

# Create evaluator with restrictions on one entity

[authorization](#), [certificate](#), [codeable](#), [evaluator](#), [evaluators](#), [restrict](#), [restrictions](#)

Codeable evaluator is useful for restricting privileges on selected entity. For example, if you want one user to be able to see only other user (with defined username or uuid), or for restricting that user to see only a role (defined by code or uuid).


This tutorial describes how admin can create a new evaluator to achieve that.

## Define evaluator with restriction for one identity (user)

This section describes how to create evaluator that restricts permission to see only one identity (user).

### Step 1. - Get username of user

In first step we must get username of identity that will be restricted by this new evaluator.

 John Doe (john.doe) User details

John Doe (john.doe)

Personal data

More information

Change password

Roles

Permissions

Positions

Subordinates

Authorize roles

Accounts

Provisioning

Audit

Entity events

Personal data

Drag files here, or click to select files.

Login

john.doe

First name

John

Surname

Doe

Personal number

Titles before

Titles after

E-mail

Users e-mail

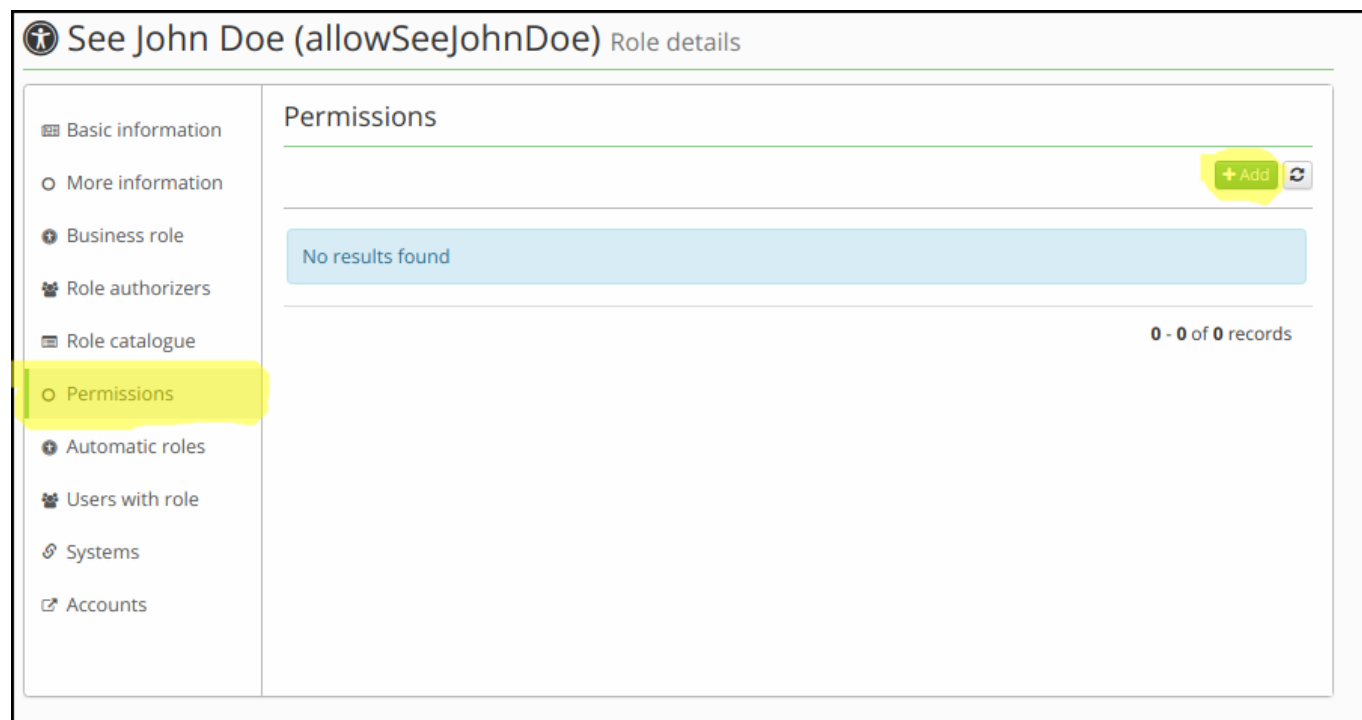
Phone

Phone number

Note

## Step 2. - Create codeable evaluator for role

For this step a role must exist so we can hook a new evaluator to this role. If you don't have such a role, please create one. Once you have a role, go to its submenu **Permission** and then add new evaluator by button **Add**.



## Step 3. - Define new evaluator

On a modal window, select:

- Entity type: **IdmIdentity**.
- Evaluator type: **CodeableEvaluator**

Then, application will display an evaluator configuration dialog with one option marked **identifier**. Put UUID or username of a user (identiti) into this field.

