



EverTrust OCSP documentation v3.1.3

Administration Guide

EVERTRUST

Table of Contents

| | |
|--|----|
| 1. Introduction | 1 |
| 1.1. Description | 1 |
| 1.2. Scope | 1 |
| 1.3. Out of Scope | 2 |
| 2. NGINX Specific Configurations | 3 |
| 2.1. Enabling OCSP Stapling | 3 |
| 2.2. Renewing the Server certificate | 5 |
| 3. Initial Management Console Access and Logout | 9 |
| 3.1. Management Console Access | 9 |
| 3.2. Management Console Logout | 11 |
| 4. Administrator Profile | 12 |
| 4.1. Account Information | 12 |
| 4.2. Resetting Password | 14 |
| 5. Managing Administrators | 15 |
| 5.1. Creating an Administrator | 15 |
| 5.2. Setting Administrator Password Policy | 22 |
| 5.3. Editing or deleting Administrators | 23 |
| 6. Managing Roles | 27 |
| 6.1. Creating a Role | 27 |
| 6.2. Editing a Role | 30 |
| 6.3. Display and manage Members of a Role | 32 |
| 6.4. Deleting a Role | 33 |
| 7. Managing Hardware Security Modules | 34 |
| 7.1. Supported Hardware Security Modules | 34 |
| 7.2. Managing Modules | 34 |
| 7.3. Managing HSM slots | 40 |
| 7.4. Managing FIPS 140-2 Level 3 Key Generation Mode | 48 |
| 7.5. HSM specifics | 52 |
| 8. Managing Certificate Authorities | 53 |
| 8.1. Importing a Certificate Authority | 53 |
| 8.2. Editing a Certificate Authority | 59 |
| 8.3. CRL management | 61 |
| 8.4. Downloading the CA certificate | 63 |
| 8.5. Deleting a Certificate Authority | 64 |
| 8.6. Understanding the Cache Management | 66 |
| 9. Managing OCSP Signers | 68 |
| 9.1. Creating a Signer | 68 |
| 9.2. Managing Signer Certificate Requests | 70 |
| 9.3. Managing Signers | 75 |

| | |
|---|-----|
| 9.4. Downloading a Signer Certificate | 81 |
| 9.5. Enabling or Disabling Signers | 82 |
| 10. Managing Services | 87 |
| 10.1. Starting the OCSPd services | 87 |
| 10.2. Stopping the OCSPd services | 87 |
| 11. Backup and Restore | 88 |
| 11.1. Backup | 88 |
| 11.2. Restore | 90 |
| 12. Logs & Monitoring | 92 |
| 12.1. Logs location | 92 |
| 12.2. Logs download from the Web Management Console | 92 |
| 12.3. Managing the OCSPd Log Level | 93 |
| 12.4. Monitoring | 96 |
| 13. HTTP Proxies | 97 |
| 13.1. Creating an HTTP Proxy | 97 |
| 13.2. Editing an HTTP Proxy | 99 |
| 13.3. Deleting an HTTP Proxy | 101 |
| 14. Key Performance Indicator(s) | 103 |
| 15. Consuming the OCSP service | 106 |

1. Introduction

1.1. 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**.

1.2. 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.

1.3. Out of Scope

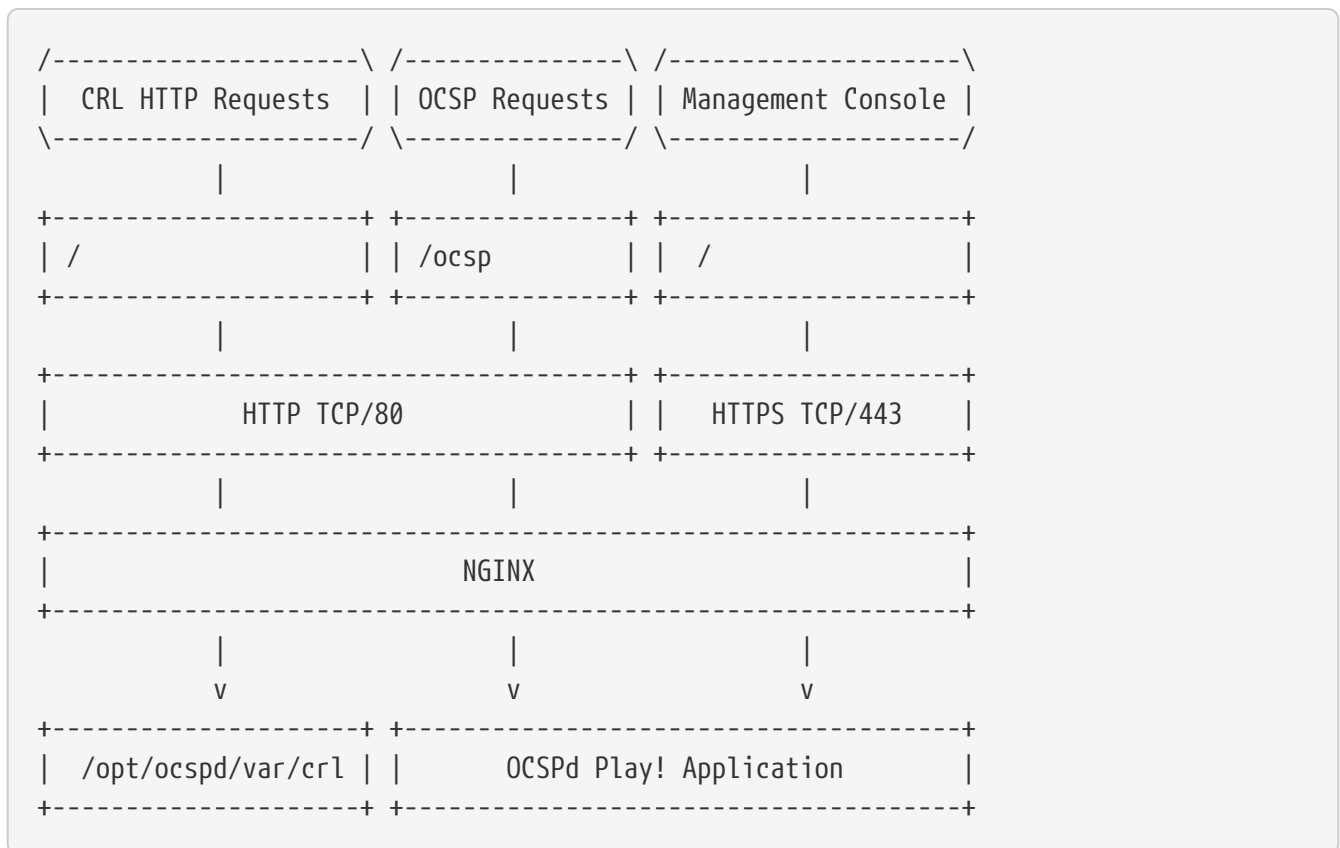
This document does not detail how to install the OCSPd component. For installation and uninstallation procedures, please refer to the '**OCSPd Installation Guide**'.

2. 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:



CAUTION

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.

2.1. Enabling OCSP Stapling

NOTE

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.

TIP

More information regarding OCSP Stapling can be found here [OCSP Stapling](#).

CAUTION

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
```

2.2. Renewing the Server certificate

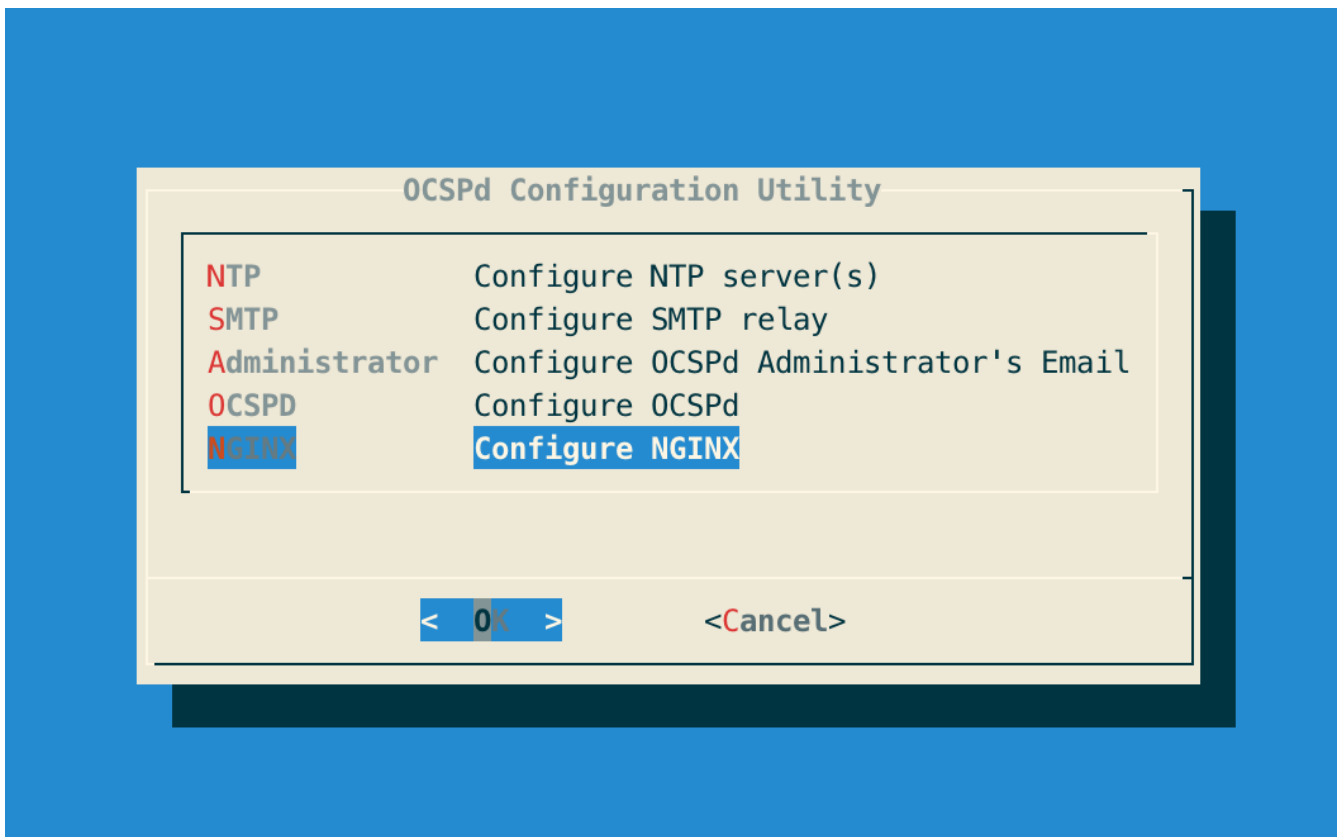
2.2.1. Issuing a Certificate Request (PKCS#10)

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

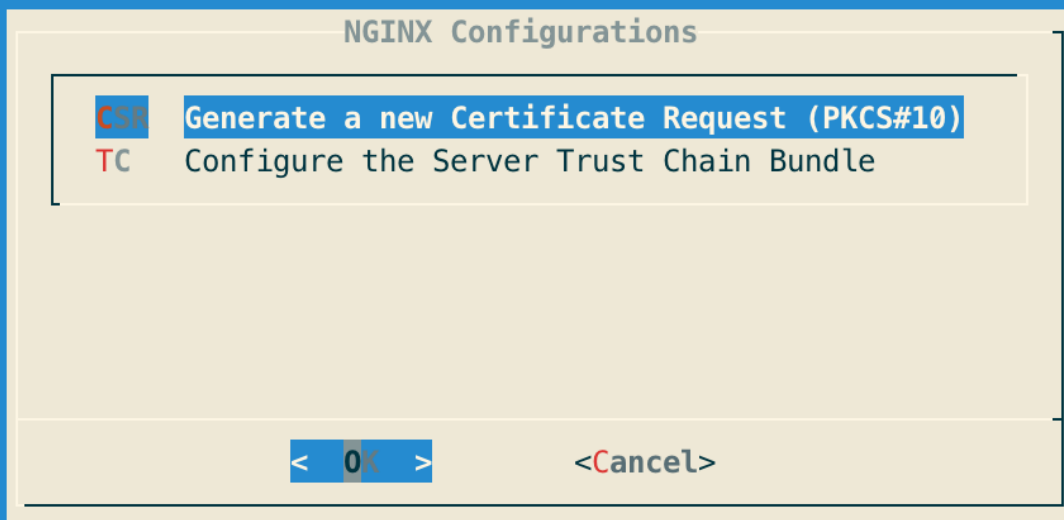
Step 2: Load the OCSPd Configuration Utility with the following command:

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

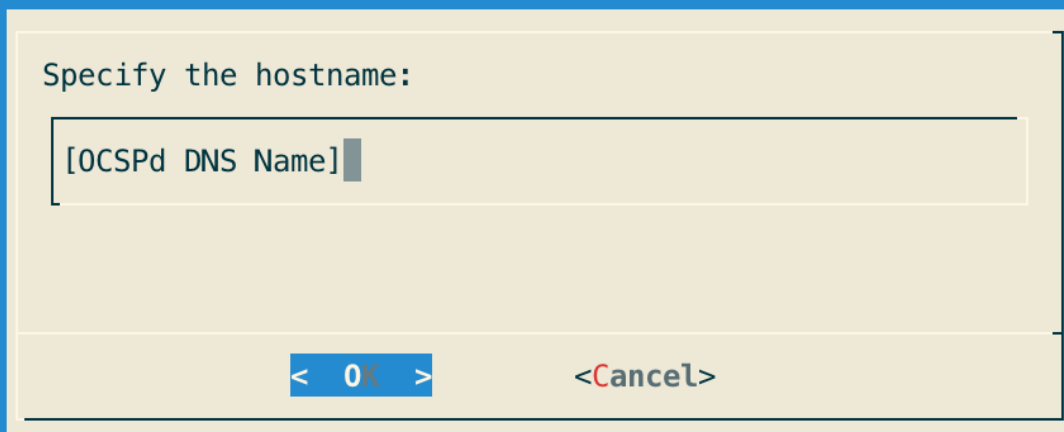
Step 3: In the main menu, select 'NGINX':



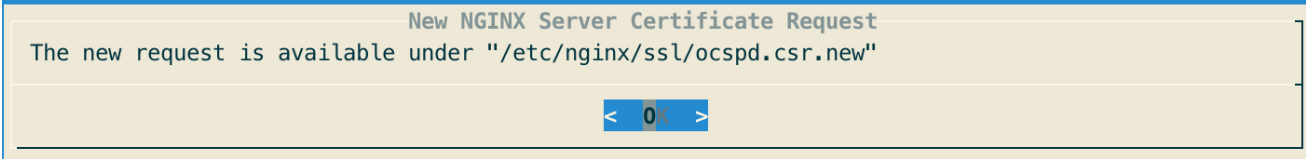
Step 4: In the NGINX menu, select 'CSR':



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'`:

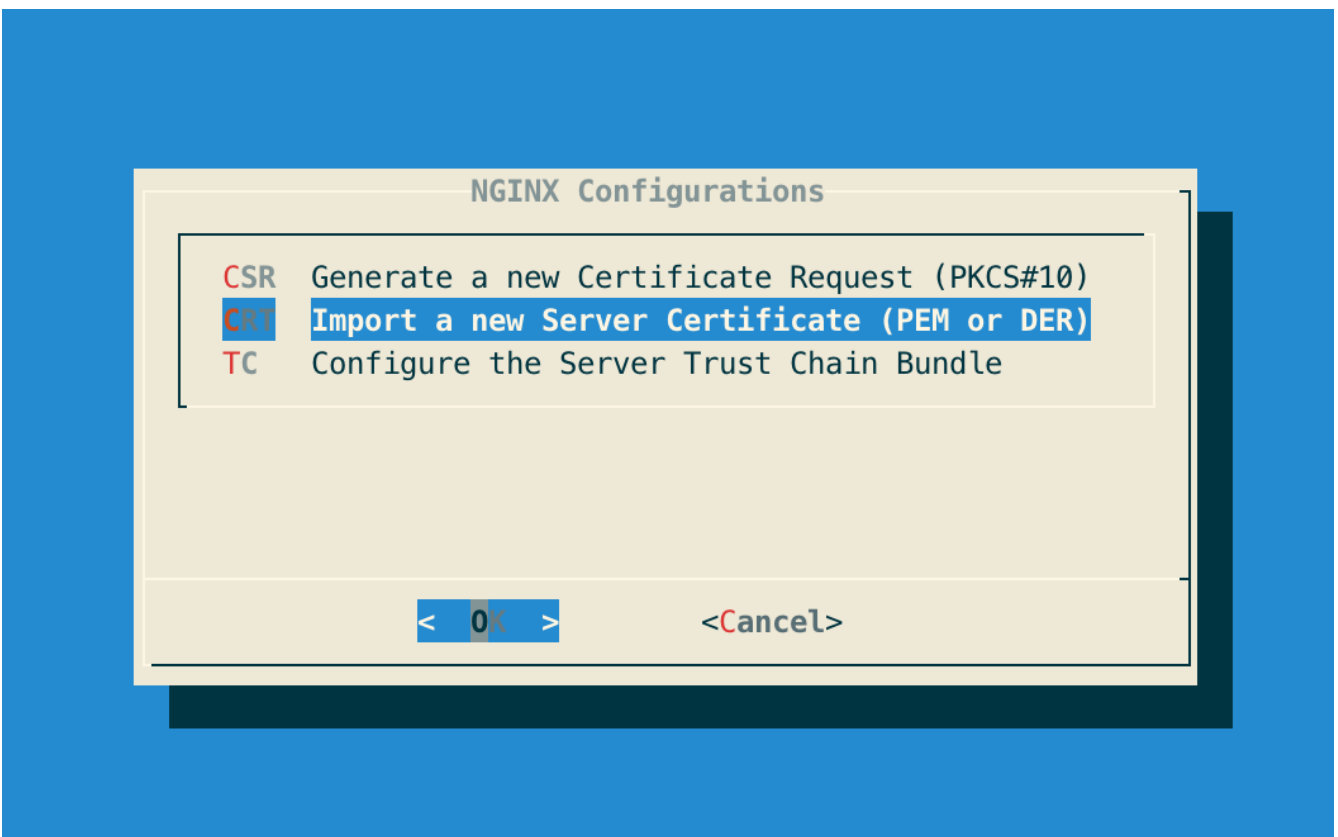


Step 7: Sign the certificate request using the corporate PKI.

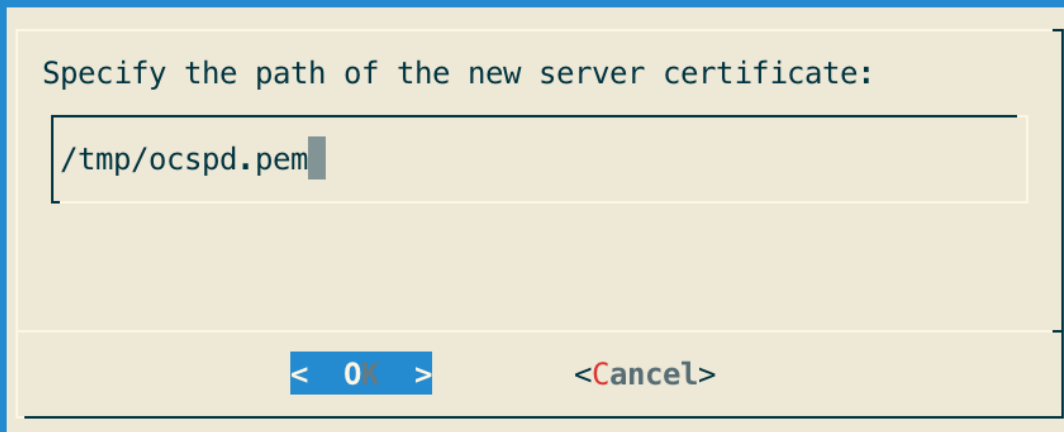
2.2.2. Installing a Server Certificate

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

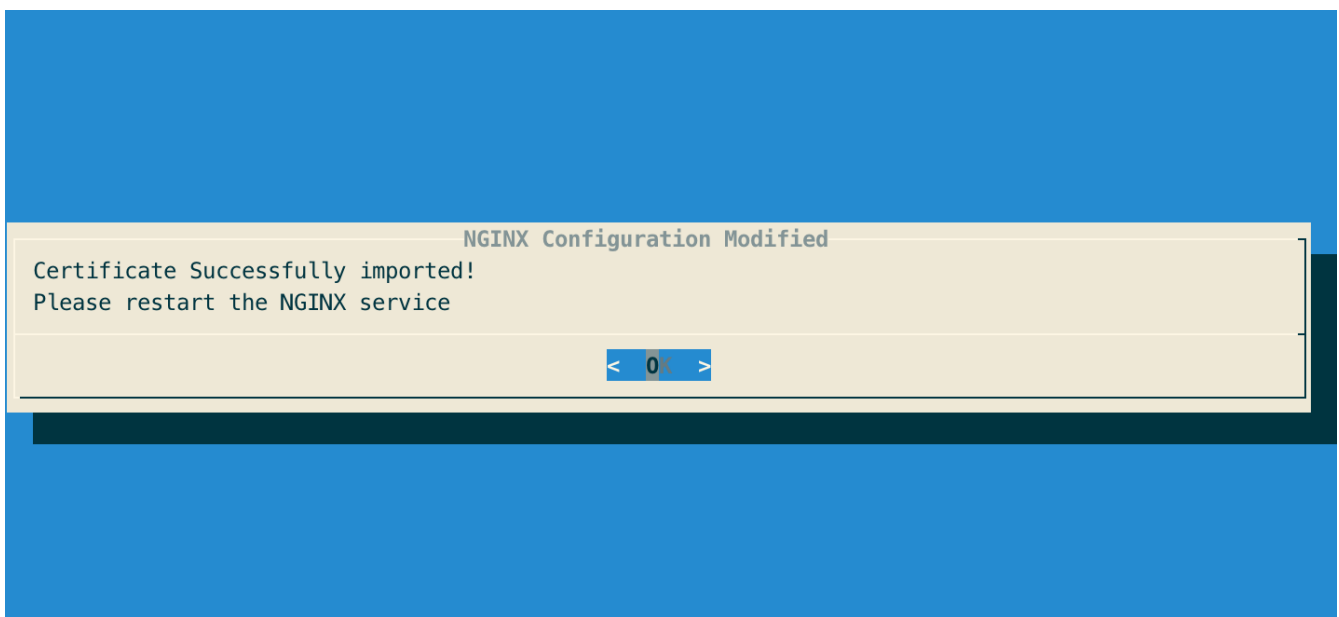
Step 2: In the NGINX configuration menu, select 'CRT':



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
```

3. Initial Management Console Access and Logout

3.1. Management Console Access

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

NOTE

Default credentials are:

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

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



Welcome to EverTrust OCSP Management Console

Username

Password

[Reset password](#)

Step 3: The Web Management Console is displayed:

Configuration

- Certification Authorities
- CRL Cache
- Signers
- Hardware Security Modules

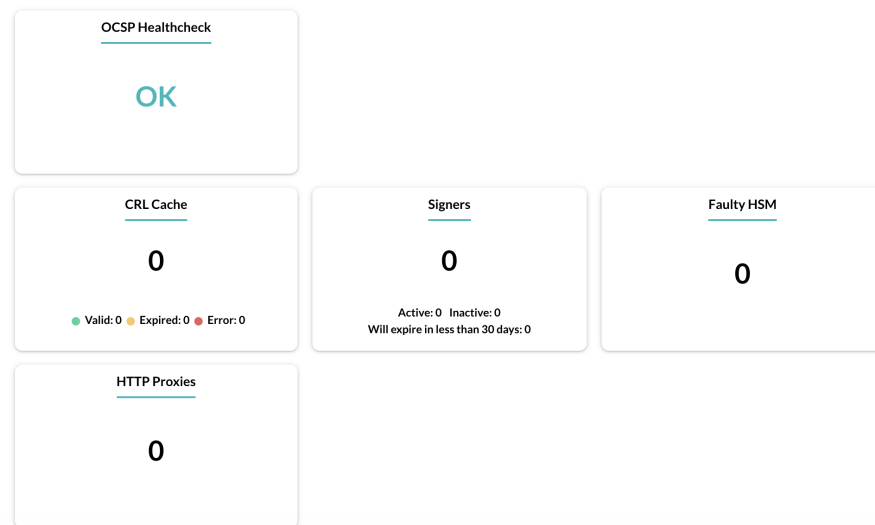
Permissions

- Administrators
- Roles

System

- Backup
- Restore
- Logs
- HTTP Proxies

Welcome administrator,

**CAUTION**

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).

