

[role](#), [incompatible](#), [business](#), [automatic](#), [SoD](#), [Segregation](#), [Duties](#)

# Roles

A role in CzechIdM is an entity representing a set (1 or more) of permissions on the end system or in CzechIdM itself ([permission](#)). From the perspective of the identity manager, it does not matter whether the user acquires an account in a specific application, is placed in a group in LDAP, his indication is set to “can use VPN”, or permission is set for him in the application. In all these cases, a role is assigned. A simplification carried out like this allows general rules to be applied for assigning all types of permissions (~roles) in the same way.

Users acquire roles:

- [automatically](#) - according to the organizational placement of the identity, or identities attributes like address or company.
- manually
  - [by request](#) in the CzechIdM self-service or by a CzechIdM administrator.
  - [copying](#) from an existing user.

Request for a role [can be approved](#) by a specific user, usually helpdesk, user's manager or IT security.

## Business roles

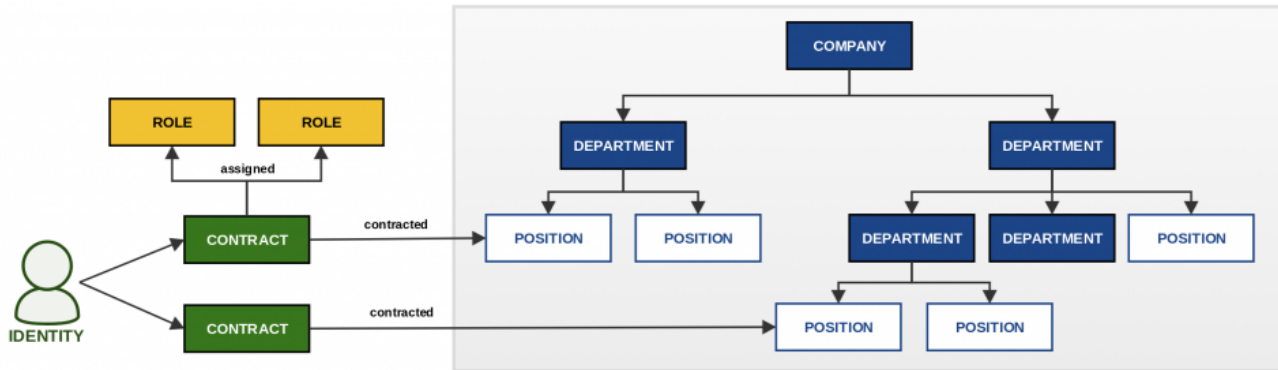
Roles can be aggregated into [business roles](#). Provided role A is a subrole of role B, if role B is assigned (no matter how - automatically or manually) to the user, he or she acquires role A as well.

## Incompatible roles (segregation of duties)

If an identity should not be placed into Security Group A and Security Group B in MS Active Directory at the same time, we can ensure it via CzechIdM mechanism of [incompatible roles](#).

## Roles and contracts

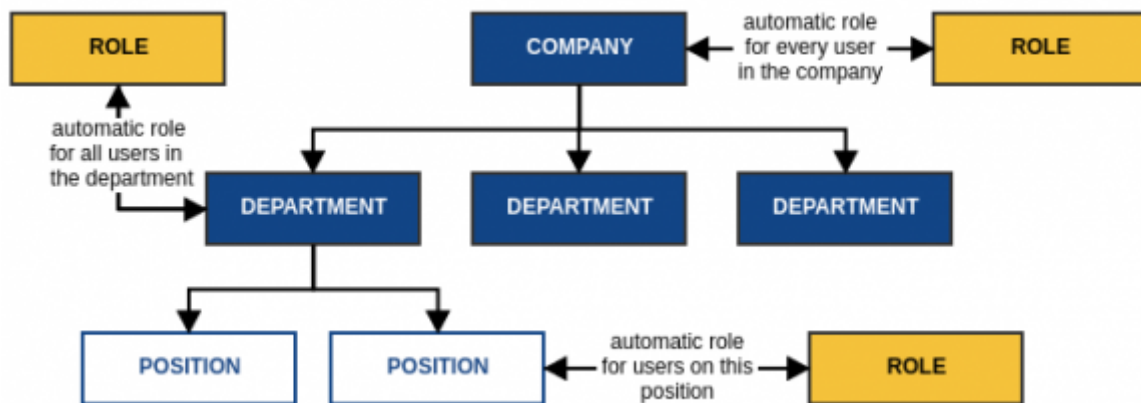
Roles are assigned to users via their contracts. If a contract is not valid (time validity) the roles on the contract are removed. In other words, the identity loses roles permissions in IdM and rights in connected systems. Since IdM13.0.17 is function which automatically prefilled start date of contract it is possible to update it freely.