New permission

Role

See John Doe (allowSeeJohnDoe)

Entity type

IDENTITY (IdmIdentity)

Permissions

ReadUpdate

Order

Description

Inactive

Inactive policy will not be applied

Evaluator type

CodeableEvaluator

Share entity by their identifier - uuid or code.

Evaluator configuration

identifier

john.doe

Close

Save

Save the new evaluator. If the action was successful, you can verify new evaluator in the list of active evaluators.

See John Doe (allowSeeJohnDoe) Role details

Basic Information

More information

Role attributes

Business role

Incompatible roles

Role authorizers

Role catalogue

Permissions

Automatic roles

Users with role

Systems

Accounts

Permissions

+ Add

Filter

Cancel filter

Filter

Entity type	Permissions	Evaluator type	Configuration	Description	Inactive	Order
IDENTITY (IdmIdentity)	Read Update	CodeableEvaluator	Identifier:john.doe		<input type="checkbox"/>	

1 - 1 of 1 records

Step 4. - Add role to user

Choose some other user (the user you want to give the permission to) and add him the role you configured. This user now obtains a new permission as defined in the evaluator.

Add roles

Environment

Environment for which the role is intended.

Role

See John Doe (allowSeeJohnDoe)

Contracted position

Default

Connection to organization or another tree structure

Valid from

Valid till

Close

Set

Richard Roe (richard.roe) User details

Richard Roe (richard.roe)

Personal data

More information

Change password

Roles

Permissions

Positions

Subordinates

Authorize roles

Accounts

Provisioning

User roles

Requests

Directly assigned roles

Manage authorizations

Role	Contracted position	Other positon	Valid from	Valid till	Automatic role	Id
See John Doe (allowSeeJohnDoe)	Default					5d6b255