3.2. Management Console Logout

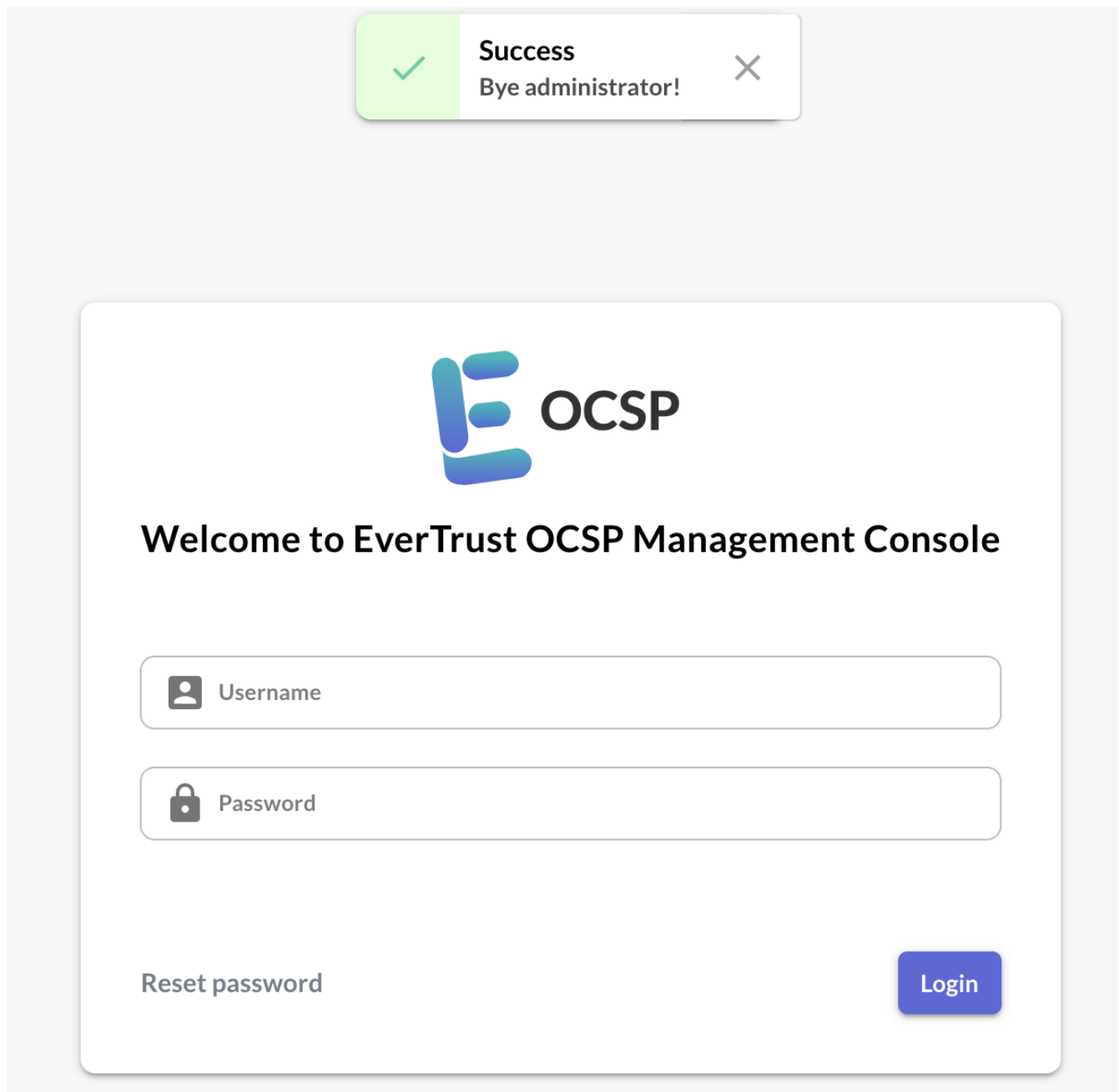
3.2.1. Logout when logged in with Password (Local, Radius or LDAP)

Step 1: Hit 'Logout' in the header:



Profile About English ▼ Logout

Step 2: The Administrator is successfully logged out:



Logout when logged in with Certificate

NOTE

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

4. Administrator Profile

4.1. Account Information

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



[Profile](#) [About](#) [English](#) ▾ [Logout](#)

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

You'll find below your account information:

Username

administrator

Email

administrator@evertrust.fr

Certificate DN

Authentication Type

Password

You are not member of any role.

You own the following permissions:

Manage

Audit

System

Local Password *



Confirm Local Password *



Change Password

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.

4.2. Resetting Password

WARNING

- 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**'.

NOTE

The password must be compliant with the Password Policy defined.


TIP


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:

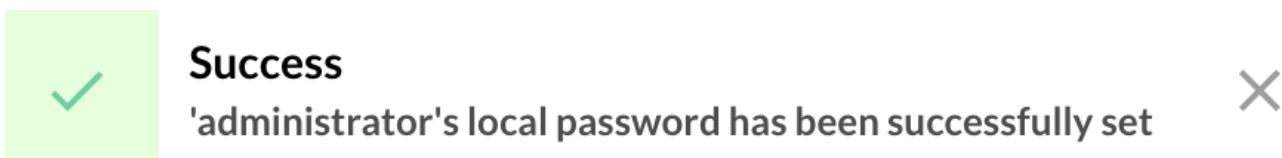


Step 4: Specify the Administrator password (double input) and hit the '**Change Password**' button:





Step 5: The Administrator password is set / reset:



5. Managing Administrators

5.1. Creating an Administrator

CAUTION

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.

TIP

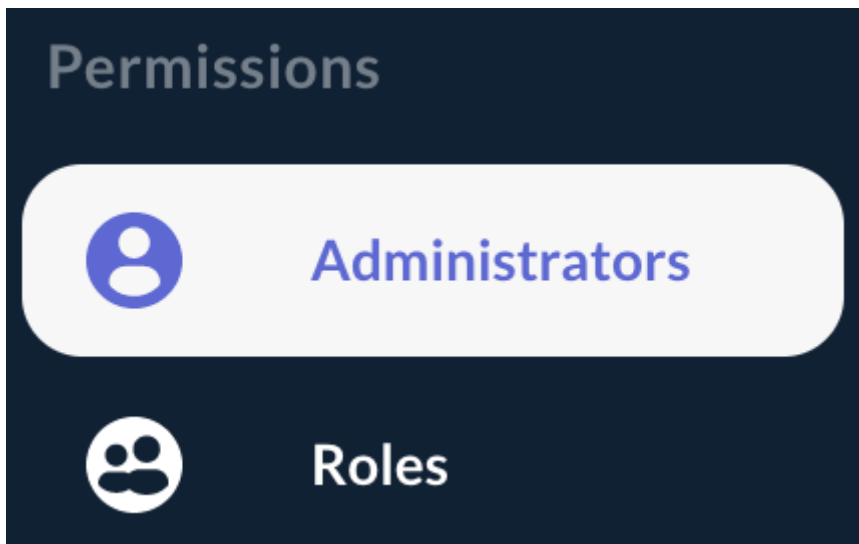
Administrators can be declared:

- Manually;
- By providing a certificate.

5.1.1. 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.

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

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

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

Username *
jjalvado

Email *
jja@evertrust.fr

Certificate DN 

Authentication Type *
Password

Roles

Please select the following rights you want to affect to the administrator:

- Manage Certification Authorities
- Audit Certification Authorities
- Manage Signers
- Audit Signers
- Manage HSMs
- Audit HSMs
- Manage Permissions
- Audit Permissions
- Backup
- Restore
- Logs Access
- Manage HTTP Proxies
- Audit HTTP Proxies

Cancel 

Step 5: The Administrator is successfully created:



Success
'jjalvado' successfully created



Administrators Search

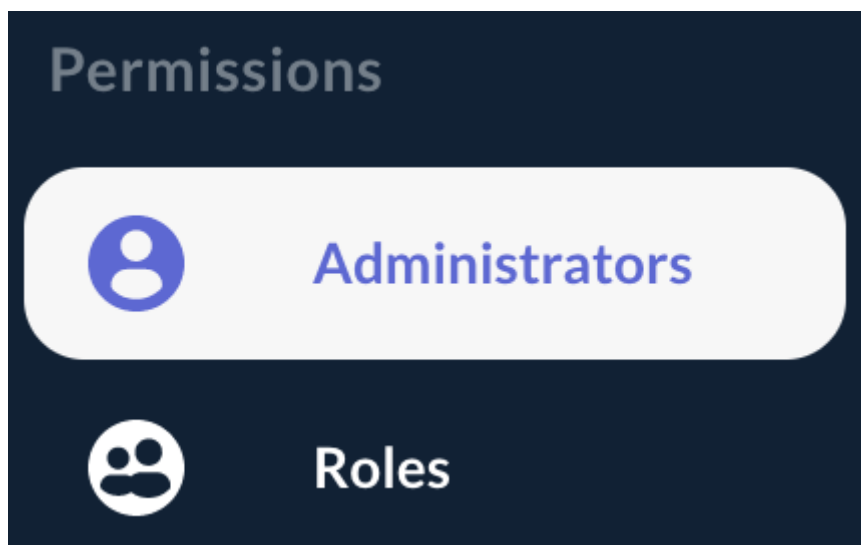
| Username | Email | Certificate DN | Authentication Type | Roles | |
|---------------|----------------------------|----------------|---------------------|-------|--|
| administrator | administrator@evertrust.fr | - | Password | - | |
| jjalvado | jj@evertrust.fr | - | Password | - | |

Records per page: 10 |< < 1/1 > >| +

5.1.2. 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:



Please select the following rights you want to affect to the administrator:

Manage Certification Authorities

Audit Certification Authorities

Manage Signers

Audit Signers

Manage HSMs

Audit HSMs

Manage Permissions

Audit Permissions

Backup

Restore

Logs Access

Manage HTTP Proxies

Audit HTTP Proxies

Cancel

Add

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

Please select the Administrator Certificate to upload (PEM or DER format)

Browse
jjalvado.pem  

Cancel

Submit



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:

Username *
jjalvado

Email *
jja@evertrust.fr

Certificate DN
CN=Jean-Julien Alvado, OU=Users, O=EverTrust, C=FR  

Authentication Type *
X509 

Roles 

Please select the following rights you want to affect to the administrator:

- Manage Certification Authorities
- Audit Certification Authorities
- Manage Signers
- Audit Signers
- Manage HSMs
- Audit HSMs
- Manage Permissions
- Audit Permissions
- Backup
- Restore
- Logs Access
- Manage HTTP Proxies
- Audit HTTP Proxies

Cancel

Update

Step 6: The Administrator is successfully created:



Success

'jjalvado' successfully created



| Administrators | | | | | Search |
|----------------|----------------------------|--|---------------------|-------|--------|
| Username | Email | Certificate DN | Authentication Type | Roles | |
| administrator | administrator@evertrust.fr | - | Password | - | |
| jjalvado | jjalvado@evertrust.fr | CN=Jean-Julien Alvado, OU=Users, O=EverTrust, C=FR | X509 | - | |

