
EJBCA-REST Documentation

Release 0.2.0a1

Matheus Magalhaes

May 19, 2020

Contents:

1	Profile configuration tutorial	3
1.1	Configuration	3
2	REST API	5
3	How to build/update/translate documentation	7
3.1	Build	7
3.2	Update workflow	7
4	Index	9
5	Description	11
6	Dependencies	13
7	Configuration	15
7.1	Configuring EJBCA Profiles	15

[Docker badge]

Profile configuration tutorial

1.1 Configuration

If you are using the provided docker container, all configuration explained on this document has already been done on the container.

This document list the steps taken to configure EJBCA.

Misconfiguring a Certificate authority can severely affect all systems that rely on it for authentication purposes, leading to a swath of security vulnerabilities being implicitly added to them. Please be extra careful when dealing with this.

1.1.1 Pre Configuration

To configure EJBCA via the web interface, first you need to configure your browser certificates.

Copy the client side certificate from your EJBCA instance, located on '/p12/superadmin.p12' and '/p12/ca.crt' to your local machine.

The way trusted and client certificates are configured vary from browser to browser. Please, check you favorite browser manual. Add 'ca.crt' to your 'Certificate Authorities' list. Add 'superadmin.p12' to 'personal certificates' list. The password for the file is 'ejbca' (all lowercase, without quotes)

Now you can access the EJBCA Web service at hostname:8443/ejbca You may need to authorize the site to use a personal certificate. Select the certificate superadmin.p12.

1.1.2 Configuring EJBCA Profiles

Follow the link for the administration menu. Click on 'Certificate Profiles' Clone the ENDUSER default profile. Give the new profile the name CFREE. Click the button edit on the new created profile.

Change the following fields:

- Available bit lengths: deselect key lengths bellow 2048 bits
- Signature Algorithm: Sha256WithRSA

- Allow extension override: check
- Basic Constraints: unselect critical
- Key Usage: unselect critical, select 'data encipherment' and 'Key agreement'
- Extended Key Usage: unselect

Click 'save' at the bottom of the page to save editions.

Click on 'End Entity Profiles'. Create a new profile, called 'EMPTY_CFREE' Edit the profile

- Batch generation (clear text pwd storage)
 - Select 'Use'
- Subject Alternative Name
 - Add DNS Name
 - Add IP Address
- Default Certificate Profile
 - Select CFREE
- Available Certificate Profiles
 - Select CFREE

Click 'save' at the bottom of the page to save editions

CHAPTER 2

REST API

This is the REST API documentation for EJBA-REST. This page is automatically generated from `this file`.

All APIs are available in [Github pages API description](#)

How to build/update/translate documentation

If you have a local clone of this repository and you want to change the documentation, then you should follow this simple guide.

3.1 Build

The readable version of this documentation can be generated by means of sphinx. In order to do so, please follow the steps below. Those are actually based off [ReadTheDocs documentation](#).

```
pip install sphinx sphinx-autobuild sphinx_rtd_theme sphinx-intl
make html
```

For that to work, you must have pip installed on the machine used to build the documentation. To install pip on an Ubuntu machine:

```
sudo apt-get install python-pip
```

To build the documentation in Brazilian Portuguese language, run the following extra commands:

```
sphinx-intl -c conf.py build -d locale
make html BUILDDIR=build/html-pt_BR O='-d build/doctrees/ -D language=pt_BR'
```

3.2 Update workflow

To update the documentation, follow the steps below:

1. Update the source files for the english version
2. Extract translatable messages from the english version

```
make gettext
```

3. Update the message catalog (PO Files) for pt_BR language

```
sphinx-intl -c conf.py update -p build/gettext -l pt_BR
```

4. Translate the messages in the pt_BR language PO files

This workflow is based on the [Sphinx i18n guide](#).

CHAPTER 4

Index

- *Description*
- *Dependences*
- *Configuration*

CHAPTER 5

Description

This is a utility library to simplify the call for EJBCA SOAP API with a more modern and easy to use REST JSON API.

CHAPTER 6

Dependencies

`pip install zeep`

(optional) for the docs: `pip install aglio`

7.1 Configuring EJBCA Profiles

EJBCA-REST is configured out of the box with Certification Profiles compatible with Mosquitto TLS and other IoT Brokers.

If you need to configure EJBCA manually, check our [Profile configuration tutorial](#).