1 - 1 of 1 records

Roles assigned by business roles

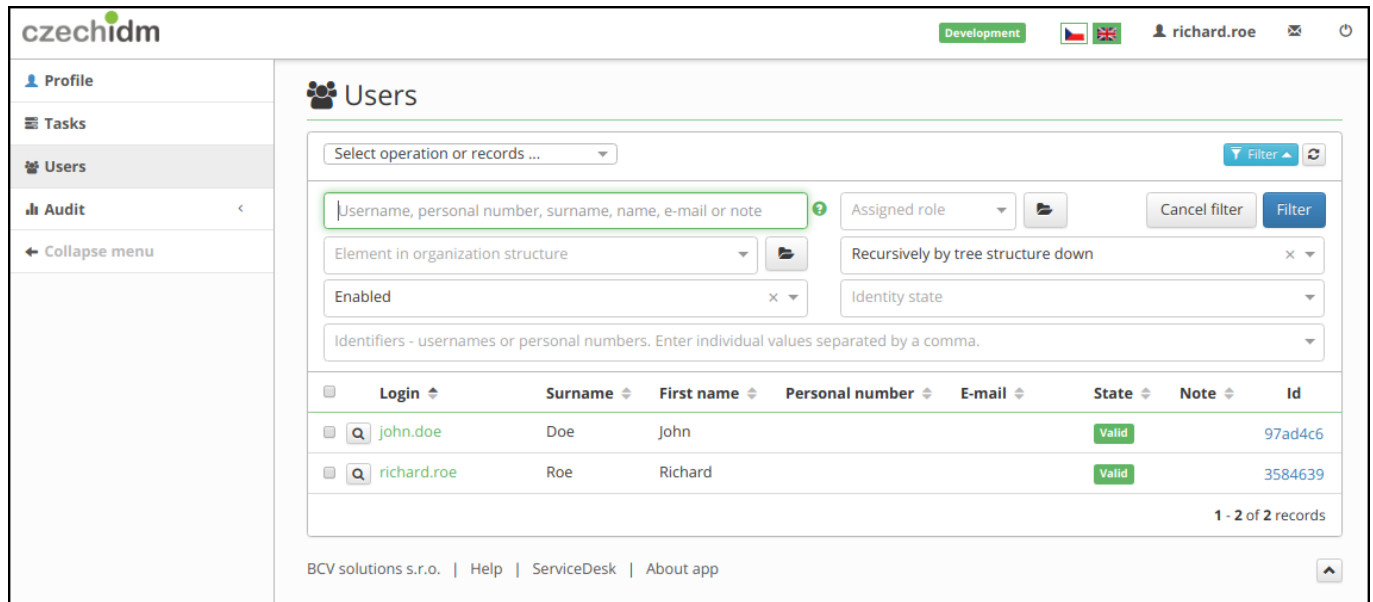
No results found

Step 5. - Result

Final result. We assigned a role to the richard.roe. This user now can see the john.doe identity in IdM.

https://wiki.czechidm.com/

Printed on 2024/03/06 23:32



The screenshot displays the 'Users' management page in the CzechIDM application. The sidebar on the left includes links for Profile, Tasks, Users (selected), and Audit. The main content area features a search bar with the placeholder 'Username, personal number, surname, name, e-mail or note'. Below the search bar are several filter options: 'Assigned role', 'Element in organization structure', 'Enabled', 'Recursively by tree structure down', and 'Identity state'. A table of users is shown below the filters, with columns for Login, Surname, First name, Personal number, E-mail, State, Note, and Id. Two users are listed: john.doe and richard.roe, both with a 'Valid' state. The footer of the page includes the text 'BCV solutions s.r.o. | Help | ServiceDesk | About app'.

Login	Surname	First name	Personal number	E-mail	State	Note	Id
john.doe	Doe	John			Valid		97ad4c6
richard.roe	Roe	Richard			Valid		3584639

## Define evaluator with restriction for access to one certification authority

This tutorial is similar to the first one. Instead of an identity, we grant user a permission to work with some certificate authority. For example, this restriction can be used for adding permissions to request certificates only from particular certificate authority authority. If you have multiple CAs defined, you can create one role for each of your CAs and then assign those roles to users as necessary.

### Step 1. - Get code of certification authority

Get the **code** of certification authority.