Records per page: 10 |< < 1/1 > >|

5.2. Setting Administrator Password Policy

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

WARNING

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
```

5.3. Editing or deleting Administrators

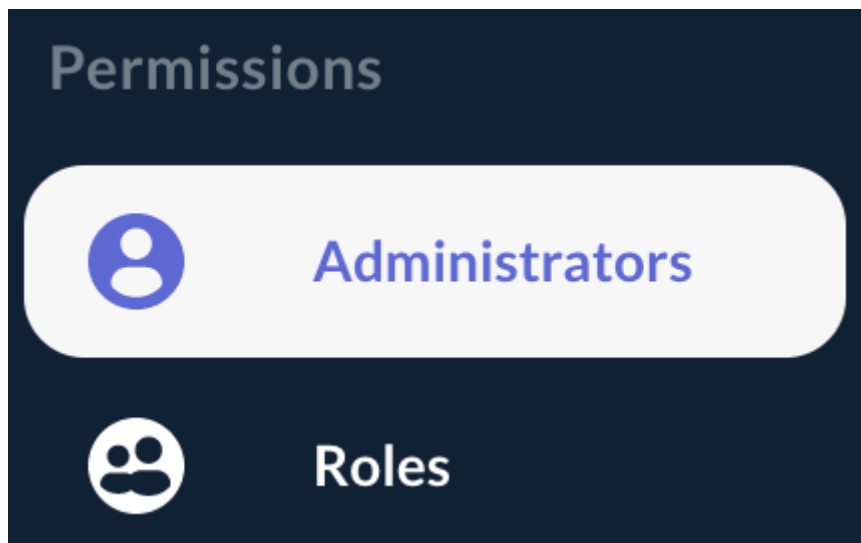
5.3.1. Editing an Administrator

NOTE

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:

jjalvado

jjja@evertrust.fr

-

Password


-



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

Username *
jjalvado

Email *
jja@evertrust.fr

Certificate DN 

Authentication Type *
Password

Roles

Please select the following rights you want to affect to the administrator:

- Manage Certification Authorities
- Audit Certification Authorities
- Manage Signers
- Audit Signers
- Manage HSMs
- Audit HSMs
- Manage Permissions
- Audit Permissions
- Backup
- Restore
- Logs Access
- Manage HTTP Proxies
- Audit HTTP Proxies

Cancel

Update

Step 5: The Administrator is successfully updated:



Success

'jjalvado' successfully updated



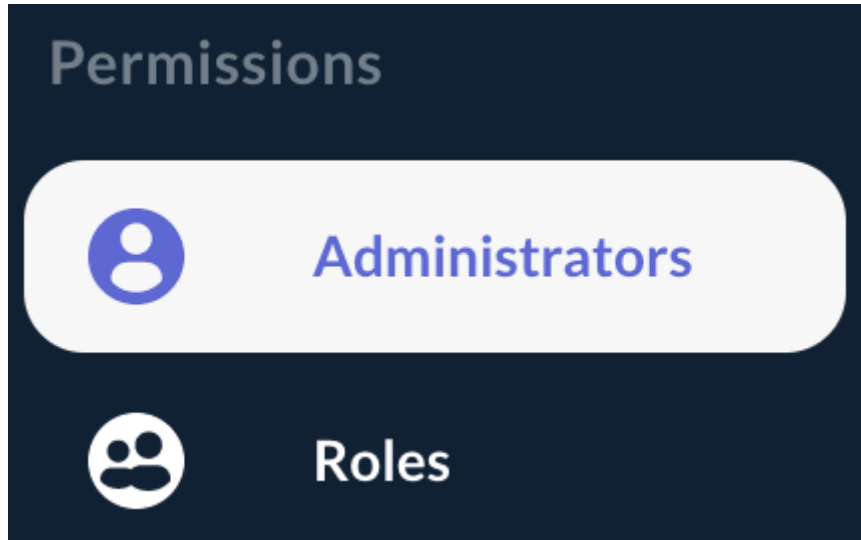
5.3.2. Deleting an Administrator

WARNING

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

Step 1: Access the OCSPd Web Management Console;

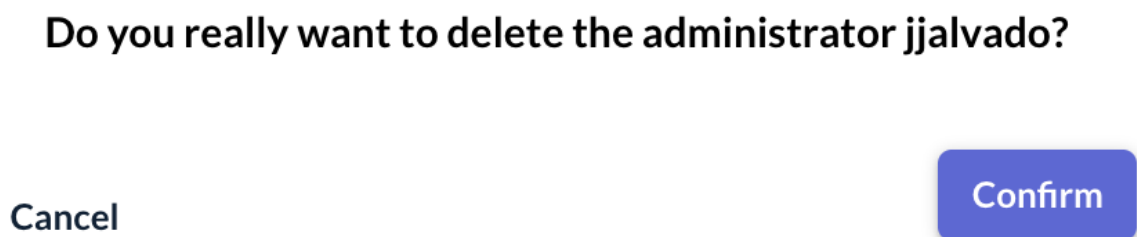
Step 2: In the 'Permissions' left menu, select 'Administrators':



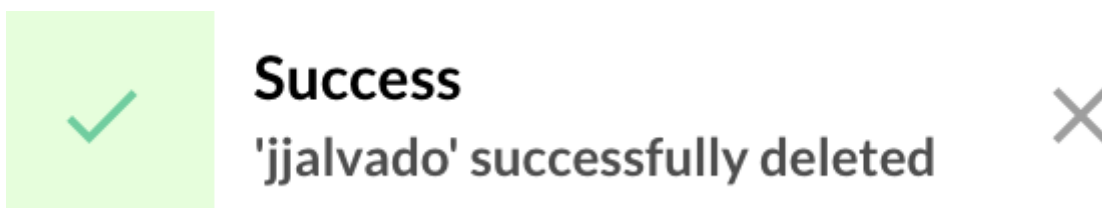
Step 3: Hit the  button of the Administrator you are willing to delete:



Step 4: Hit the 'Confirm' button:



Step 5: The Administrator is successfully deleted:



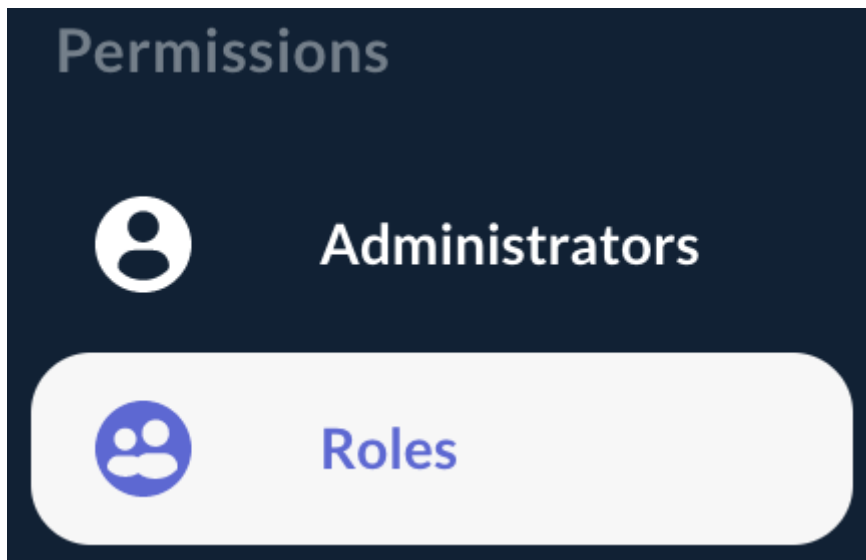
6. Managing Roles

This section details how to manage OCSPd Roles.

6.1. 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.

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

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

Name *

Auditor

Description

Can audit all modules

Please click on the rights you want to affect to this role:

Manage Certification Authorities

✓ Audit Certification Authorities

Manage Signers

✓ Audit Signers

Manage HSMs

✓ Audit HSMs

Manage Permissions

✓ Audit Permissions

Backup

Restore

Logs Access

Manage HTTP Proxies

✓ Audit HTTP Proxies

Cancel

Add

Step 5: The Role is successfully created:




Success




'Auditor' successfully created





Role

Search 

| Name | Description | Permissions | |
|------|-------------|-------------|--|
|------|-------------|-------------|--|

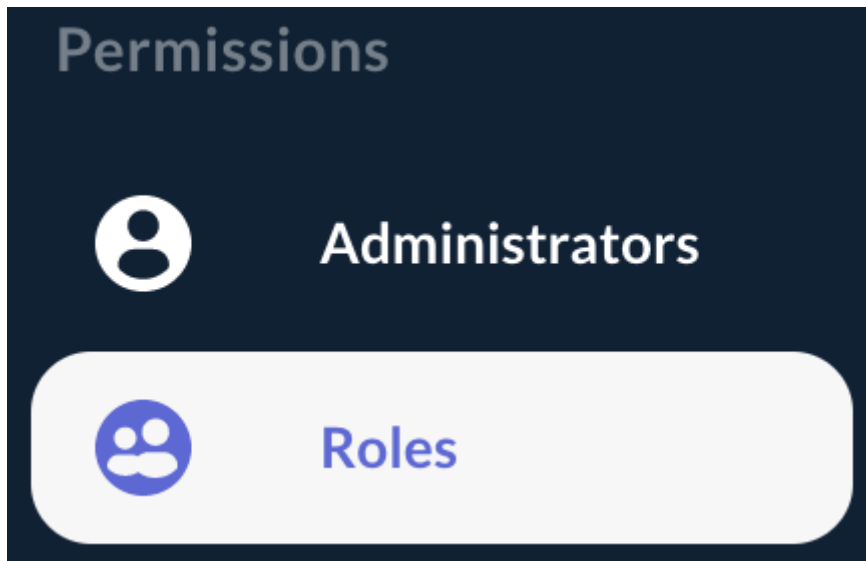
| | | | |
|---------|-----------------------|--|---|
| Auditor | Can audit all modules | Audit System |    |
|---------|-----------------------|--|---|

Records per page: 10  |< < 1/1 > >| 

6.2. 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:

Auditor

Can audit all modules

Audit

System



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

Name *

Auditor

Description

Can audit all modules

Please click on the rights you want to affect to this role:

Manage Certification Authorities

✓ Audit Certification Authorities

Manage Signers

✓ Audit Signers

Manage HSMs

✓ Audit HSMs

Manage Permissions

✓ Audit Permissions

Backup

Restore

Logs Access

Manage HTTP Proxies

✓ Audit HTTP Proxies

Cancel

Update

Step 5: The Role is successfully updated:



Success

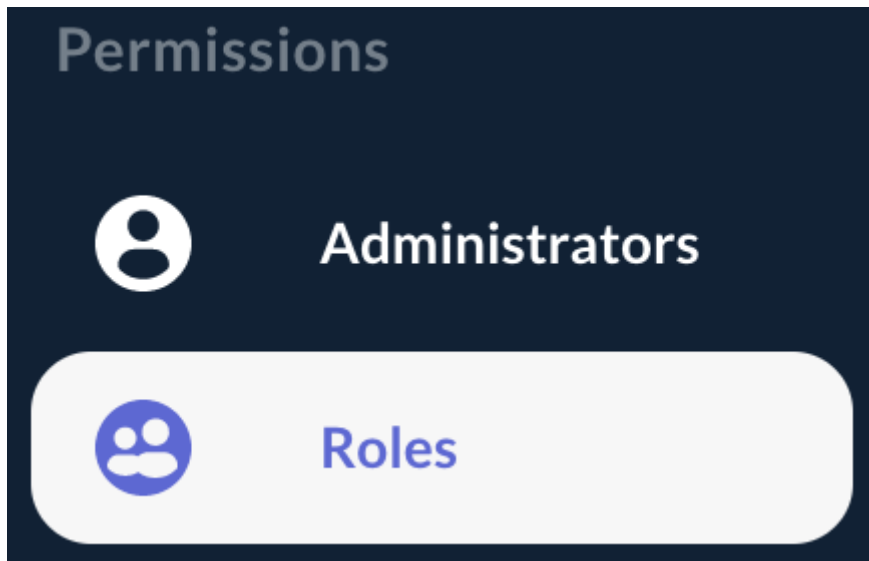
'Auditor' successfully updated




6.3. Display and manage Members of a Role


Step 1: Access the OCSPd Web Management Console;

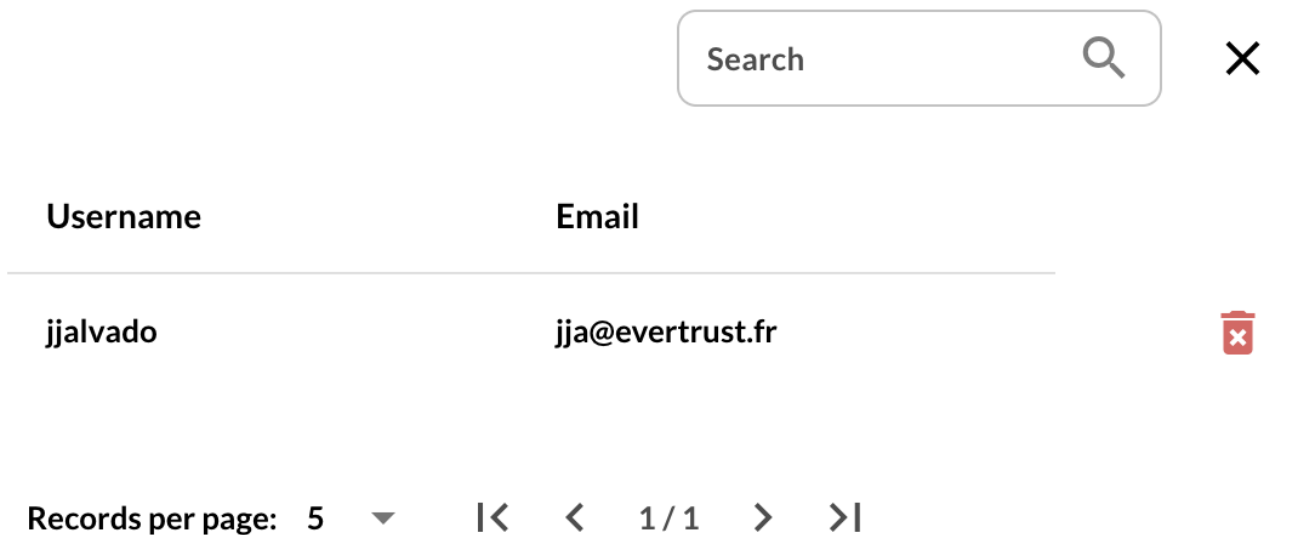
Step 2: In the 'Permissions' left menu, select 'Roles':



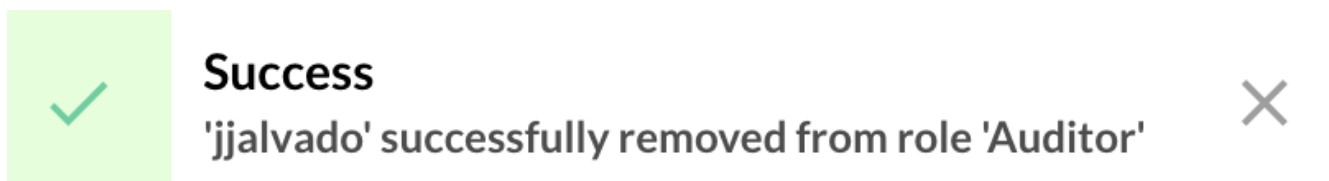
Step 3: For the Role you want to see the Members, hit the  button:



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



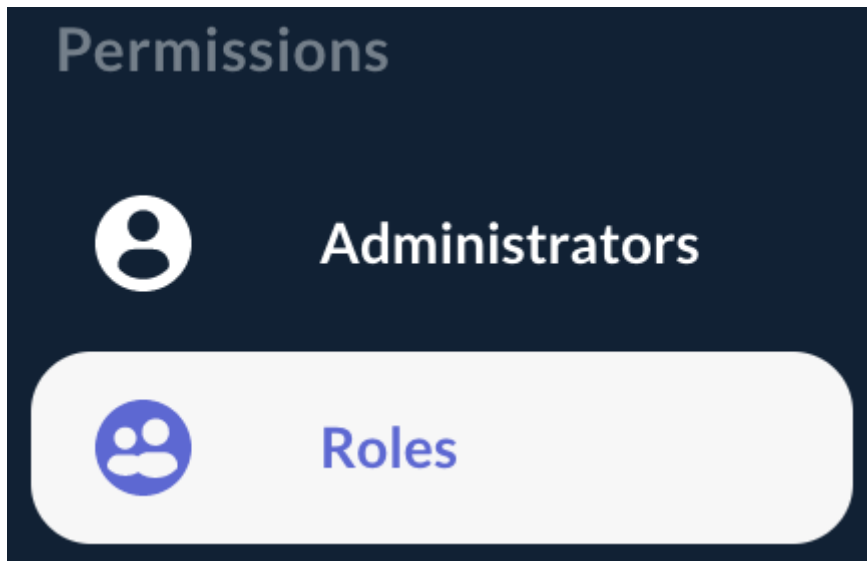
Step 5: The Administrator is successfully removed from the Role:



6.4. 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:



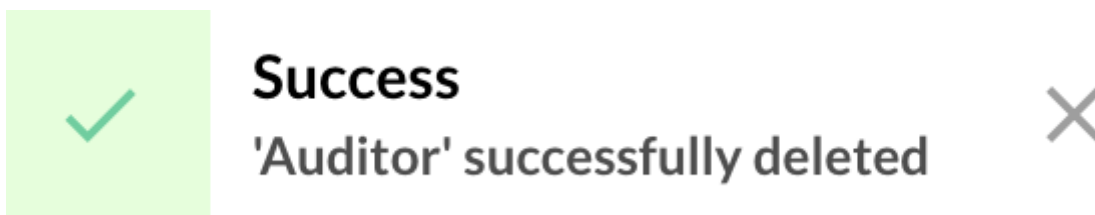
Step 4: Hit the 'Confirm' button:

Do you really want to delete the role Auditor?

Cancel

Confirm

Step 5: The Role is successfully deleted:



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.

7.1. Supported Hardware Security Modules

As of today, OCSPd has been successfully tested 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.

IMPORTANT

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.

7.2. Managing Modules

7.2.1. Registering a Module

CAUTION

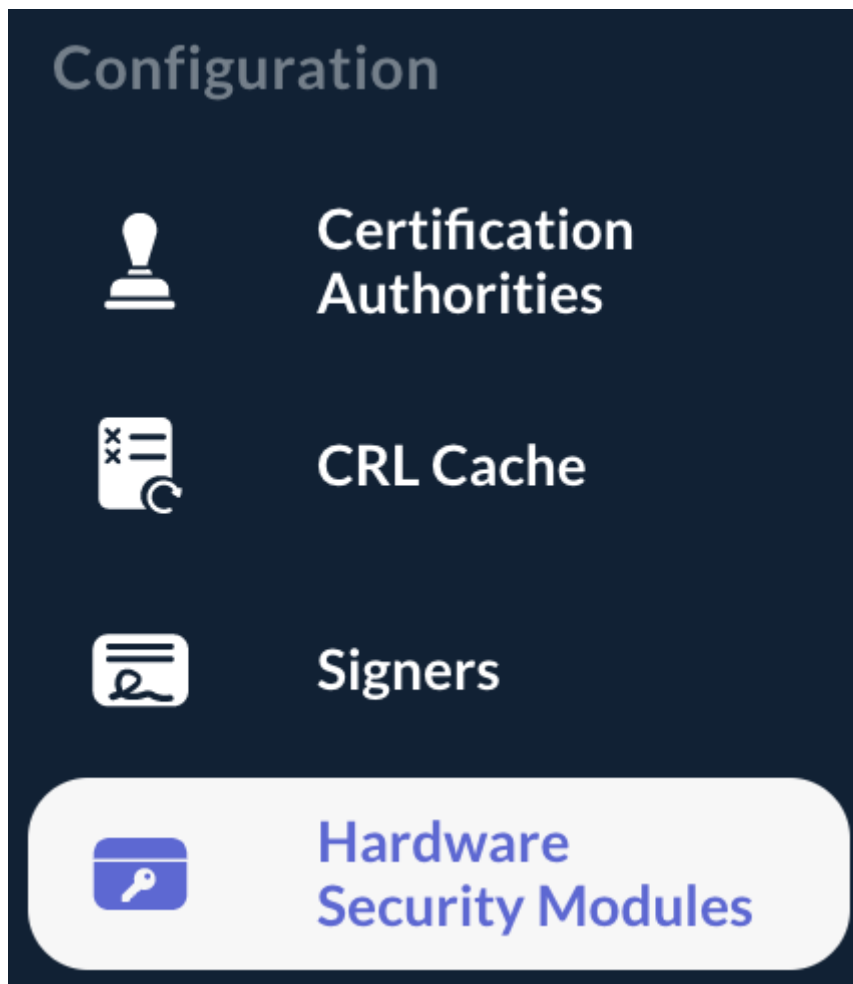
Initializing the PKCS#11 module must be performed using the tools provided by the HSM provider.

NOTE

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:


Name *
SoftHSMv2

Description
Software HSM v2

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


Cancel Register

Step 5: The PKCS#11 module is registered:



Success

'SoftHSMv2' successfully registered







Hardware Security Module

SoftHSMv2 ●

Software HSM v2

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

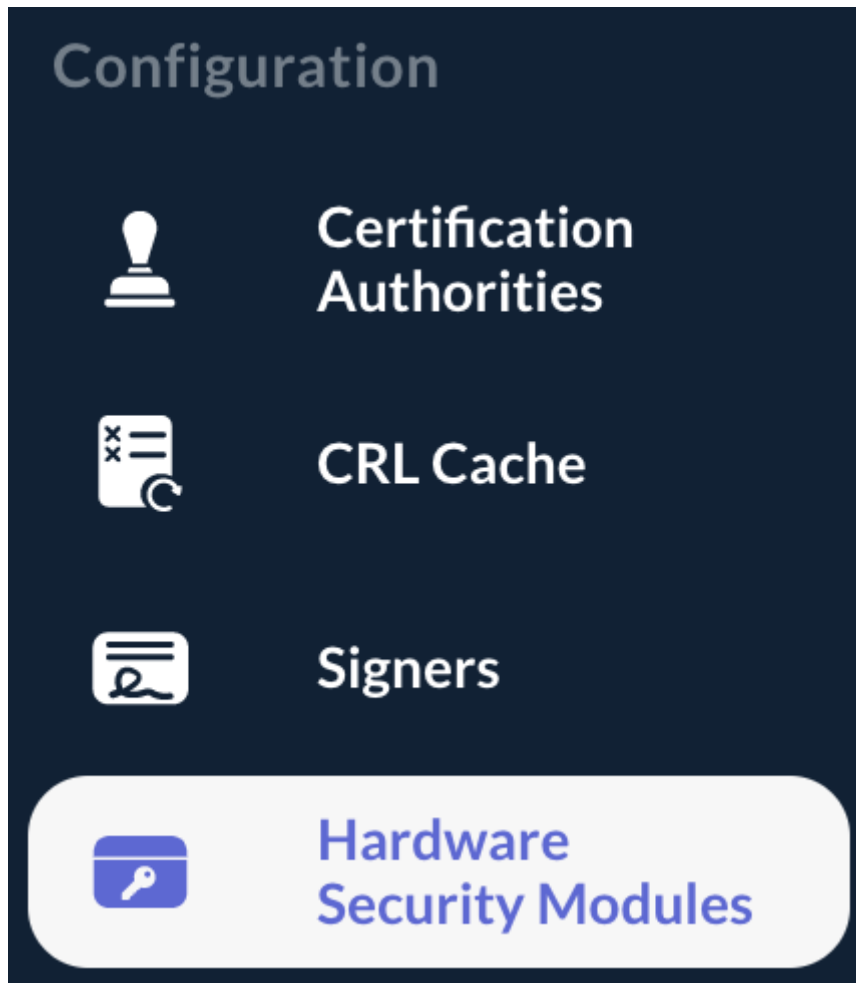
  



7.2.2. Editing a Module

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:

SoftHSMv2 

Software HSM v2

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



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

Name *

SoftHSMv2

Description

Software HSM v2

Library *

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

Cancel

Update

Step 5: The Module is successfully updated:



Success

'SoftHSMv2' successfully updated



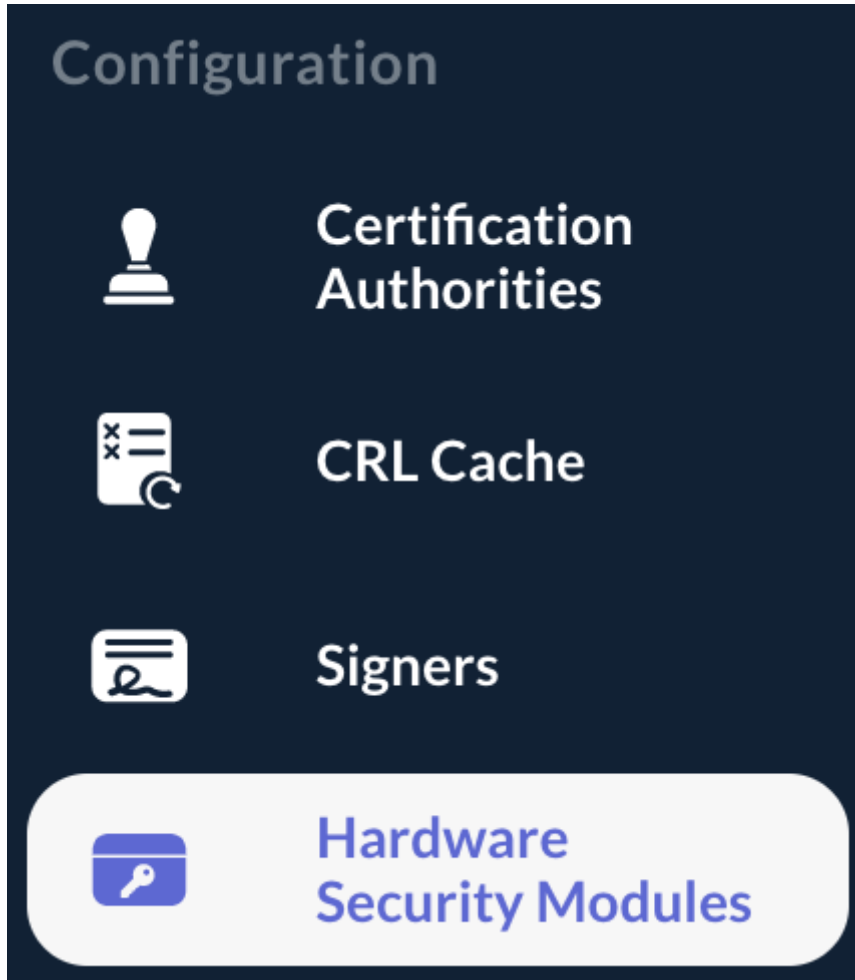
7.2.3. Unregistering a Module

WARNING

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:

SoftHSMv2 

Software HSM v2

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



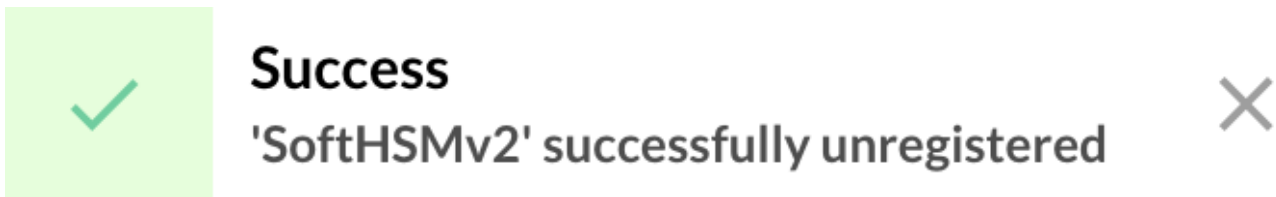
Step 4: Hit the 'Confirm' button:

Do you really want to unregister the HSM SoftHSMv2? No cryptographic material will be deleted if you proceed.

Cancel

Confirm

Step 5: The module is unregistered:



7.3. Managing HSM slots

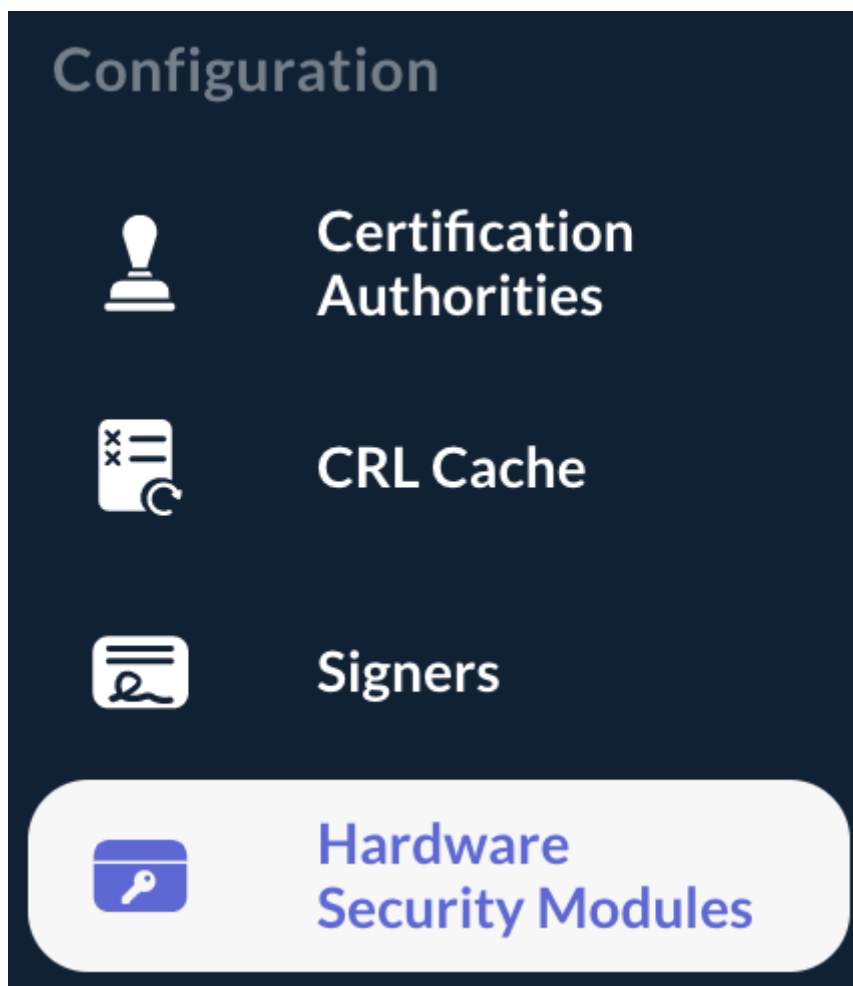
7.3.1. Registering a Slot

NOTE

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:

SoftHSMv2 ●

Software HSM v2

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



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:

HSM Name
SoftHSMv2

Slot ID *
0x31c6937c

PIN *
●●●●

Worker(s) *
1

Cancel Register

Step 5: The Slot is successfully registered:

Success

'0x31c6937c' successfully registered

×

SoftHSMv2 ●

Software HSM v2

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

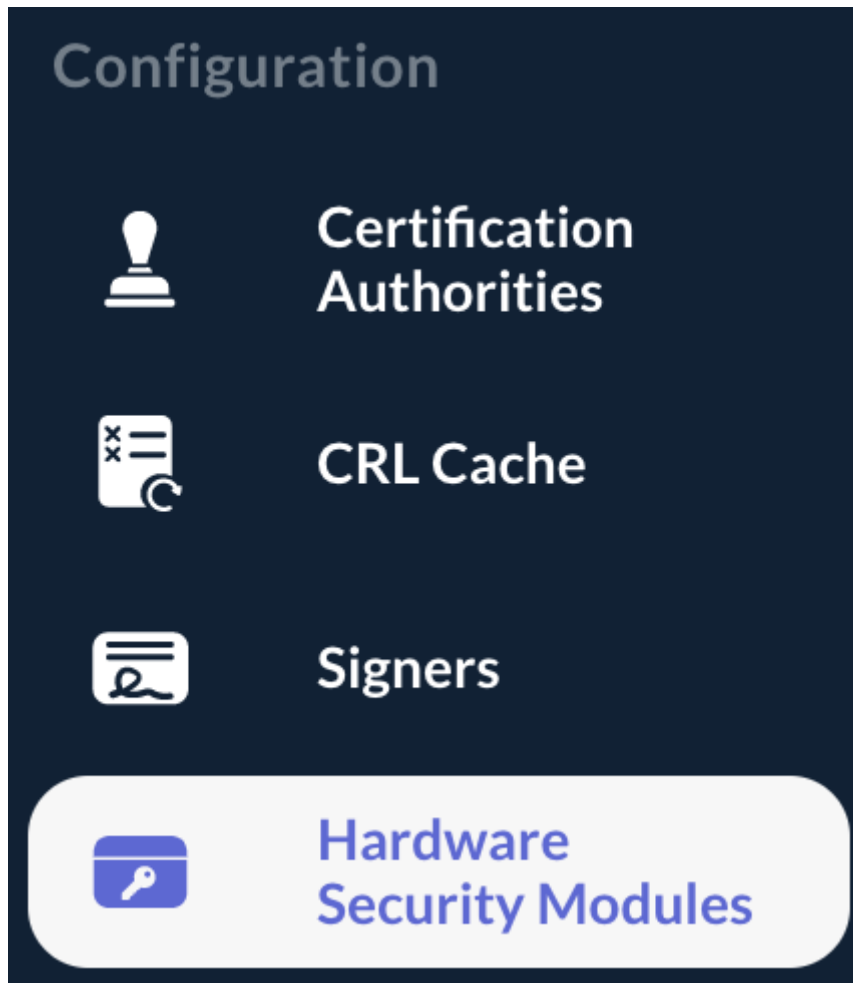
✎ + 🗑

| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) | |
|------------|--------------------|--------|-----------|--|
| 0x31c6937c | ✕ | ● | 1 | 🔒 🔧 🗑 |

7.3.2. 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:

SoftHSMv2 

Software HSM v2

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



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

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

PIN *
●●●●



Confirm PIN *
●●●●



Cancel

Set

Step 5: The Slot PIN is successfully set:



Success

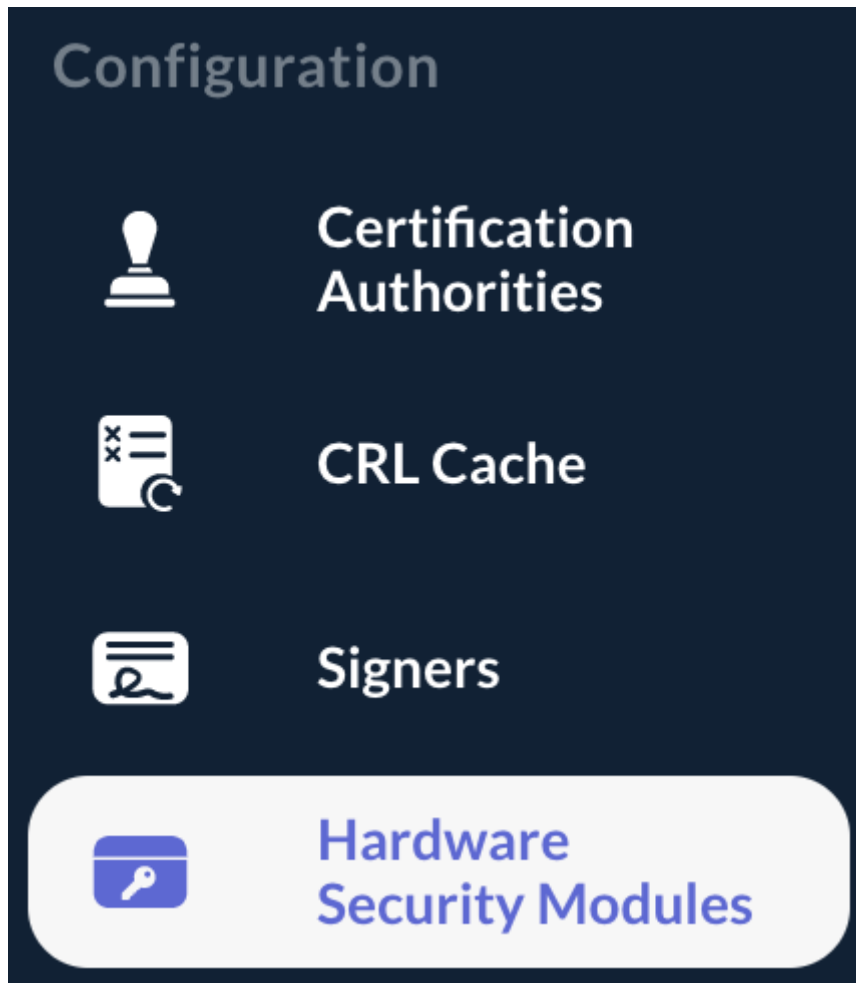
'0x31c6937c' successfully updated



7.3.3. 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):

SoftHSMv2 ●

Software HSM v2

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



| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) | |
|------------|--------------------------|--------------------------------------|-----------|---|
| 0x31c6937c | <input type="checkbox"/> | ● | 1 |    |

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

Worker(s) *
5

Cancel

Set

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



Success

'0x31c6937c' successfully updated



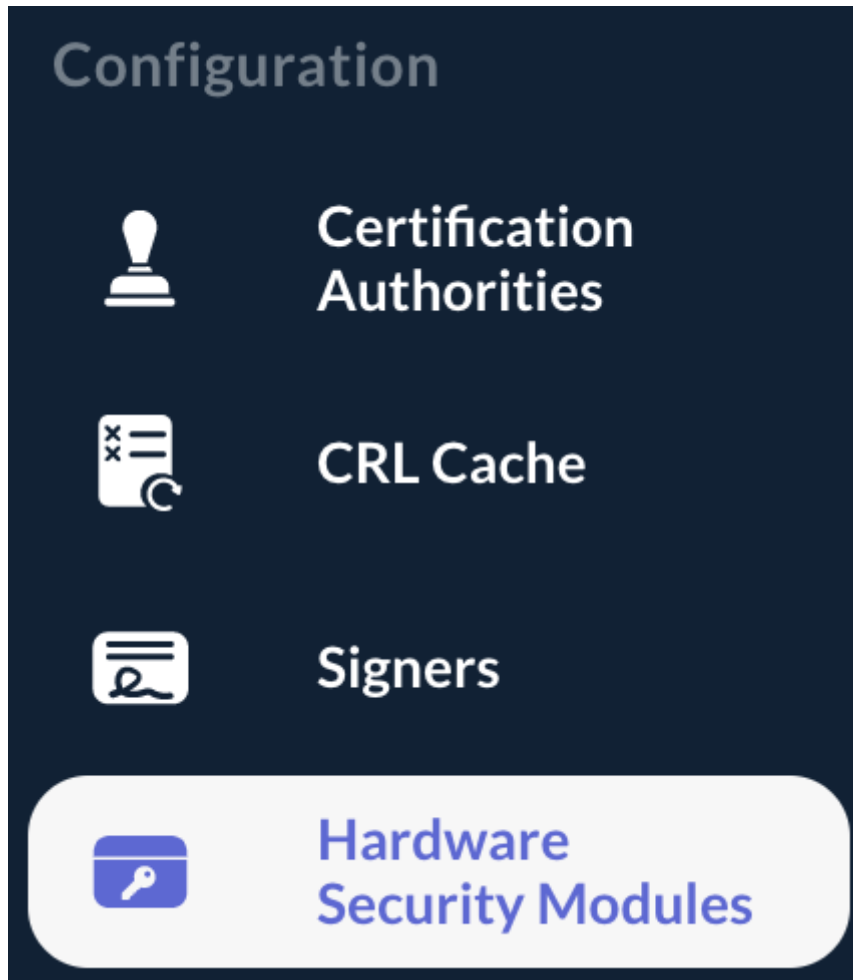
7.3.4. Unregistering a Slot

WARNING



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:

SoftHSMv2 ●   
Software HSM v2
`/usr/local/opt/softhsm/lib/softhsm/libsofthsm2.so`

| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) |
|------------|-------------------------------------|--------------------------------------|-----------|
| 0x31c6937c | <input checked="" type="checkbox"/> | ● | 1 |

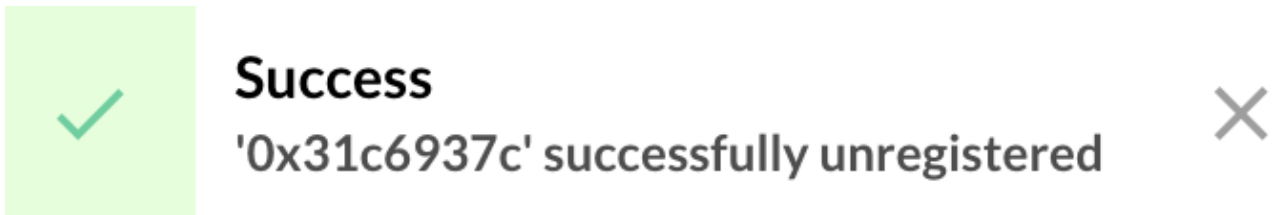
Step 4: Hit the 'Confirm' button:

Do you really want to unregister the slot 0x31c6937c? No cryptographic material will be deleted if you proceed.

Cancel

Confirm

Step 5: The Slot is successfully unregistered:



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

7.4.1. Enabling FIPS 140-2 Level 3 Key Generation Mode

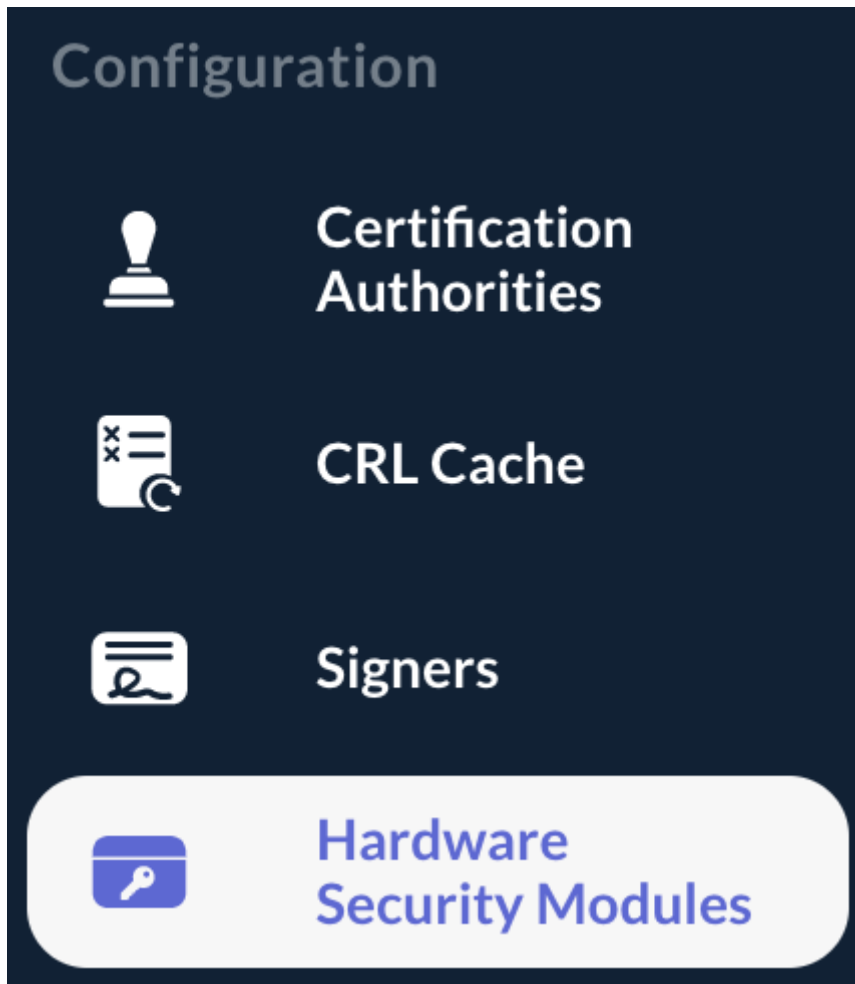
CAUTION

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:

SoftHSMv2 ●

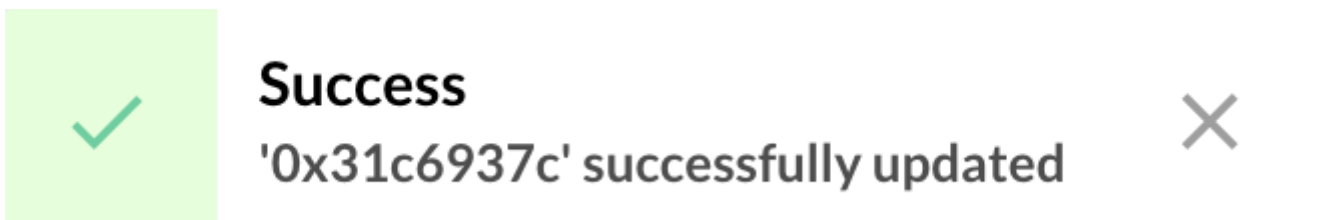
Software HSM v2

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



| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) | |
|------------|-------------------------------------|--------------------------------------|-----------|--|
| 0x31c6937c | <input checked="" type="checkbox"/> | ● | 1 | |

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

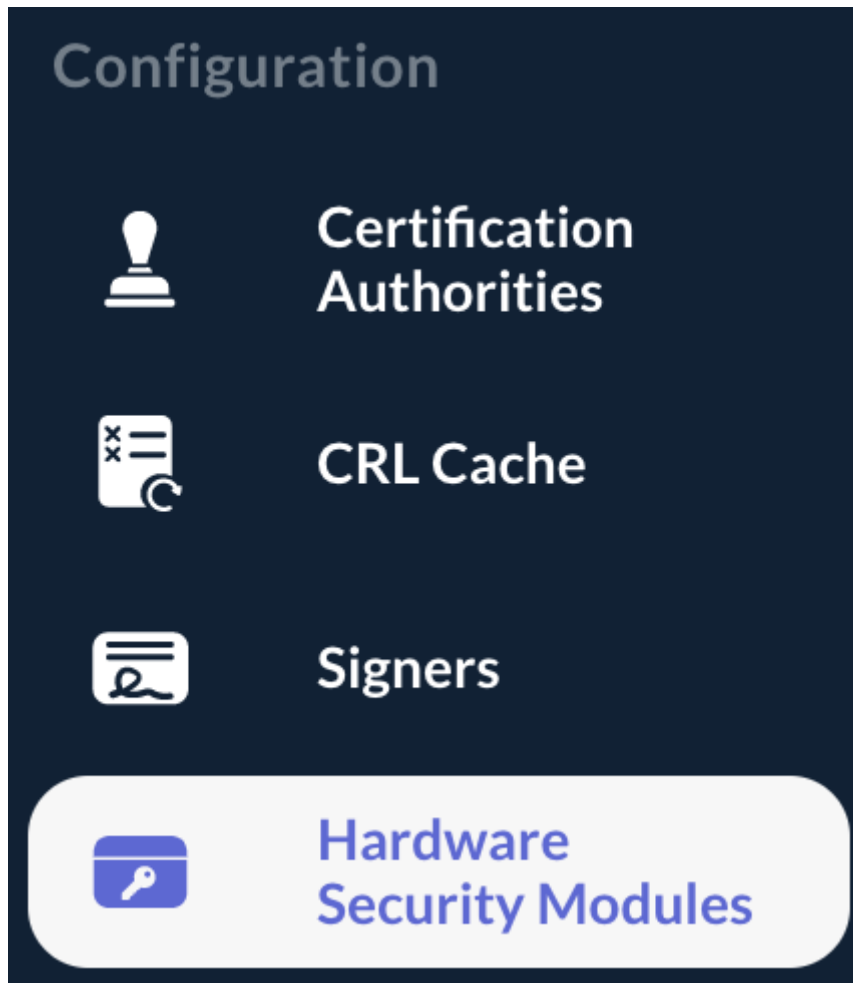



| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) | |
|------------|--------------------|--------------------------------------|-----------|--|
| 0x31c6937c | | ● | 1 | |





7.4.2. 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:

SoftHSMv2 
Software HSM v2
/usr/local/opt/softhsm/lib/softhsm/libsofthsm2.so   

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

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



Success

'0x31c6937c' successfully updated






SoftHSMv2



Software HSM v2

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



| Slot ID | FIPS 140-2 Level 3 | Status | Worker(s) | |
|------------|--------------------------|--------------------------------------|-----------|---|
| 0x31c6937c | <input type="checkbox"/> | ● | 1 |    |

7.5. HSM specifics

7.5.1. 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
```

