

Modules - Certificates: Approving certificate request

This tutorial shows how to set approvers for certificate requests.

What do you need before you start

- You need install **CzechIdM 7.7.0** (and higher).
- You need be logged in as **admin**.
- You need enable **Certificate** module.
- You are familiar with [certificates module](#) tutorial.

Create role for approvers

- In the left menu click on **Roles**.
- In the following page click on **Add** green button in the upper-right corner.
- Fill **Name** as "certificate_approvers".
- Click on **Save and continue** green button.
- Click on **Permissions** tab.
- In the following page click on **Add** green button in the upper-right corner.
- Choose **Entity type** as "Certificate requests" and in **Permissions** choose "all" (as in picture below)

New permission ×

Role

certificate_approvers

Evaluator type

BasePermissionEvaluator ×

Simple permission evaluator - evaluates selected permissions on selected entity type

Entity type

Certificate requests (CrtRequest) ×

If entity type is not selected, then all types will be evaluating

Permissions

× Administration (all) ×

Permissions will be granted by evaluator configuration

Order ?

Description

☐ Inactive

Inactive policy will not be applied

Close

Save

- Now click again on **Add** button to add another permission.
- And fill to **Entity type** "Certificates" and to **Permissions** "all".
- **Add** another permission **Entity type** is "Certificate authorities" and to **Permission** fill "autocomplete".
- Our new role needs one more permission: **Entity type** - "Workflow - tasks" **Permission** - "Read" to actually get into **Tasks** agenda.

Now we have a role for approvers. In next step, we will create a user and assign him this approver role.

Create user for approving requests

* In the left menu click on **Users**.

- On the following page click on **Create user** green button in the upper-right corner.
- Fill **Login**, **First name**, **Surname** and **Password**. In the tutorial, we are using "Login: crtapp, First name: Jack, Surname: Approver".
- Then click on green **arrow** next to **Create** button and click on **Create and edit**.
- Click on **Roles** tab and then on **Manage authorizations** yellow button.

Jack Approver (crtapp) User details

Jack Approver (crtapp)

- Personal data
- More Information
- Change password
- Roles**
- Permissions
- Positions
- Subordinates
- Authorize roles
- Accounts
- Provisioning
- Certificates
- Audit

Assigned roles

No results found

[Manage authorizations](#)

Requests for authorization change

No results found

0 - 0 of 0 records

Roles pending approval

No results found

0 - 0 of 0 records

BCV solutions s.r.o. | [Help](#) | [ServiceDesk](#) | [About app](#)

- On this page click on **Add** button.
- In popup window select role **certificate_approvers** and click on **Set** button.
- Now you should have the same state as in the picture below. Then click on **Submit a request** button.

Requested for

Jack Approver (crtapp)

E-mail

Phone

[Show full detail](#)

Applicant

Administrator (admin)

State

Concept

Description

Verbal description of a request to change the permissions

Current assigned roles (includes requested changes)

Role name	Contracted position	Valid from	Valid till	Automatic role	Actions
certificate_approvers	Jack Approver (crtapp) - Default			<input type="checkbox"/>	Add Set

Requested change of permissions

Role	Employment relationship	Operation	State	From	Till	Id WF process	Id
certificate_approvers	Jack Approver (crtapp) - Default	Add	Concept				65c4d30

1 - 1 of 1 records

[Back](#) [Submit a request](#)

Set role as approver

Now you may begin tutorial for [certificates module](#). But when we are creating **certificate authority** we fill in **Approver roles** and enable **Enable approving by workflow process** as in the picture

below. (Or you can modify another certificate authority already created in same section.)

New certificate authority

Code

Main CA

Driver

caw-driver

Identifier

users

Identifier of CA.

Supported certificate types (multi)

AUTHENTICATION
SIGNING

This CA supported this certificates types. Values have to be items from 'CertificateType' enumeration!

Path to the CAW distribution

/home/patrik/local/caw/caw

Path where is installed CAW distribution.

Path to the certificate for that authority

/home/patrik/local/caw/ca/ca.crt

Country

CZ

Abbreviation for the country

Locality

Prague

ORG

BCV

Organization

OU

test

Organization unit

State

Czech Republic

Include certificate chain

Enable approving by workflow process

Key of approving workflow process

crt-approve-request

Approver roles

certificate_approvers

Every requests (generate, revoke, renew) for this CA have to be approve by approvers (with that roles).

Inactive

Disabled authority cannot be used for generating new certificates.

Back

Save and continue

Approving of certificates

You can continue [certificates module](#) tutorial. And in **Generate certificate** after you submit a **New certificate request** (in **Generate certificate by CSR** this popup window's name is **Certificate request detail**) you will be left with this:

	State	Created	Type	Certificate type	Certificate	Certificate authority	Actions	Id
<input type="checkbox"/>	Approving	07.02.2018 13:27:15	New certificate	Authentication		Main CA		2a02ad2

1 - 1 of 1 records

So now we have to wait for approvers to accept our request. But since it is tutorial we will do it ourselves: Sign in as Jack. and then:

- Go to **Tasks**
- Click on our "create certificate" request.
- Read request and then click on green **Accept** button.
- (As you can see in the picture below, Jack Approver does not have enough permission to get information on admin.)

Approve certificate request Task details

Task name
 Approve to create the certificate for "Administrator"

Requested for
 4a1b868

Applicant
 4a1b868

Created on
 08.02.2018 10:45

Authorizer's note
 Note from authorizer.

NOT_FOUND (404:undefined)
 undefined (entity:4a1b868c-9ece-4e60-92d6-e98054f7bba1)

Type
 New certificate
 Request for create, renew, revoke certificate.

Certificate authority
 Main CA
 Certificate authority for create (renew, revoke) certificate. Authority can support different certificate types.

Description

State
 Approving

Result
 Running

Back Reject Accept

BCV solutions s.r.o. | Help | ServiceDesk | About app

And now log back in as an admin and you can continue with [certificates module](#) tutorial.



A process of renewing or revoke of certificates is approved automatically. Because especially in revoke situation user want to revoke certificate immediately.

Video Guide

[How to create certificate](#) - czech language

From:

<https://wiki.czechidm.com/> - **IdStory Identity Manager**

Permanent link:

https://wiki.czechidm.com/tutorial/adm/modules_crt_approving_request

Last update: **2019/01/07 12:04**