## Automatic roles

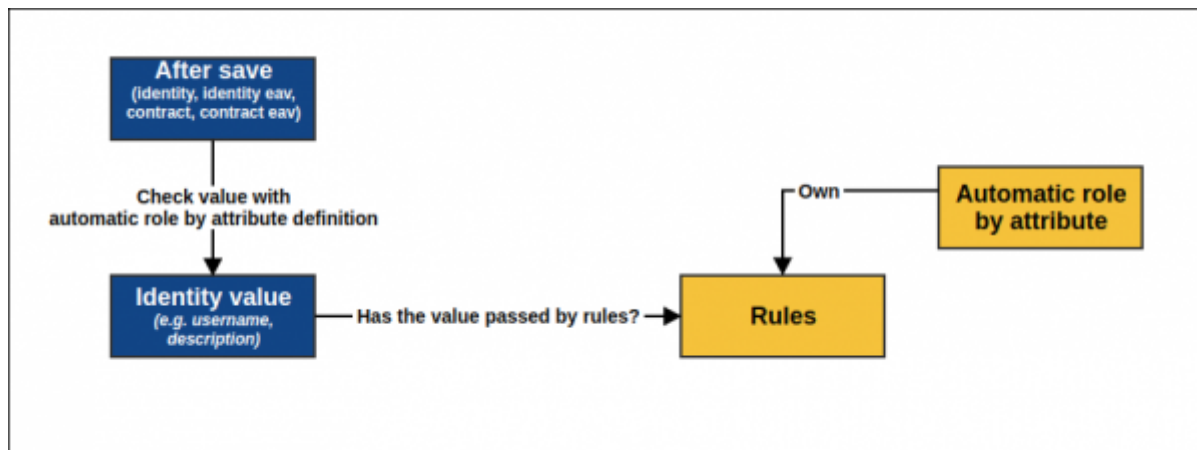
### By org. structure

The role can be linked to a Tree structure (e.g. a position in organizational structure). That role is assigned to and removed from a user based on adding/removing the user (via their contract or other contract position) to/from the organizational tree structure. If a contract is not valid yet, roles are assigned but are disabled until the contract starts.



### By identity attributes

The role can be linked by value in attribute (value can be stored in Identity, Identity extended attribute, Contract and Contract extended attribute). That role is assigned to and removed from a user based on the value in the specific attribute. Recalculating of this automatic roles is done after saving the identity, identity extended attribute attributes, contract, and contract extended attribute attributes. All necessary attributes that define automatic role by attribute are defined by the agenda "Automatic role by attribute".



## Roles and accounts

Roles can also be assigned directly to accounts. This is particularly when a user has multiple accounts and we want the role to apply to only one account or when we are managing technical accounts.

## Read more

### Admin guide

- [Icons and description of roles](#)
- [Copy roles](#)
- [Authorization policies overview](#)
- [Permissions Setting Mechanism](#)
- [Automatic roles overview](#)
- [Incompatible roles](#)
- [Assigned roles deduplication](#)

### Admin tutorials

- [Creating a role](#)
- [Defining permissions for a role](#)
- [Creating an automatically assigned role by organization structure](#)
- [Creating an automatically assigned role by identity attribute](#)
- [Copying assigned roles from one user to another](#)
- [Create a codeable evaluator](#)

### Devel guide

- [Authorization policies: base interfaces and classes](#)
- [Automatic roles by organization structure: heredity of roles](#)
- [Automatic roles by attribute, rules, and recalculation](#)

- [Cloning roles](#)

From:

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

Permanent link:

<https://wiki.czechidm.com/devel/documentation/roles>

Last update: **2024/08/06 07:36**