7.5.2. Utimaco CryptoServer

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

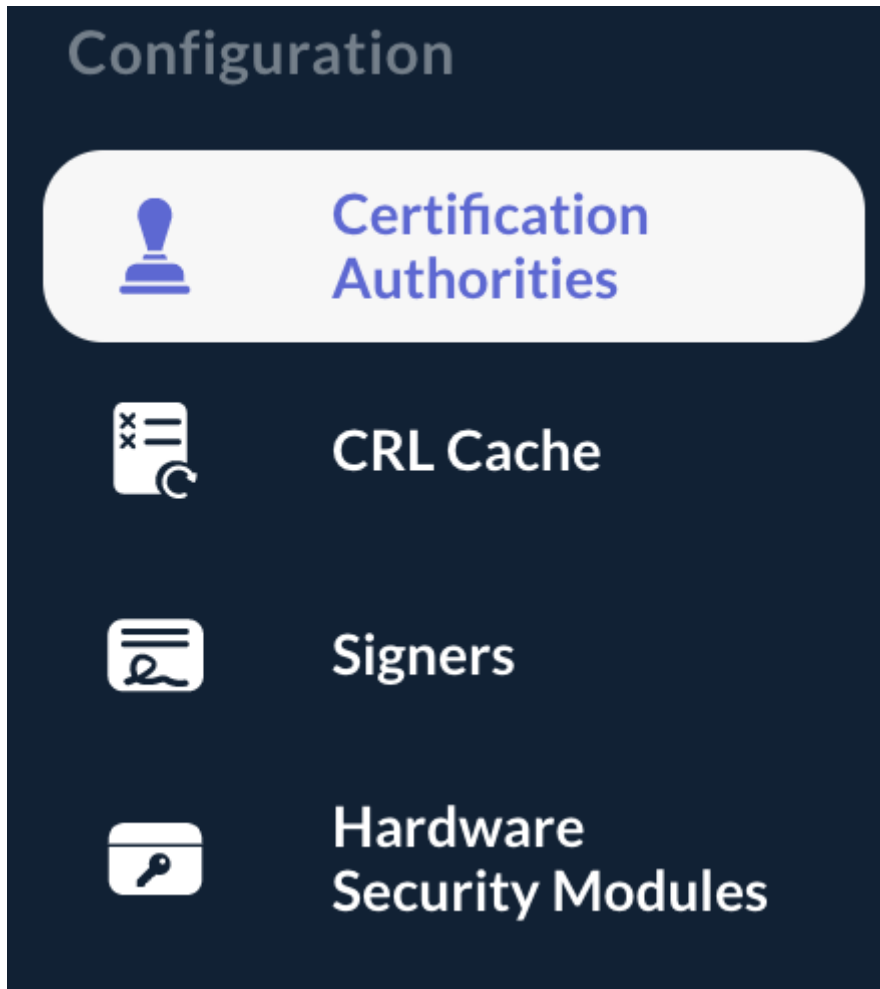
```
# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true
```

8. Managing Certificate Authorities

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:

Please select the CA certificate to register (PEM or DER format).

Browse
EverTrust_TCA.pem  

Cancel

Submit

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



Details



Conf



CRL

DN

CN=EverTrust Technical CA, O=EverTrust, C=FR

Issuer DN

CN=EverTrust Root CA, O=EverTrust, C=FR

Serial

0x5d0b9d09fdceb7ecb0abd669

Not Before

Mar 27, 2019 12:57 PM +01:00

Not After

Sep 20, 2038 01:57 PM +02:00

Cancel

Next

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 this 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.



CA Name *
EverTrust Technical CA

Is compromised?

Trusted for Authentication?

Enable OCSP?

Outdated Revocation Status Policy
Revoked

Default Signer

Back

Cancel

Next

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:



Details



Conf



CRL

CRL URL

http://pki.evertrust.fr/tsa.crl

CRL Name

tca

Refresh Period (in seconds)

300



Timeout (in milliseconds)

60



HTTP Proxy



Notify on CRL Expiration?



CRL Expiration Prior Notice Delay (in seconds)

43200

Notify On CRL Error?