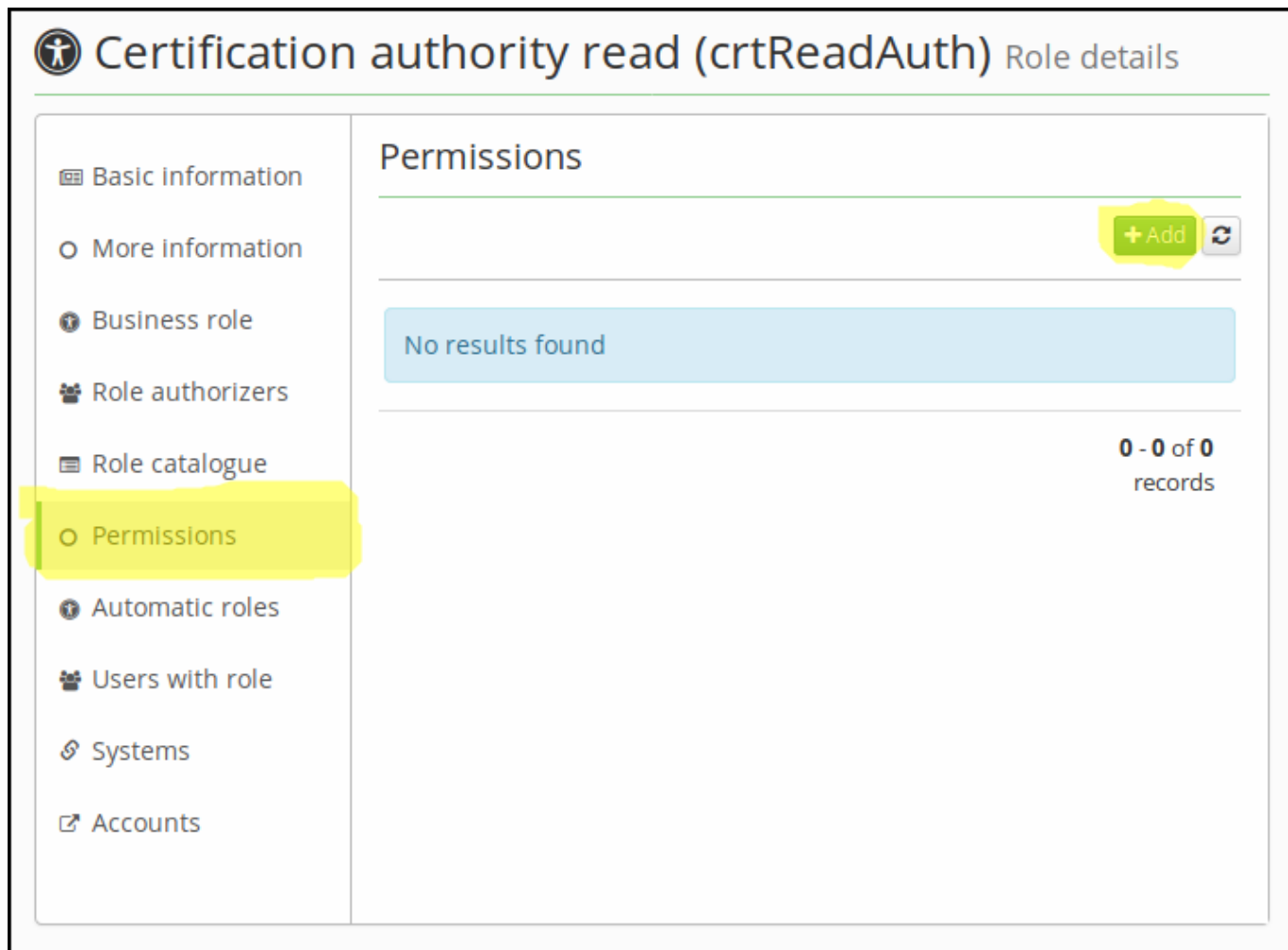
**Code** can be used in 1.3.0 (and later) version of crt module. If you use lower version of crt module, you have to use UUID as an identifier. UUID can be found in browser URL when you open the certificate authority detail page.

The screenshot shows the 'czechidm' web application interface. The top navigation bar includes the logo, a 'Development' status indicator, language flags (Czech and English), a user profile 'admin', and system icons. The left sidebar contains a menu with items: Profile, Tasks, Users, Organization, Roles, Systems, Virtual systems, Certificates (highlighted), Certificates (sub-item), Authorities (highlighted), and Audit. The main content area is titled 'Certificate authority detail' and contains the following form fields:

- Code:** A text input field containing 'testCertificateAuthority' with a red asterisk indicating a required field.
- Password policy for validation:** A dropdown menu currently showing 'Password policy for validation'.
- Password policy for generating:** A dropdown menu currently showing 'Password policy for generating'.
- Driver:** A dropdown menu currently showing 'caw-driver' with a close button (X) and a dropdown arrow.
- Identifier:** A text input field containing 'one' with a red asterisk indicating a required field.

