry	Signification
_source.ocspd.logtype	Type of log
_source.ocspd.request.status	Response status of the associated request
_source.ocspd.request.error	Response error of the associated request

EverTrust OCSP item

You will find attached an example of an '**item-ocspd.json**' log as stored by Elasticsearch in JSON format.

Here is the explanation of this JSON file.

JSON Entry	Signification
_source.ocspd.hostname	Hostname of OCSP node where the log is from
_source.ocspd.clientname	Hostname of the Client that did the request
_source.ocspd.logid	Identifier of log
_source.ocspd.logtype	Type of log
_source.ocspd.CAissuer.keyhash	Key hash of the CA issuer
_source.ocspd.CAissuer.name	Name of the CA issuer
_source.ocspd.cert.info	Information about the certificate (Certificate Serial Number/CA Issuer Name)
_source.ocspd.cert.status	Status of the certificate