Back

Cancel

Import

Step 9: The Certificate Authority is successfully imported:



Success

'EverTrust Technical CA' successfully created



Certification Authority

Search

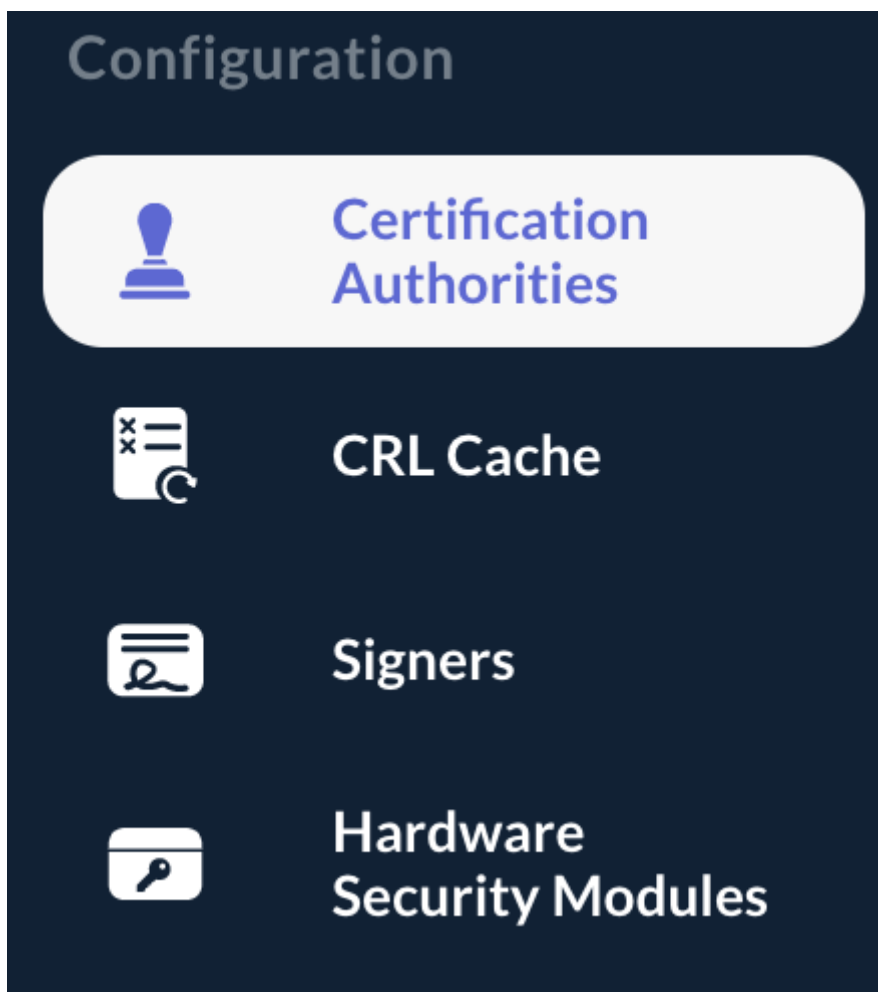
| Name | DN | Default Signer | |
|------------------------|--|----------------|--|
| EverTrust Technical CA | CN=EverTrust Technical CA, O=EverTrust, C=FR | - | |

Records per page: 10 |< < 1/1 > >|

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:

Configuration CRL Details

CA Name *
EverTrust Technical CA

Is compromised?

Trusted for Authentication?

Enable OCSP?

Outdated Revocation Status Policy
Revoked

Default Signer

Cancel **Update**

Step 5: The Certificate Authority is successfully updated:



8.3. CRL management

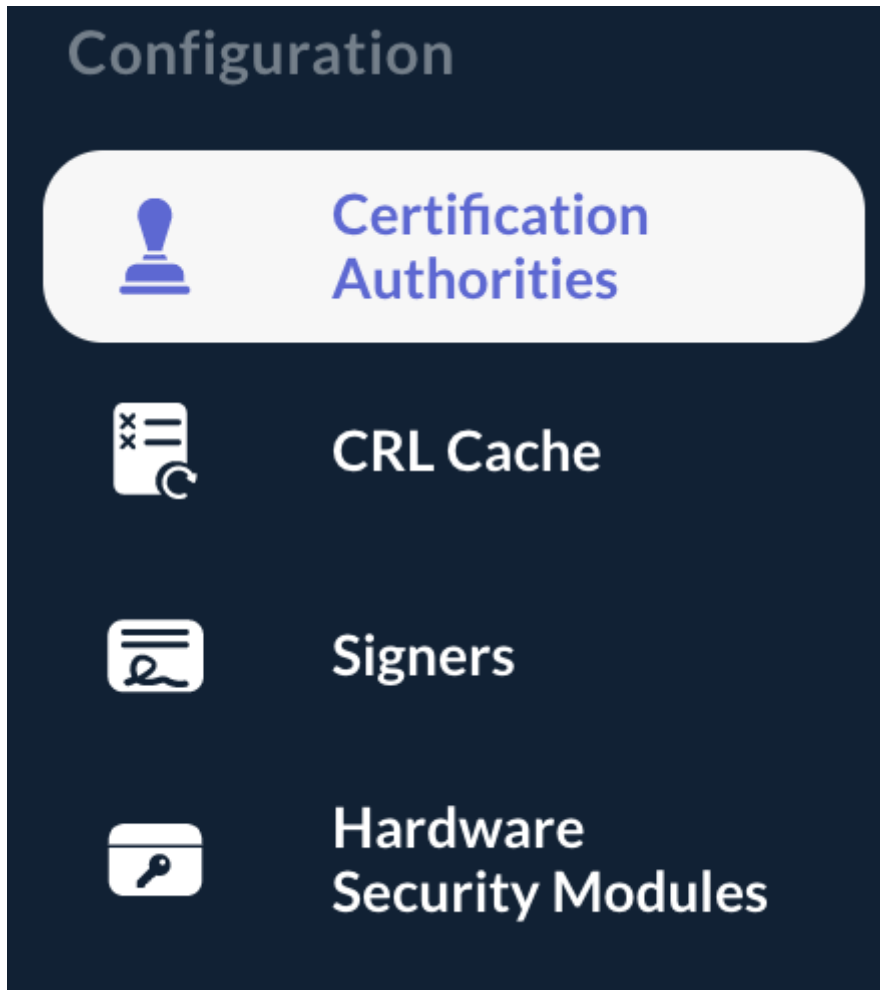
8.3.1. Forcing a CRL Refresh

NOTE

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':



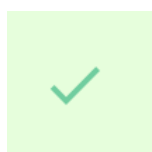
Step 3: Hit the  button of the Certificate Authority you are willing to refresh the CRL:

EverTrust Technical CA

CN=EverTrust Technical CA, O=EverTrust, C=FR



Step 4: The Certificate Authority CRL is successfully refreshed:



Success

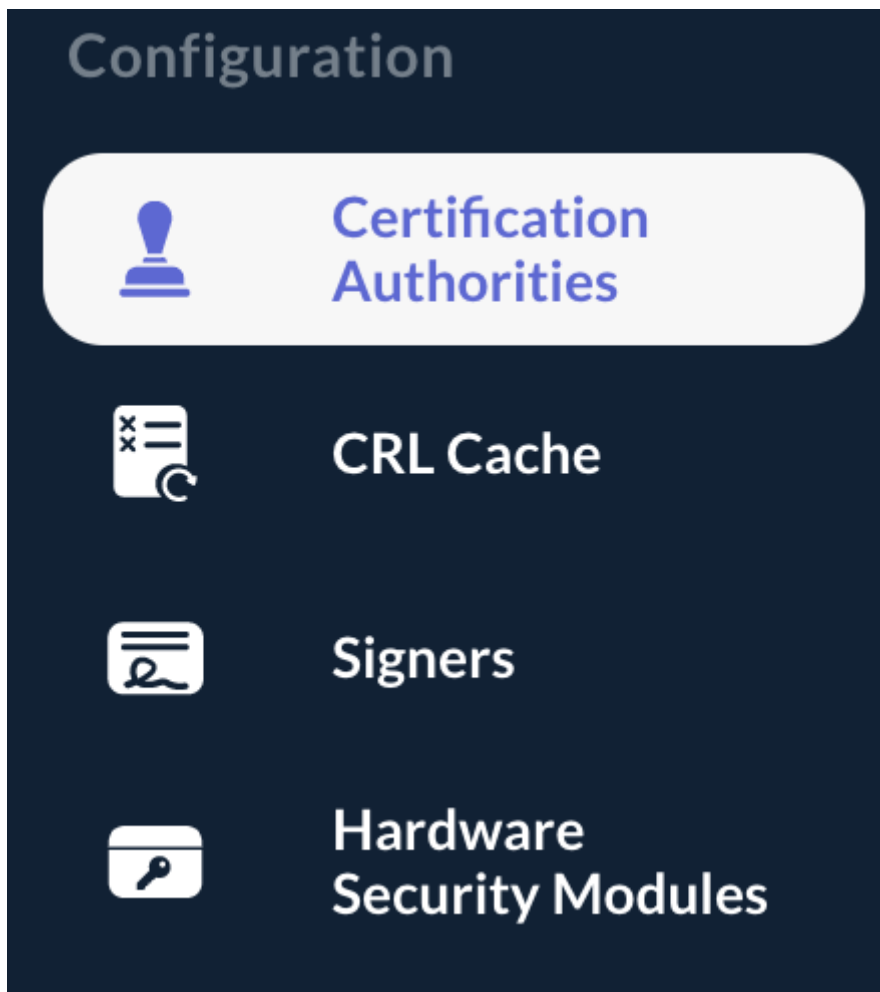
'EverTrust Technical CA' CRL has been successfully refreshed



8.3.2. 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:

EverTrust Technical CA

CN=EverTrust Technical CA, O=EverTrust, C=FR



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

Please select the CRL to upload (PEM or DER format)

Browse
tsa.crl  

Cancel

Submit

Step 5: The CRL is successfully uploaded:



Success

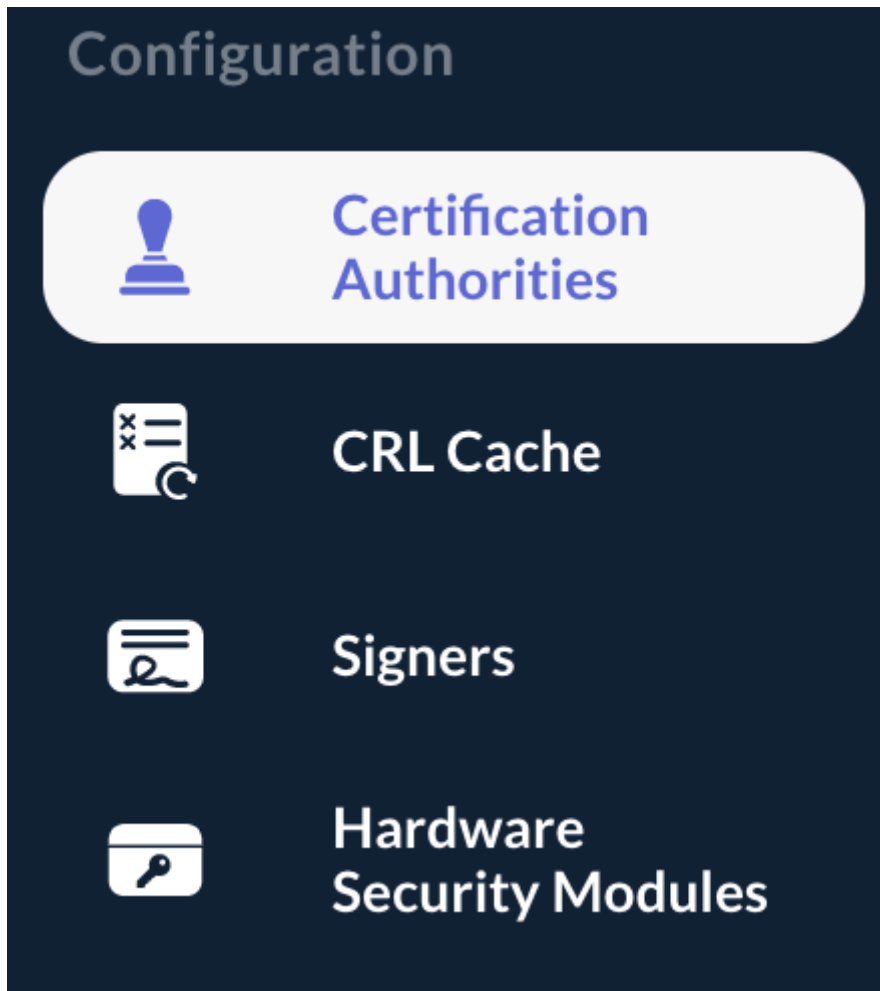
CRL successfully uploaded for 'EverTrust Technical CA'



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):

EverTrust Technical CA

CN=EverTrust Technical CA, O=EverTrust, C=FR

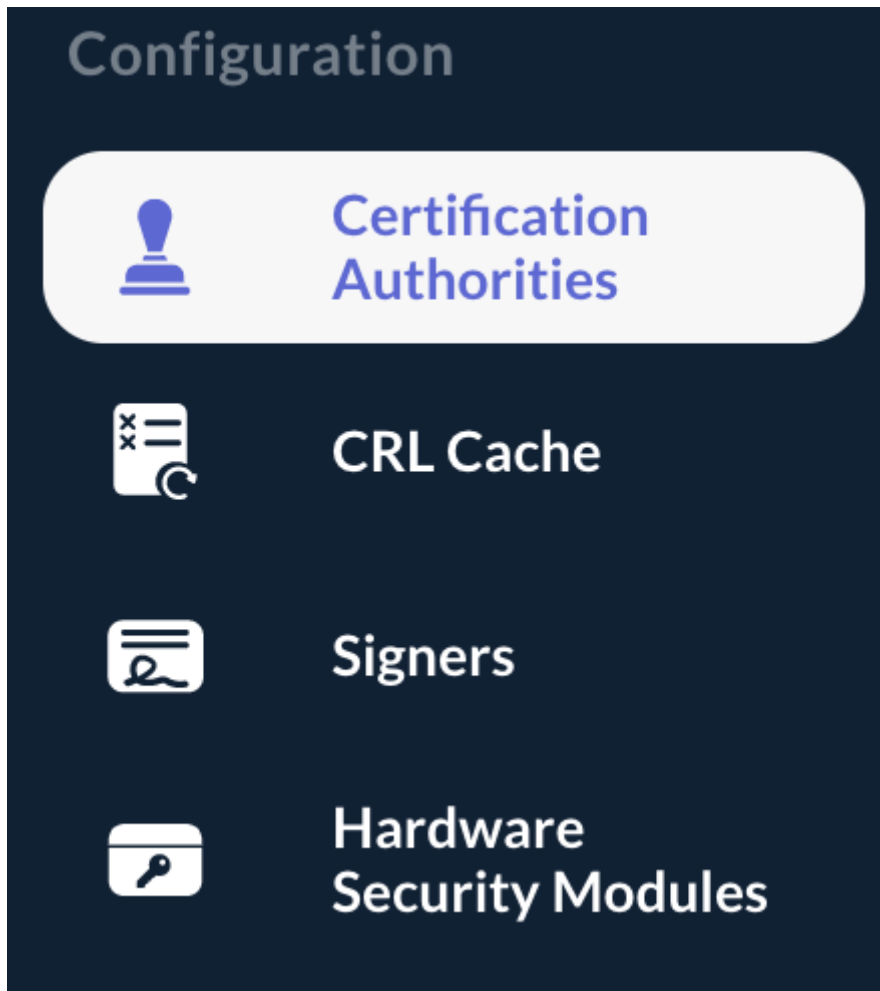


Step 4: The Certificate Authority's certificate is downloaded in PEM format.

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:

EverTrust Technical CA

CN=EverTrust Technical CA, O=EverTrust, C=FR



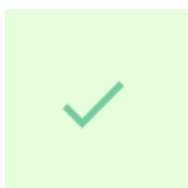
Step 4: Hit the 'Confirm' button:

Do you really want to delete the CA EverTrust Technical CA?

Cancel

Confirm

Step 5: The Certificate Authority is successfully deleted:



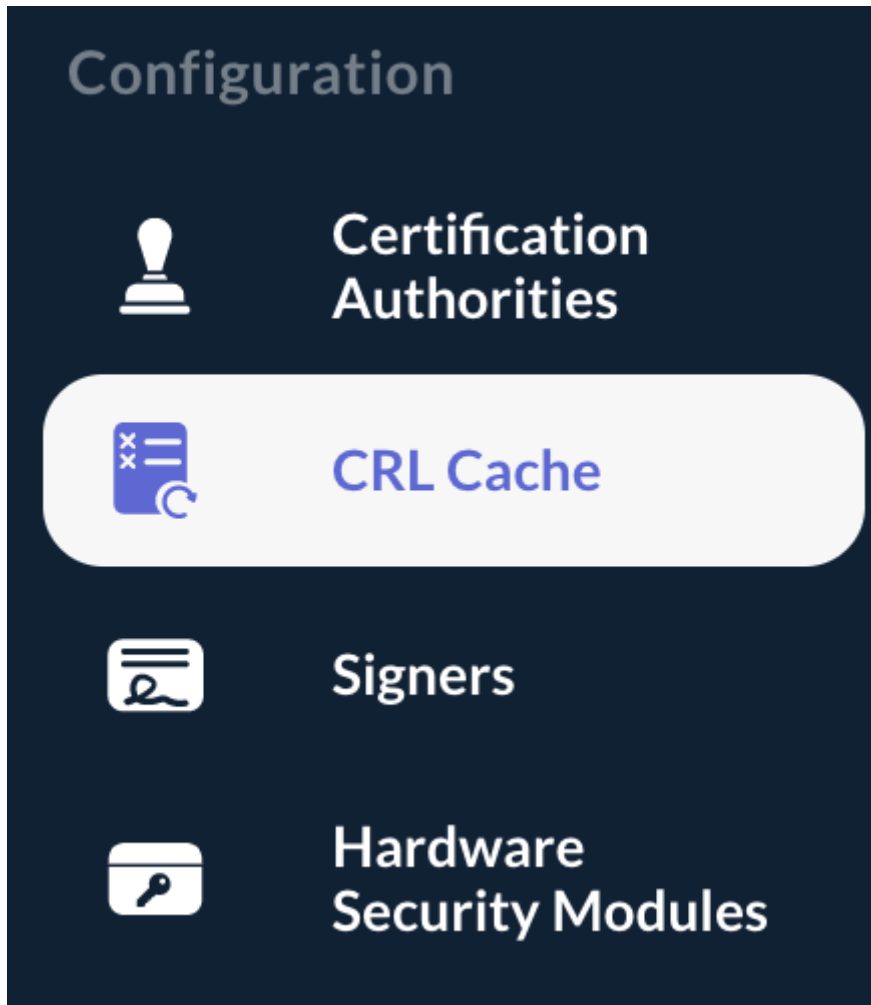
Success

'EverTrust Technical CA' successfully deleted




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.

CRL Cache

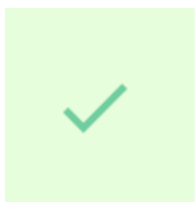
| CA Name | Cache - Last Refresh | CRL - Size | Status | |
|------------------------|------------------------------|------------|--------------------------------------|---|
| EverTrust Technical CA | Nov 18, 2020 05:34 PM +01:00 | 457 | ● |   |

Records per page: 10 |< < 1/1 > >| 

TIP

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:



Success

All CRLs have been successfully refreshed



TIP

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

NOTE

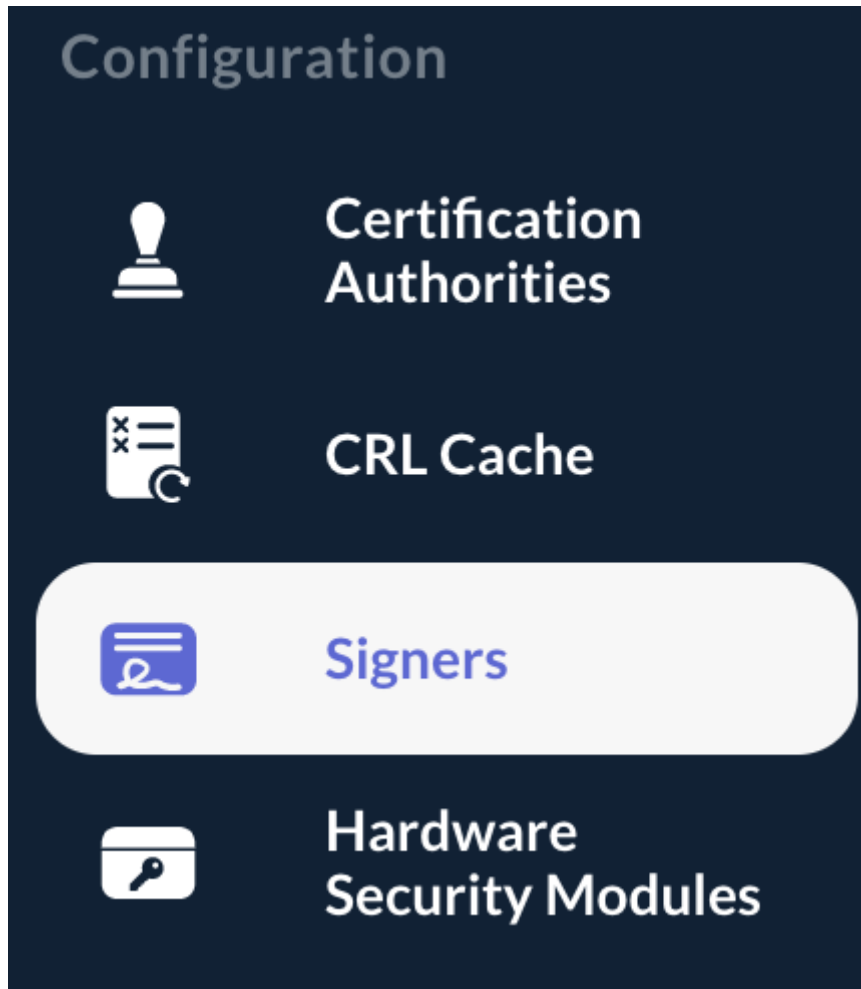
The number of cache entries in the cache does not reflect the number of entries in the CRL. Expired entries will be removed from the CRL, but not from the cache. Therefore, the cache contains at least as many entries as in the CRL, but can contain more. It contains all the revoked entries parsed in the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

9. Managing OCSP Signers

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.