## Step 2. - Create codeable evaluator for role

For this step you have to have a role created (if you do not have such a role, create it). We will now hook an evaluator to the role. For this, go to role's submenu **Permission** and then add new evaluator by clicking the **Add** button.



## Certification authority read (crtReadAuth) Role details

- Basic information
- More information
- Business role
- Role authorizers
- Role catalogue
- Permissions**
- Automatic roles
- Users with role
- Systems
- Accounts

### Permissions

**+ Add**

No results found

0 - 0 of 0 records

### Step 3. - Define new evaluator

On modal window, select:

- Entity type: **CrtAuthority**.
- Evaluator type: **CodeableEvaluator**.

Application will display an evaluator configuration dialog with one option marked **identifier**. Fill in the identifier of certificate authority.

## New permission

**Role**  
Certification authority read (crtReadAuth)

**Entity type**  
Certificate authorities (CrtAuthority)  
If entity type is not selected, then all types will be evaluating

**Permissions**  
Read View in select box (autocomplete)

**Order**

**Description**

☐ Inactive  
Inactive policy will not be applied

**Evaluator type**  
CodeableEvaluator  
Share entity by their identifier - uuid or code.

**Evaluator configuration**  
**identifier**  
testCertificateAuthority

[Close](#) [Save](#)

Save new evaluator. If everything is ok, you can see it in the list of existing evaluators.

### Certification authority read (crtReadAuth) Role details

- Basic Information
- More Information
- Business role
- Role authorizers
- Role catalogue
- Permissions**
- Automatic roles
- Users with role
- Systems
- Accounts

#### Permissions

[+ Add](#) [Refresh](#)

	Entity type	Permissions	Evaluator type	Configuration	Description	Inac
<input type="checkbox"/>	Certificate authorities (CrtAuthority)	Read View in select box (autocomplete)	CodeableEvaluator	Identifier:testCertificateAuthority		

1 - 1 of 1 records

## Step 4. - Add role to user

Add a role to some user. This user will now obtain a permission to work with particular certificate

authority (determined by CA identification in the evaluator).

Add roles

Environment

Environment for which the role is intended.

Role

× Certification authority read (crtReadAuth)

×

Contracted position

Default

Connection to organization or another tree structure

Valid from

Valid till

Close

Set

John Doe (john.doe) User details

John Doe (john.doe)

Personal data

More information

Password

Roles

Positions

Subordinates

Authorize roles

Accounts

Provisioning

Certificates

Audit

Entity events

User roles

Requests

Request to change roles

Directly assigned roles

Filter

Role	Code	Environment	Role attributes	Contracted position	Other position	Valid from
<div>× Certification authority read (crtReadAuth)</div>	crtReadAuth			<div>Default</div>		

1 - 1 of 1 records

Roles assigned by business roles

Filter

No results found

0 - 0 of 0 records

Step 5. - Result

Final result - user can see only the certification authority you want him to see.

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

czechidm

Development

john.doe

Profile

Tasks

Users

Certificates

Authorities

Audit

Collapse menu

Certificate authorities

Code	Driver	Inactive	Download	Id
<div>testCertificateAuthority</div>	caw-driver	<div></div>	<div>Certificate</div>	ceef85d

1 - 1 of 1 records

BCV solutions s.r.o.

Help

ServiceDesk

About app

From:

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

Permanent link:

[https://wiki.czechidm.com/tutorial/adm/codeable\\_permission](https://wiki.czechidm.com/tutorial/adm/codeable_permission)

Last update:

2019/05/20 09:01