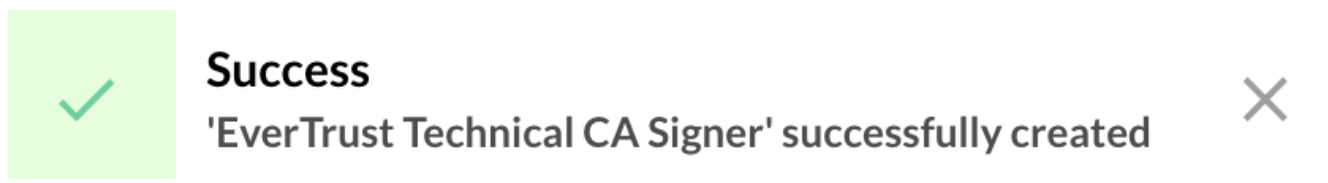
And hit the 'Add' button:

| | |
|--|--|
| Name * | EverTrust Technical CA Signer |
| Keystore * | Software |
| Key Parameter * | RSA / 2048 |
| DN * | CN = EverTrust Technical CA Signer  |
| Response Signing Algorithm * | SHA1 |
| Responder ID Type * | Distinguish Name |
| Worker(s) * | 5 |
| Notify On Signer Expiration? | <input checked="" type="checkbox"/> |
| Signer Expiration Prior Notice Delay (in days) | 15 |
| Cancel | Add |

NOTE

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

Step 5: The Signer is successfully created:



Success
'EverTrust Technical CA Signer' successfully created

Signer

| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------|------------------------------------|-----------|----------|------------|-----------|--------|--|
| EverTrust Technical CA Signer | CN = EverTrust Technical CA Signer | - | Software | RSA / 2048 | sha1 | | |

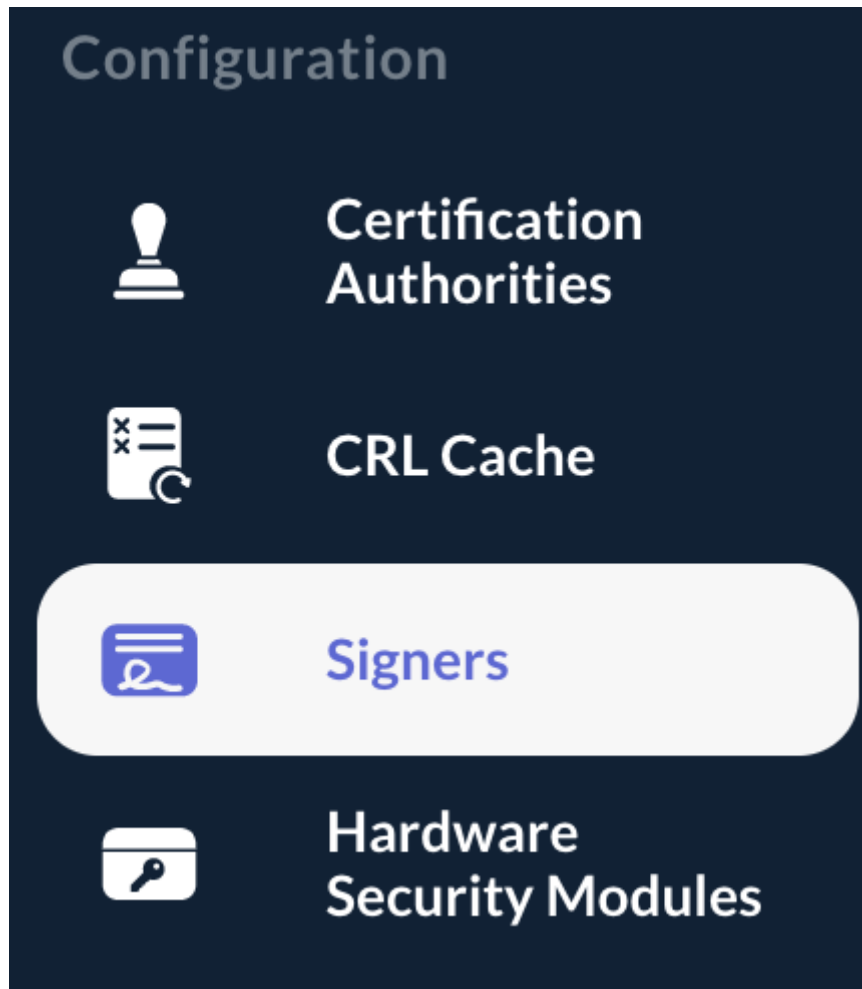
Records per page: 10 |< < 1/1 > >|


9.2. Managing Signer Certificate Requests

9.2.1. 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:

| | | | | | | | |
|----------------------------------|---------------------------------------|---|----------|------------|------|---|---|
| EverTrust Technical CA Signer | CN = EverTrust Technical CA Signer | - | Software | RSA / 2048 | sha1 |  |     |
|----------------------------------|---------------------------------------|---|----------|------------|------|---|---|

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

Name *
EverTrust Technical CA Signer

Keystore *
Software

Key Parameter *
RSA / 2048

DN *
CN = EverTrust Technical CA Signer

Response Signing Algorithm *
SHA1

Responder ID Type *
Distinguish Name

Worker(s) *
5

Notify On Signer Expiration?

Signer Expiration Prior Notice Delay (in days)
15

Cancel **Update**

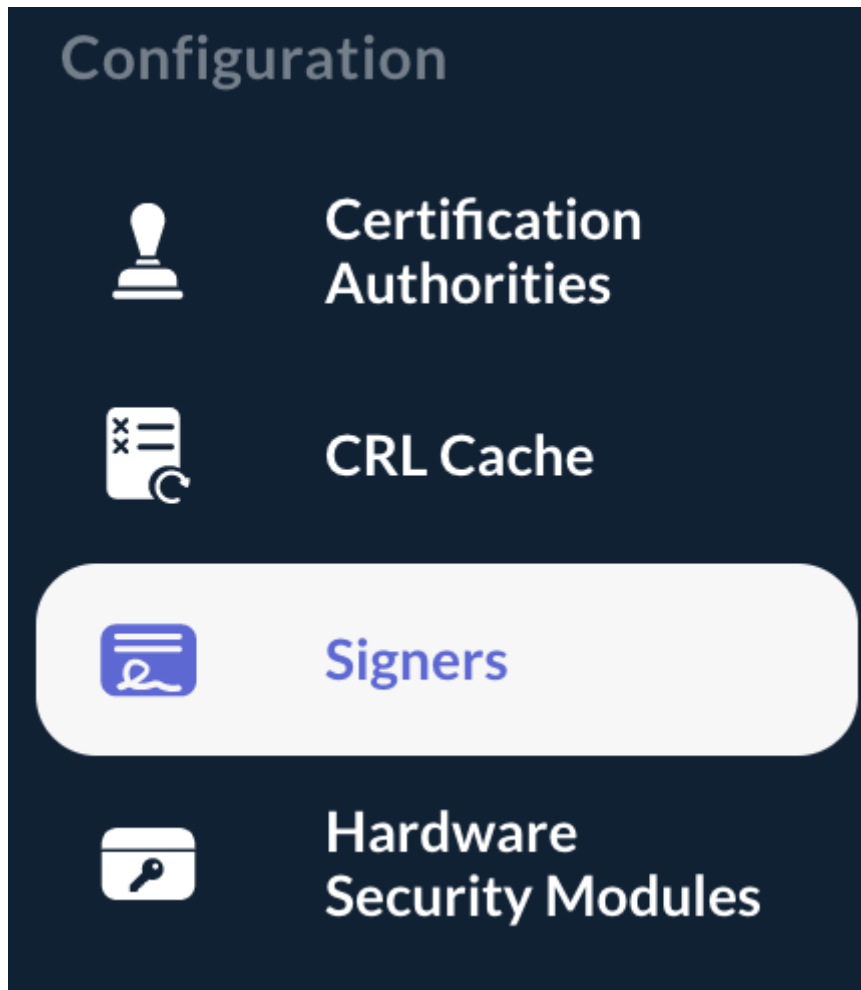
Step 5: The Signer is successfully updated:

 **Success** 'EverTrust Technical CA Signer' successfully updated 

9.2.2. 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):

| | | | | | | | |
|----------------------------------|---------------------------------------|---|----------|------------|------|---|---|
| EverTrust Technical CA Signer | CN = EverTrust Technical CA Signer | - | Software | RSA / 2048 | sha1 |  |     |
|----------------------------------|---------------------------------------|---|----------|------------|------|---|---|

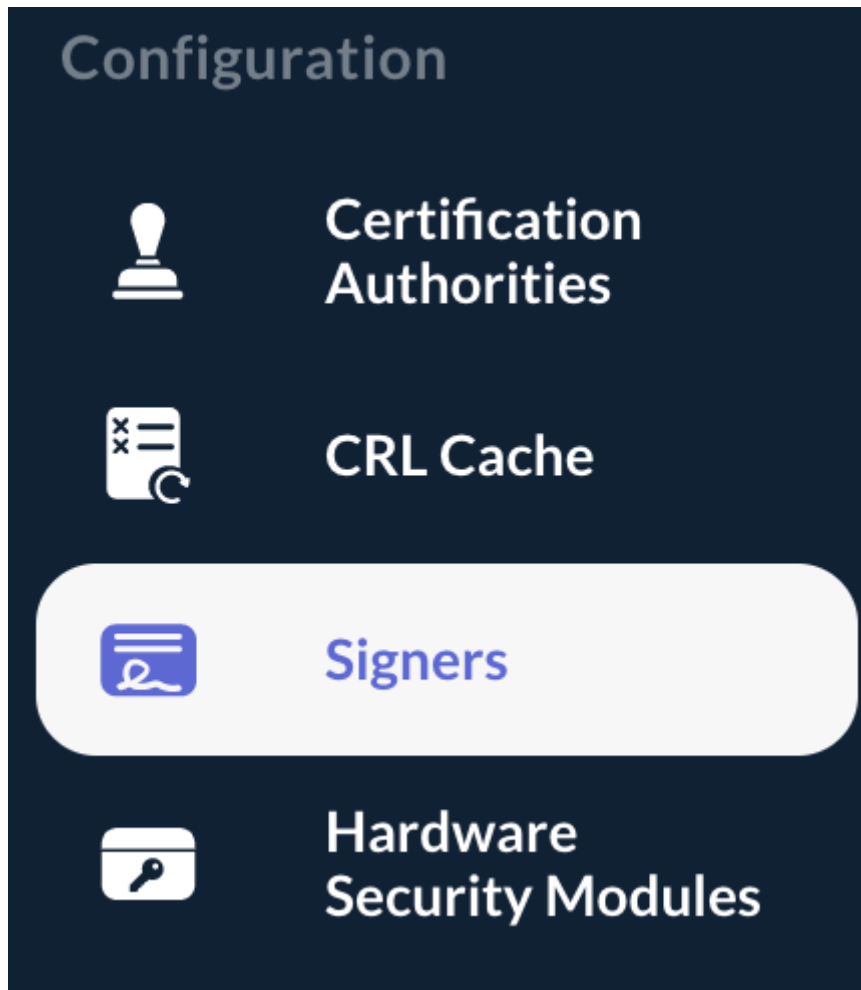
Step 4: The PKCS#10 certificate is generated.


NOTE | The request needs to be signed using your corporate PKI.


9.2.3. 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:

EverTrust Technical CA Signer CN = EverTrust Technical CA Signer - Software RSA / 2048 sha1     

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


Please select the Signer Certificate to upload (PEM or DER format)


Browse
EverTrust_Technical_CA_Signer.pem  






Cancel



Submit

Step 5: The Signer certificate is successfully installed:

 **Success** ✕
'EverTrust Technical CA Signer' successfully updated

Signer Search 

| Name | DN | Not After | Keystore | Key | Algorithm | Status |
|-------------------------------|--|------------------------------|----------|------------|-----------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 |      |

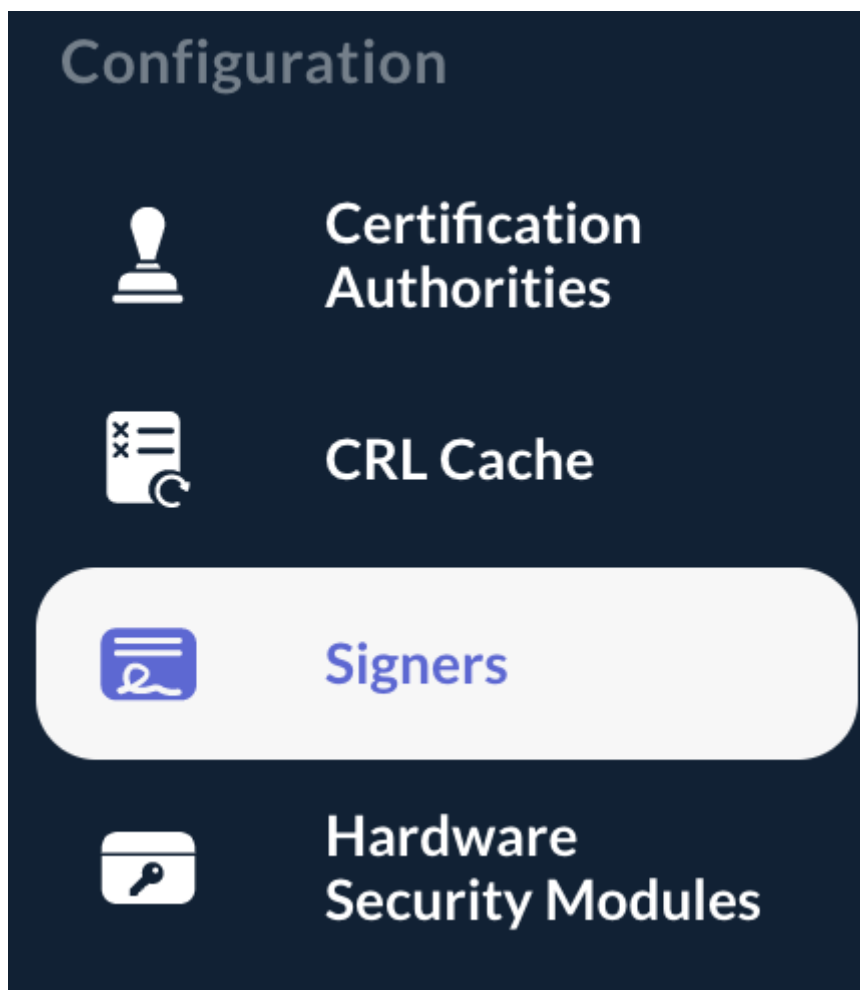
Records per page: 10  |< < 1/1 > >| 

9.3. Managing Signers


9.3.1. 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:

Signer Search 

| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------|---|---------------------------------|----------|------------|-----------|-------------------------------------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 | <input checked="" type="checkbox"/> |     |

Records per page: 10 |< < 1/1 > >| +

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 Settings

Signer Certificate Details

Name *

EverTrust Technical CA Signer

Keystore *

Software

Key Parameter *

RSA / 2048

DN *

CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR



Response Signing Algorithm *

SHA1

Responder ID Type *

Distinguish Name

Worker(s) *

5

Notify On Signer Expiration?



Signer Expiration Prior Notice Delay (in days)

15

Cancel

Update

NOTE

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

DN

CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR

Issuer DN

CN=EverTrust Technical CA, O=EverTrust, C=FR

Serial

0xd0ba88a163ddcbbd23bfa9bf

Not Before

Nov 18, 2020 05:55 PM +01:00

Not After

Nov 18, 2022 06:00 PM +01:00

Cancel

Update

Step 5: The Signer is successfully updated:



Success

'EverTrust Technical CA Signer' successfully updated



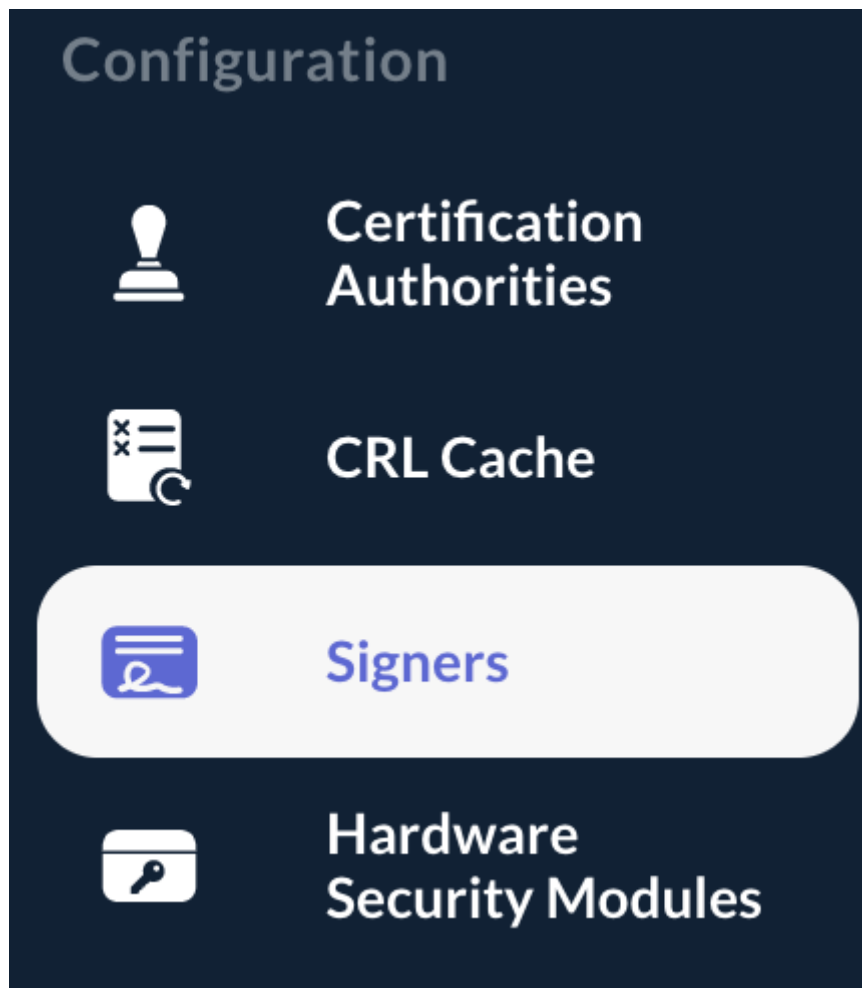
9.3.2. Deleting a Signer

WARNING





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:

| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------|--|------------------------------|----------|------------|-----------|--------------------------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 | <input type="checkbox"/> |     |

Records per page: 10 |< < 1/1 > >| 

Step 4: Hit the 'Confirm' button:

Do you really want to delete the signer EverTrust Technical CA Signer?

Cancel

Confirm

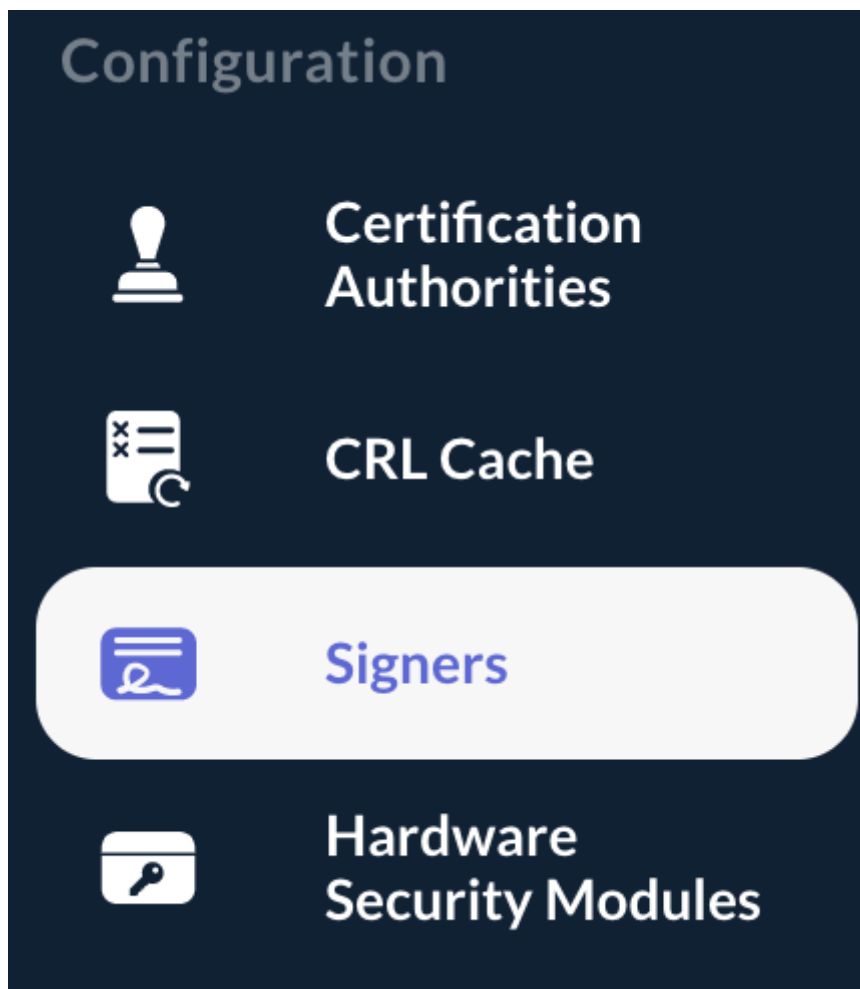
Step 5: The Signer is successfully deleted:




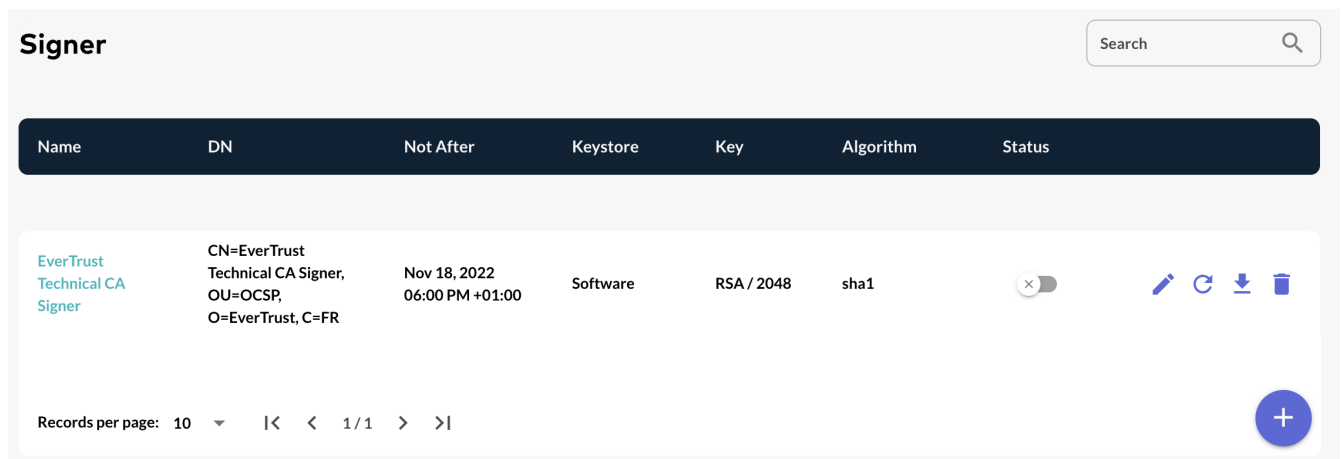
9.4. Downloading a Signer Certificate






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:



| Name | DN | Not After | Keystore | Key | Algorithm | Status |
|-------------------------------------|---|---------------------------------|----------|------------|-----------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 |      |

Records per page: 10  |   1 / 1   

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

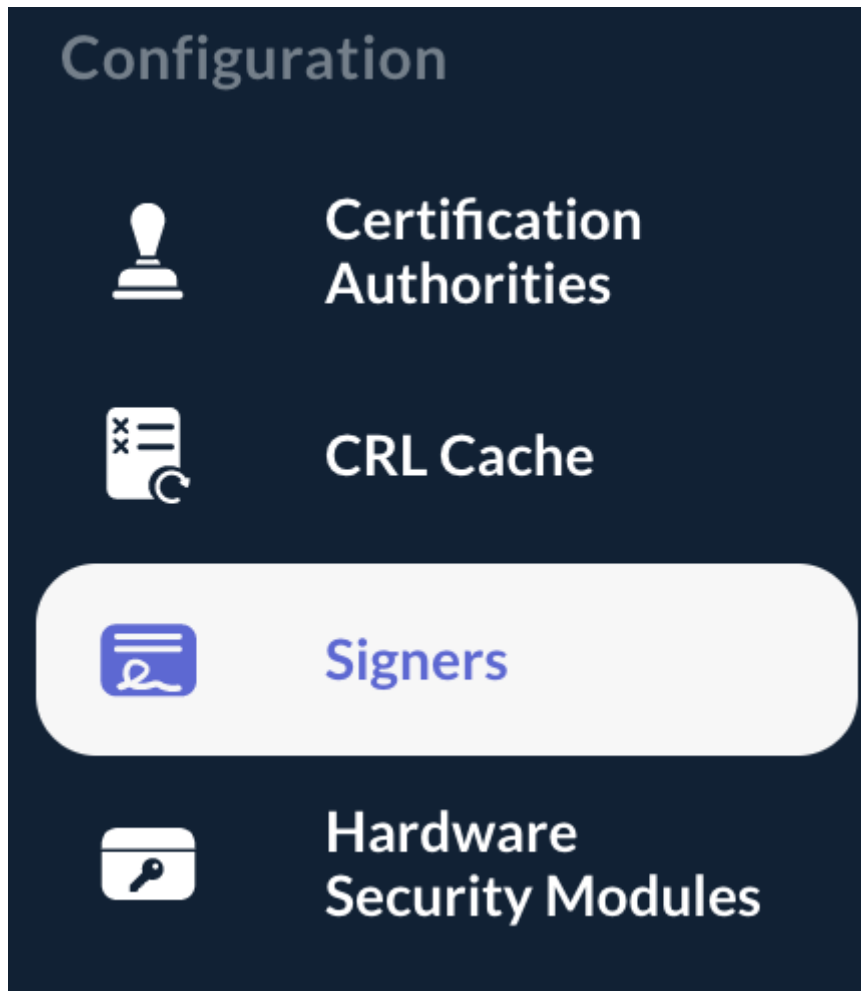
9.5. Enabling or Disabling Signers

9.5.1. Enabling a Signer





NOTE | 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**':

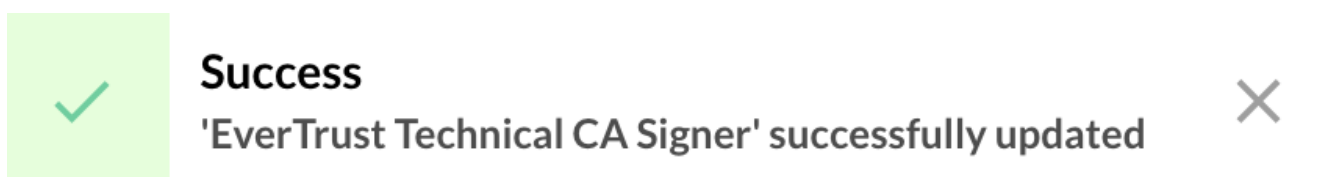


Step 3: Hit the  button of the Signer you are willing to enable:





| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------|--|------------------------------|----------|------------|-----------|-------------------------------------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 | <input checked="" type="checkbox"/> |     |


Records per page: 10 |< < 1/1 > >| 

Step 4: The Signer is successfully enabled:



Signer

| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------------|---|---------------------------------|----------|------------|-----------|-------------------------------------|---|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 | <input checked="" type="checkbox"/> |     |

Records per page: 10 |< < 1/1 > >| 

NOTE

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

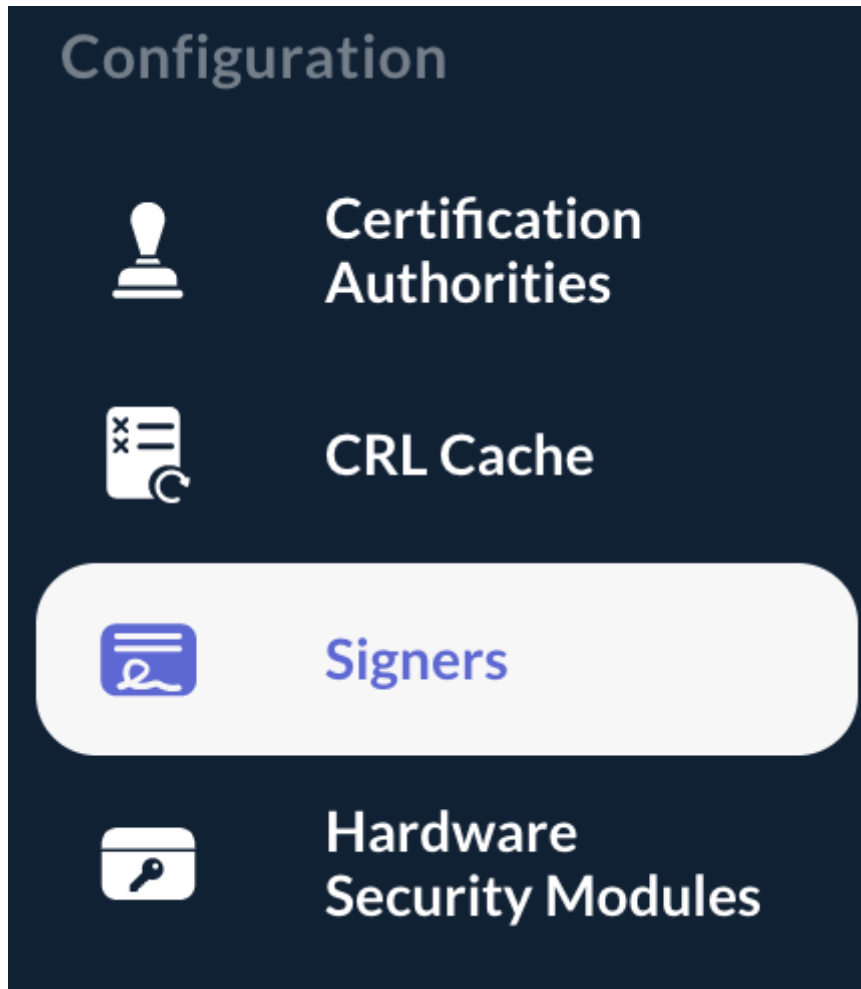
9.5.2. Disabling a Signer

WARNING






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:

| Signer | | | | | | | Search | Q | | |
|-------------------------------------|---|---------------------------------|----------|------------|-----------|---|---|---|---|---|
| Name | DN | Not After | Keystore | Key | Algorithm | Status | | | | |
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 |  |  |  |  |  |

Records per page: 10 |< < 1/1 > >| 

Step 4: The Signer is successfully disabled:



Success

'EverTrust Technical CA Signer' successfully updated



Signer

Search



| Name | DN | Not After | Keystore | Key | Algorithm | Status | |
|-------------------------------------|---|---------------------------------|----------|------------|-----------|--------------------------|--|
| EverTrust Technical CA Signer | CN=EverTrust Technical CA Signer, OU=OCSP, O=EverTrust, C=FR | Nov 18, 2022 06:00 PM +01:00 | Software | RSA / 2048 | sha1 | <input type="checkbox"/> | |

Records per page: 10 |< < 1 / 1 > >|

10. Managing Services

10.1. Starting the OCSPd services

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

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

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

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

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

10.2. Stopping the OCSPd services

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

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

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

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

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

11. Backup and Restore

11.1. Backup

CAUTION

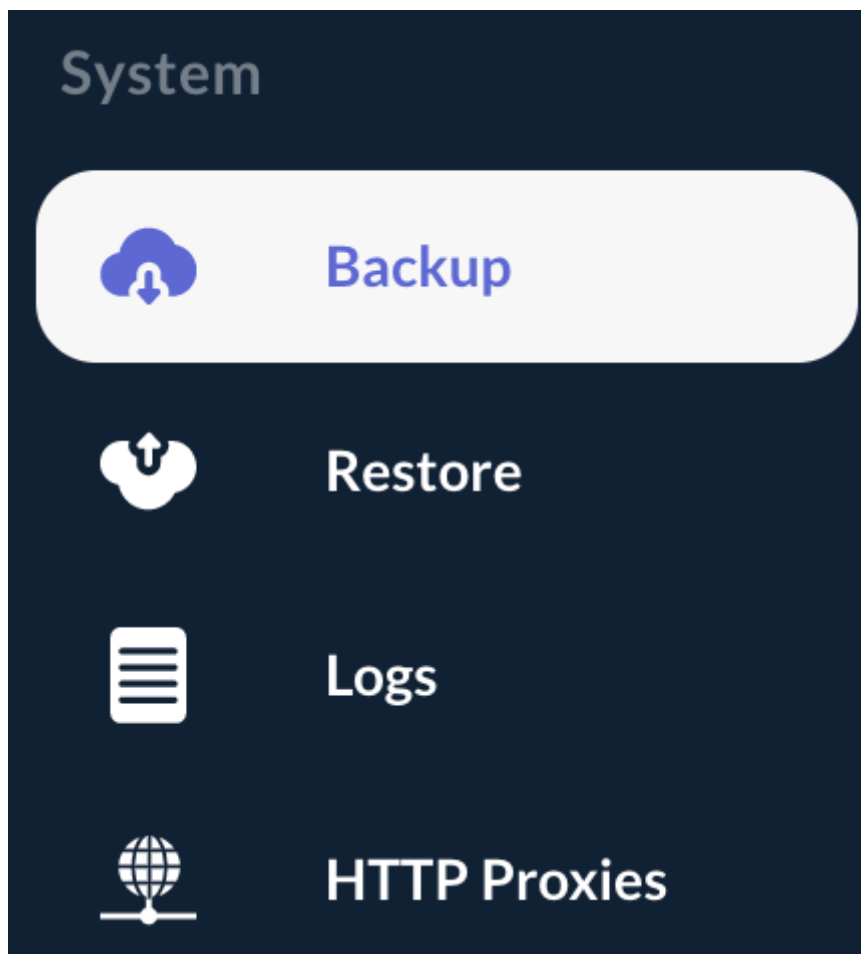
The following backup procedure does not detail how to back up the Hardware Security Module. Please refer to the HSM provider documentation and **ensure to perform an HSM backup** when using an hardware keystore.

NOTE

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

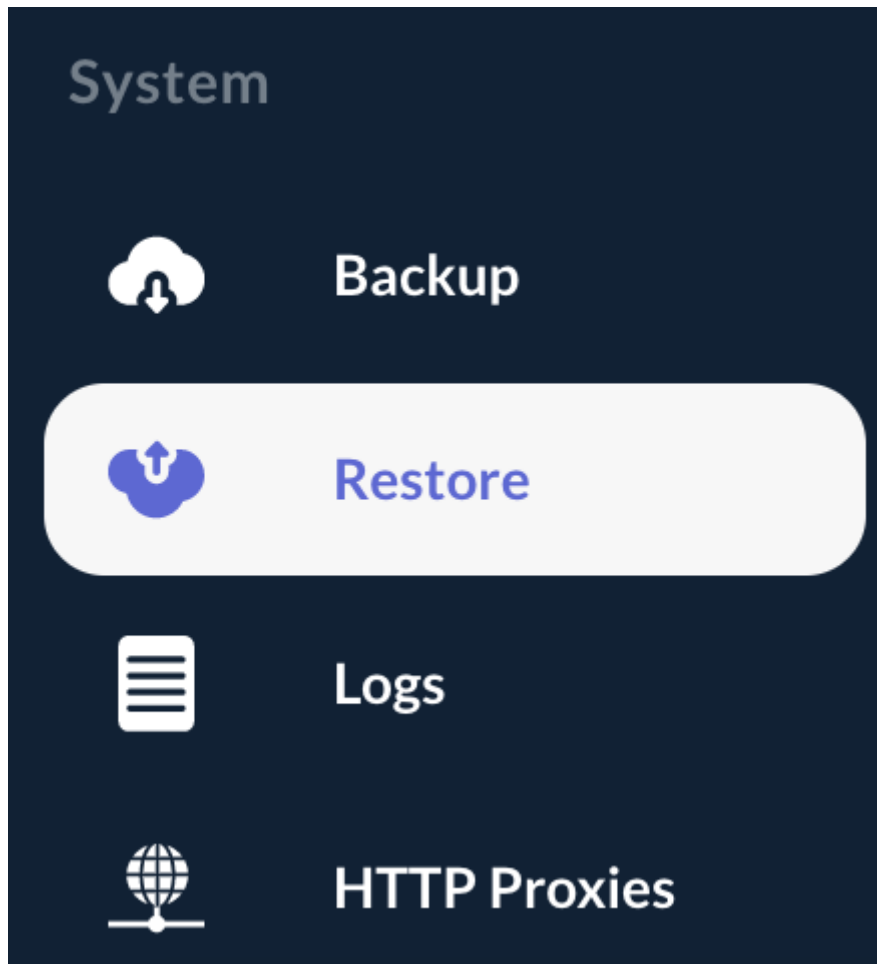
11.2. Restore

CAUTION

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:

Browse to your OCSP backup file (JSON) and click on 'Restore' to restore OCSP configuration

Browse
ocspd-backup-1605718223883.json ✕

Restore

Step 5: The Backup is successfully restored:



Success

Backup successfully restored



12. Logs & Monitoring

12.1. Logs location

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

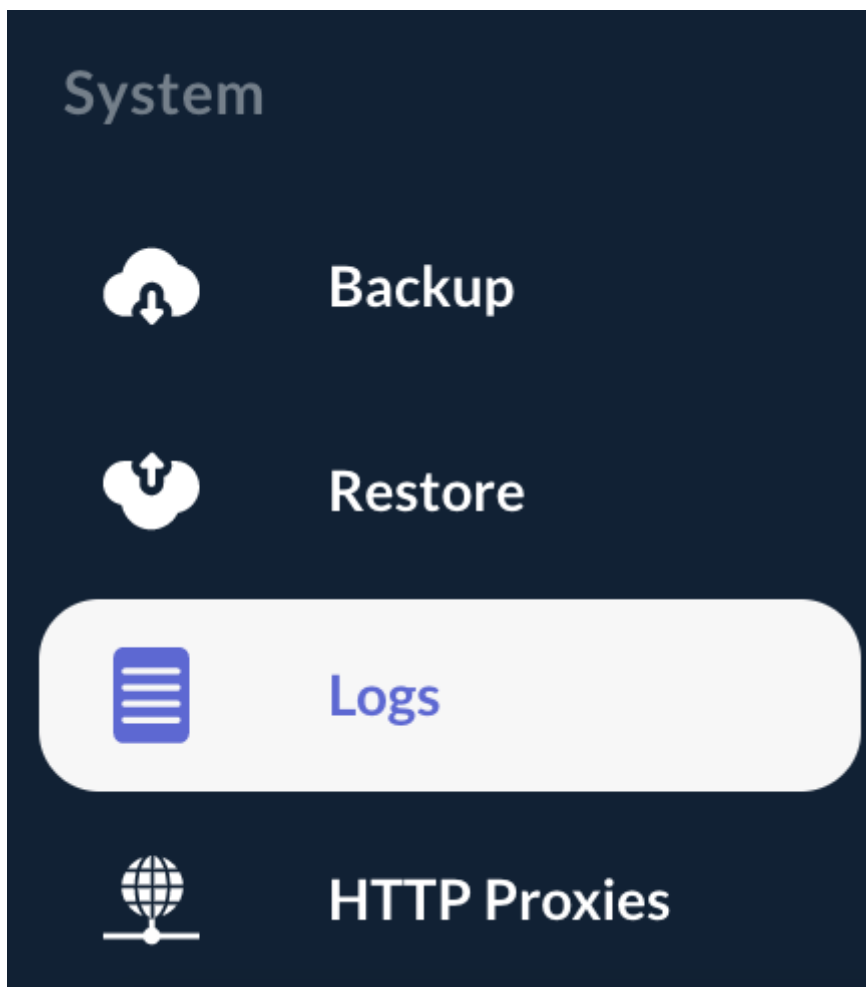
- Application logs are spooled to `'ocspd.log'`;
- Administration logs are spooled to `'ocspd-admin.log'` and the log file can be signed upon rotation.

NOTE | These log files are rotated daily.


12.2. 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:


Logs Search 

| File Name | File Size | Last Modified |
|-----------|-----------|------------------------------|
| tsa.crl | 18.5KB | Nov 18, 2020 05:40 PM +01:00 |
| tsa.pem | 25.0KB | Nov 18, 2020 05:40 PM +01:00 |

Records per page: 10 |< < 1/1 > >| 


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





Success

All log files have been successfully refreshed



12.3. Managing the OCSPd Log Level

NOTE

3 Log Levels are available within OCSPd:

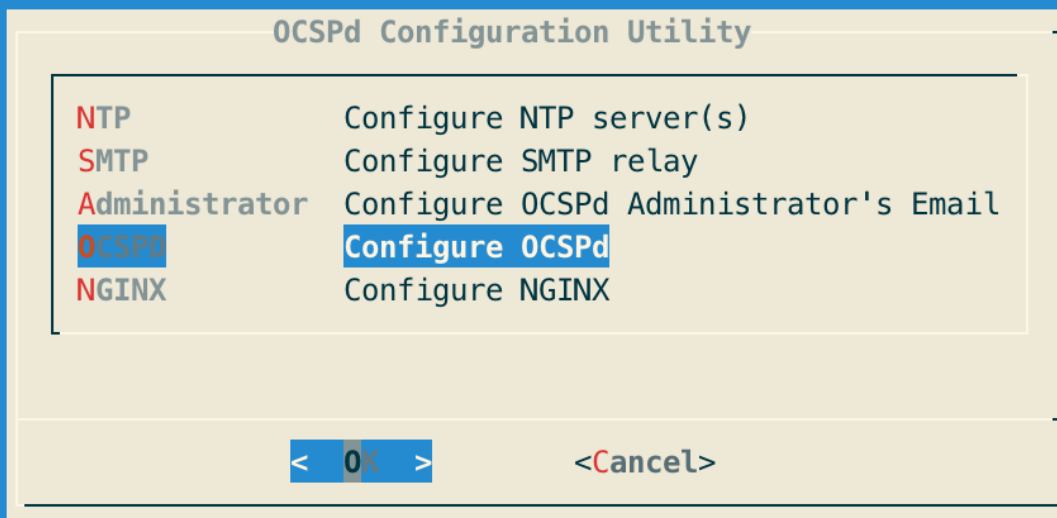
- '**DEBUG**': this mode is very verbose and provides debug information. It should not be turned on in production except for debugging purpose;
- '**INFO**': this is the default mode. It provides error information along with OCSP request information;
- '**ERROR**': this mode only logs errors.

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

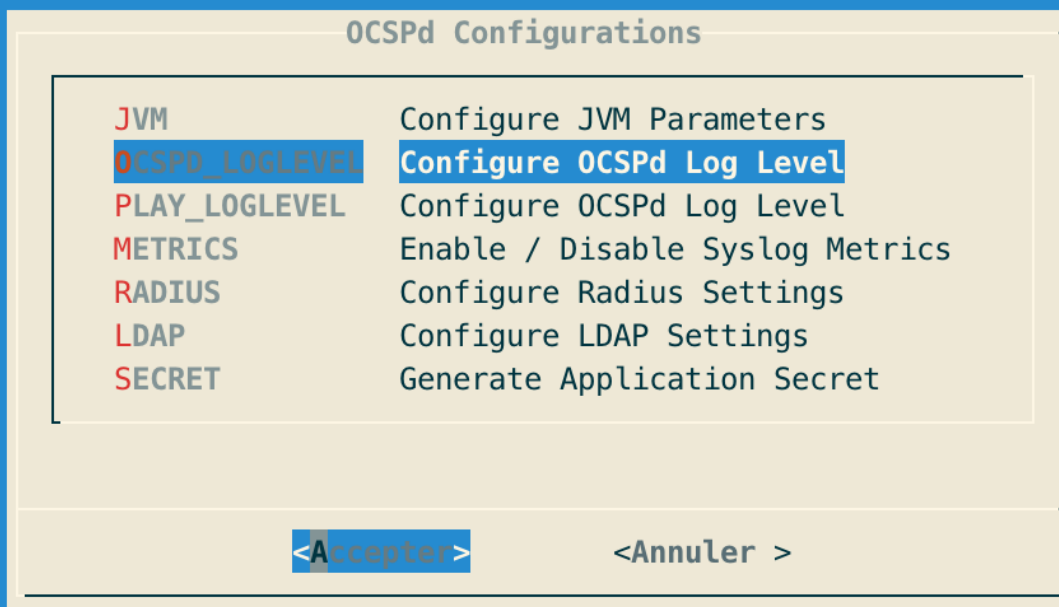
Step 2: Load the OCSPd Configuration Utility with the following command:

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

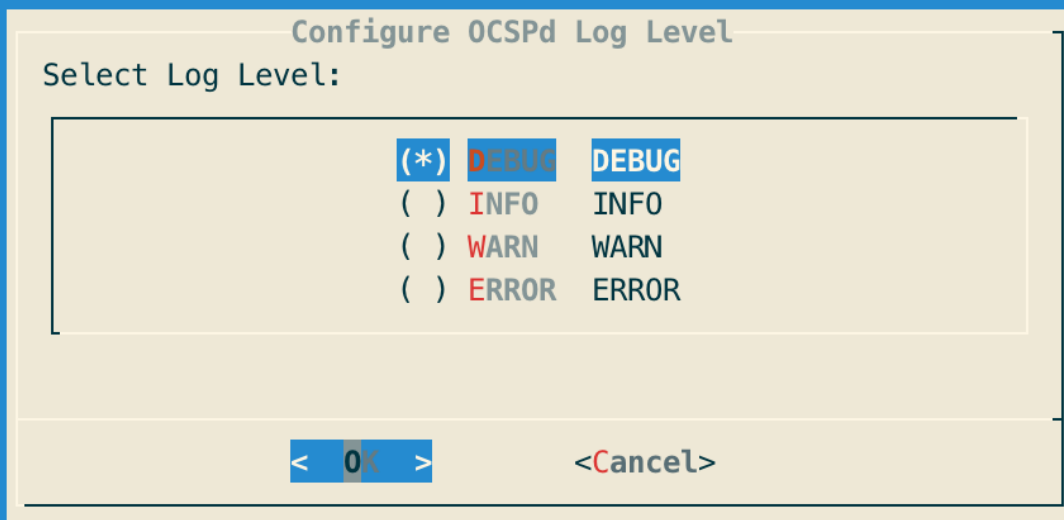
Step 3: In the main menu, select '**OCSPd**':



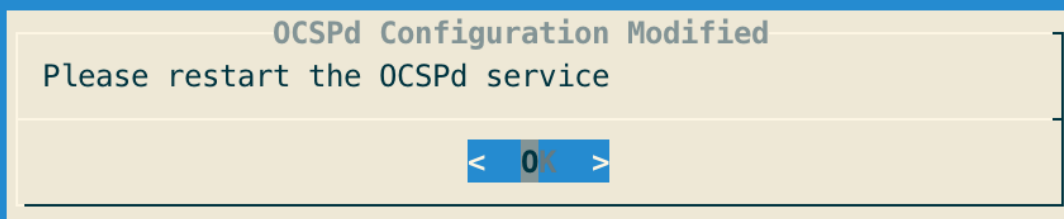
Step 4: In the OCSPPd menu, select 'OCSPPd_LOGLEVEL':



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
```

12.4. 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.

13. HTTP Proxies

This section details how to manage OCSPd HTTP Proxies.

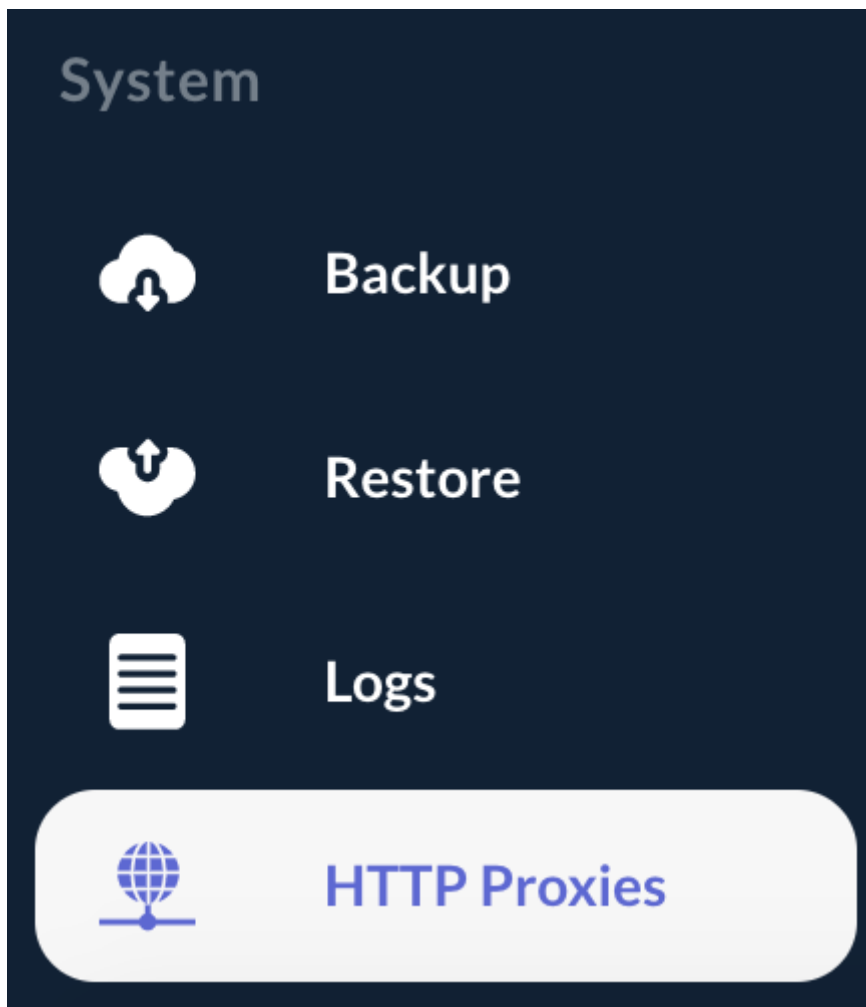
NOTE

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

13.1. 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:

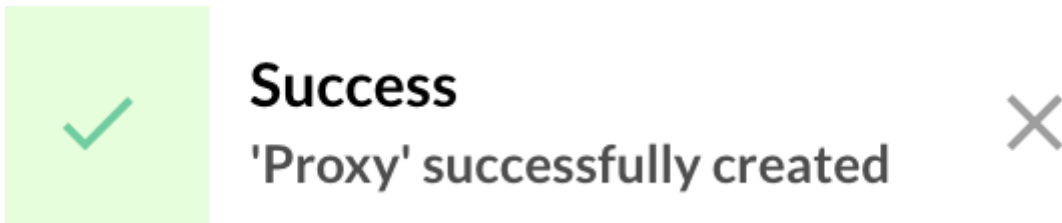
Name *
Proxy

Host *
proxy.evertrust.fr



Port *
8080


Cancel **Add**

Step 5: The HTTP Proxy is successfully created:



HTTP Proxy Search

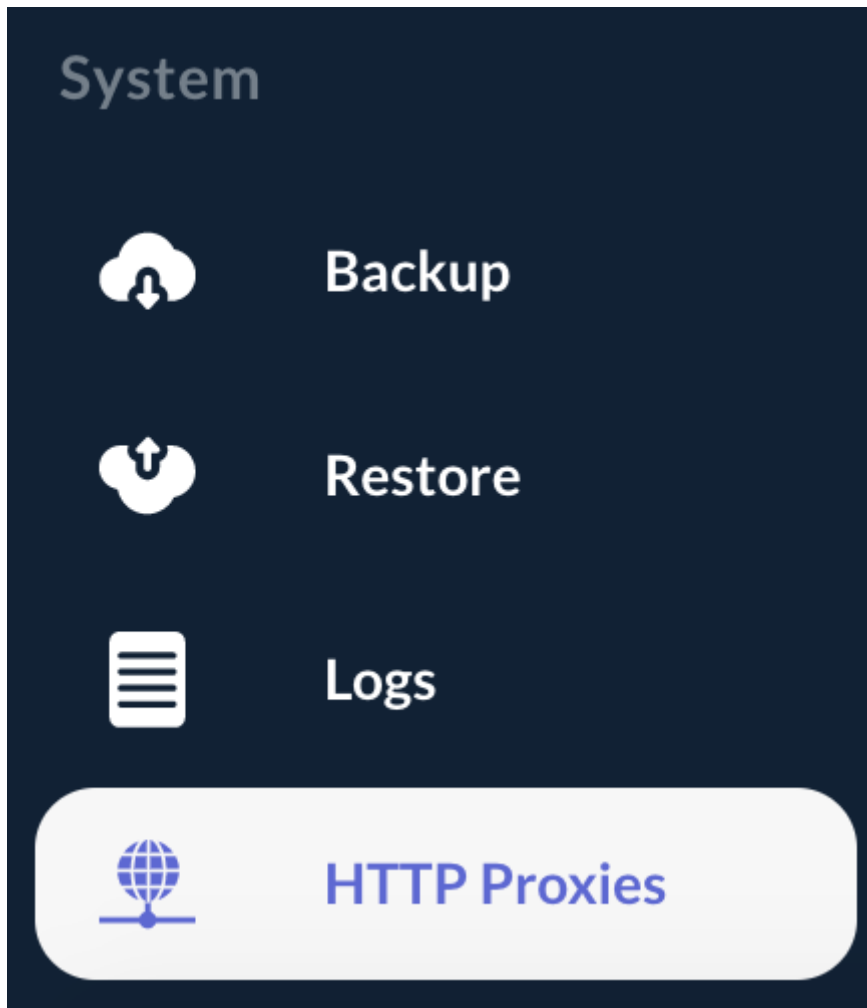
| Name | Host | Port | |
|-------|--------------------|------|---|
| Proxy | proxy.evertrust.fr | 8080 |   |


Records per page: 10 |< < 1/1 > >| 

13.2. 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:

Proxy

proxy.evertrust.fr

8080



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

Name *

Proxy

Host *

proxy.evertrust.fr

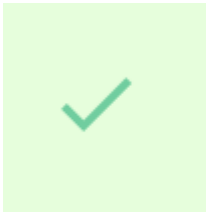
Port *

8080

Cancel

Update

Step 5: The HTTP Proxy is successfully updated:



Success

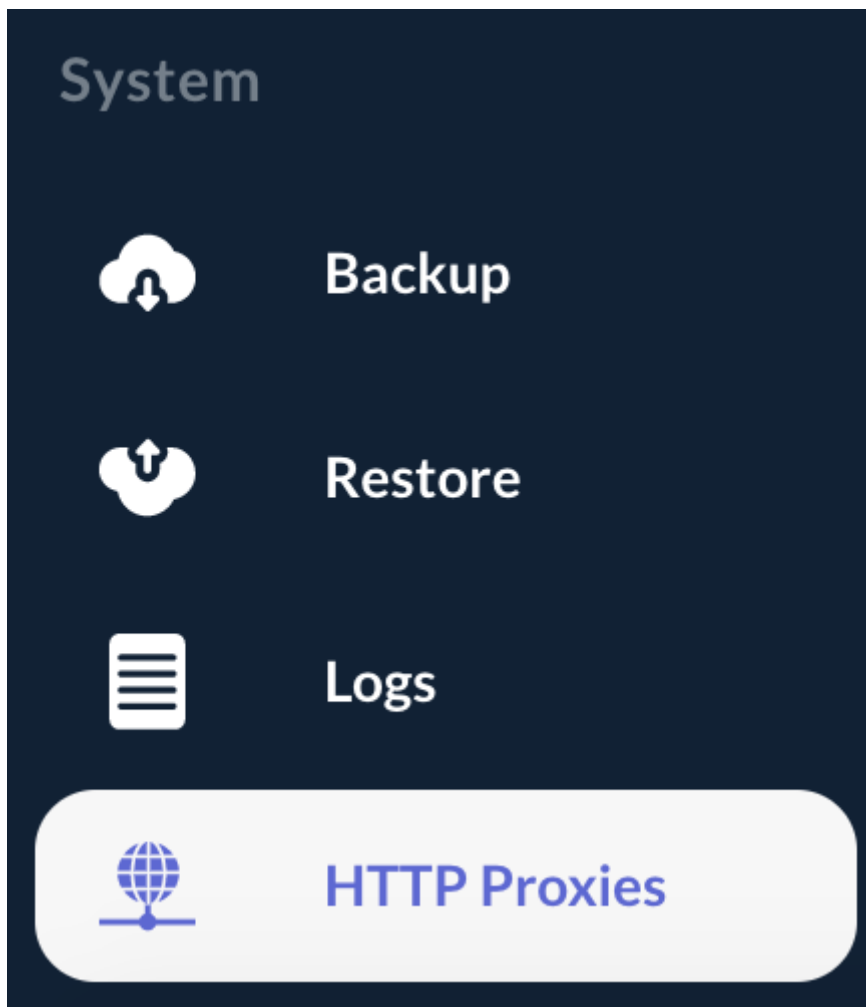
'Proxy' successfully updated



13.3. 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:

Proxy

proxy.evertrust.fr

8080



Step 4: Hit the 'Confirm' button:

Do you really want to delete the HTTP proxy Proxy?

Cancel

Confirm

Step 5: The HTTP Proxy is successfully deleted:



Success

'Proxy' successfully deleted



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.

CAUTION

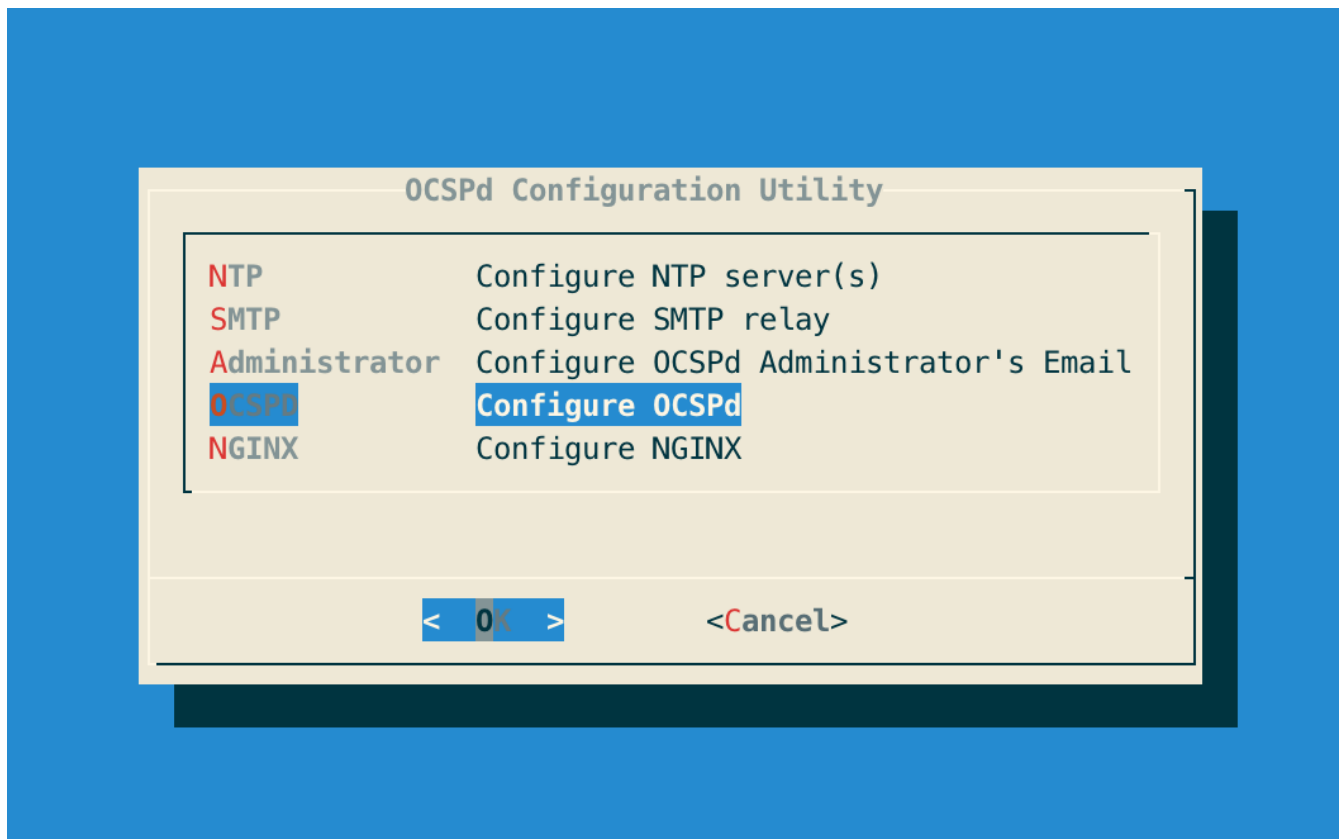
The following KPI configuration procedure does not detail how to aggregate metrics logs. Please refer to the **OCSPd KPI Integration Guide** documentation for more information.

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

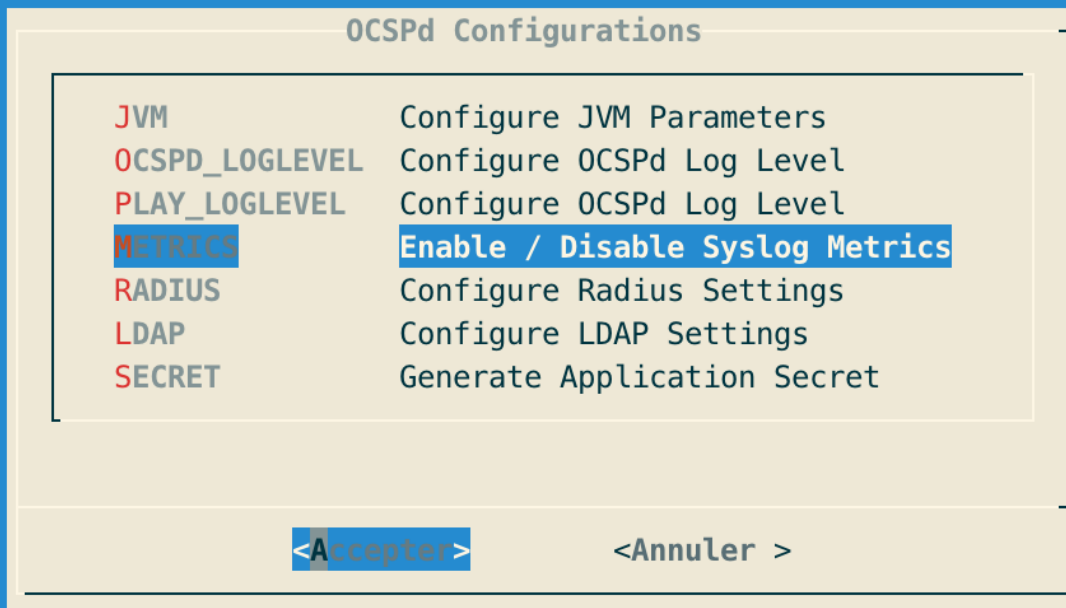
Step 2: Load the OCSPd Configuration Utility with the following command:

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

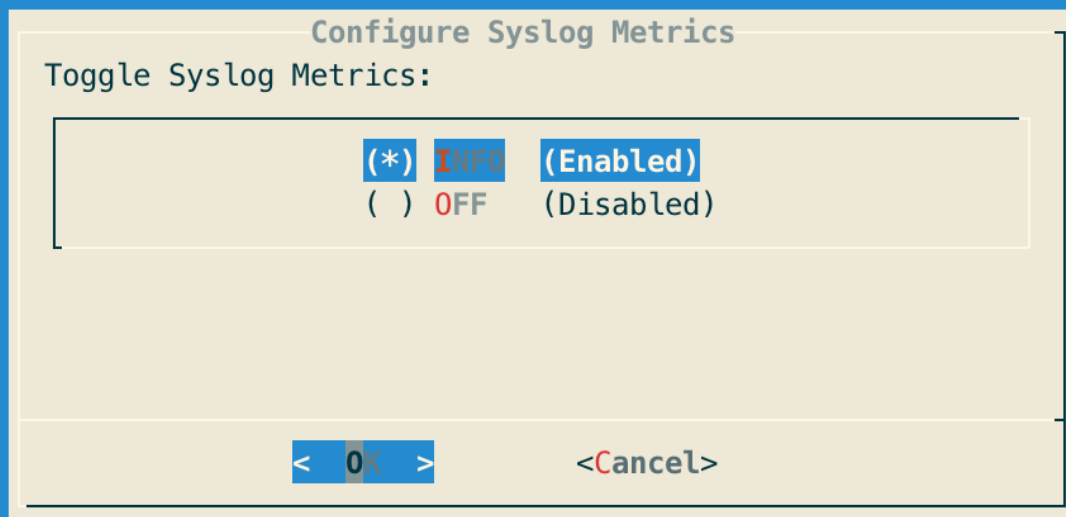
Step 3: In the main menu, select '**OCSPd**':



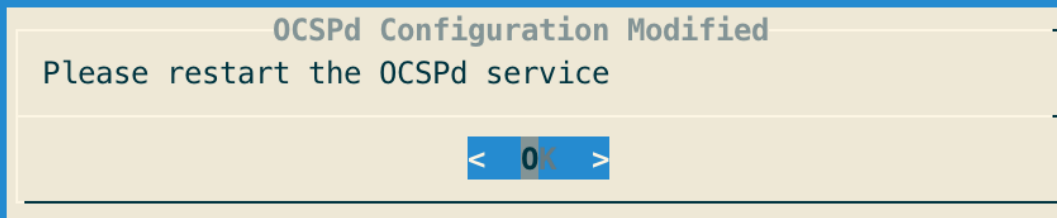
Step 4: In the OCSPD menu, select '**METRICS**':



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
```

NOTE 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
```

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.

WARNING

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