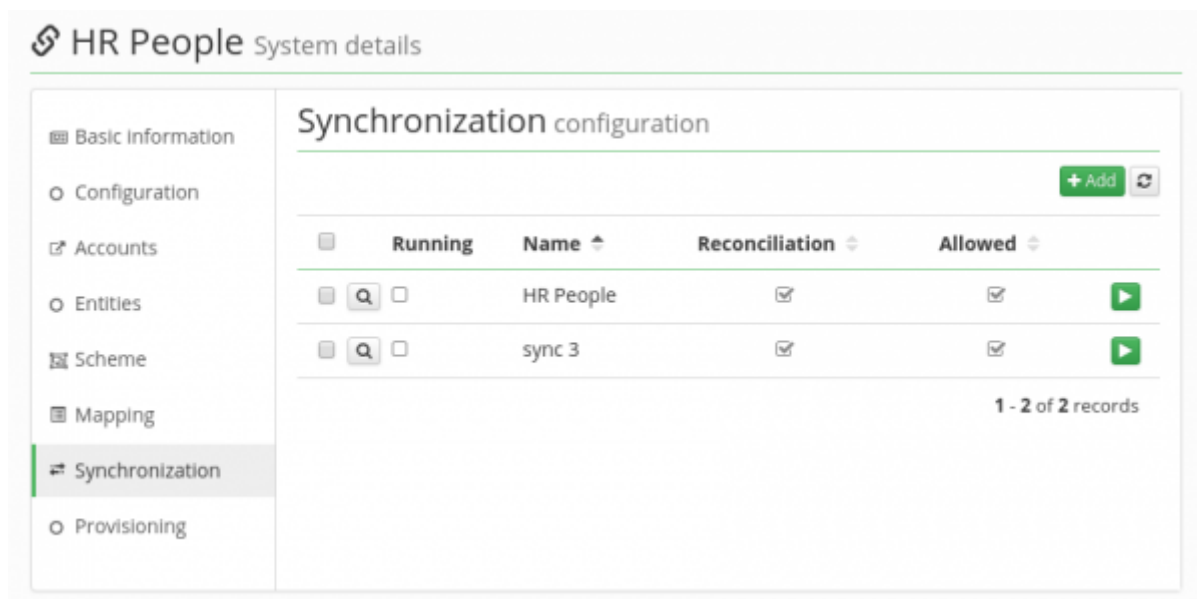


# Synchronization - generic system synchronization configuration

[Synchronization can be configured in Systems → System detail \(magnifying glass sign\) → Synchronization](#). If it is desired to add a new synchronization for the system, use the green Add button. If the configuration of already set synchronization is to be done, the magnifying glass sign should be clicked on.



The screenshot shows the 'HR People System details' page. On the left is a sidebar with navigation links: Basic Information, Configuration, Accounts, Entities, Scheme, Mapping, Synchronization (highlighted), and Provisioning. The main content area is titled 'Synchronization configuration' and features a '+ Add' button and a refresh icon. Below this is a table with columns: Running, Name, Reconciliation, Allowed, and an action column. Two records are listed: 'HR People' and 'sync 3'. Both have checkboxes for Running, Reconciliation, and Allowed, and a play button in the action column. At the bottom right of the table, it says '1 - 2 of 2 records'.

Running	Name	Reconciliation	Allowed	
<input type="checkbox"/>	HR People	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	sync 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

## Creating a new synchronization

### Basic synchronization options

## Synchronization details

Settings
Specific settings
Filter
Logs

☒ Allowed  
☒ Reconciliation  
Executes full reconciliation instead of synchronization. Synchronization will be executed for all accounts without filter. Search for missing accounts will be executed for all entities in CzechIdM.

**Name**

**Set of mapped attributes**

**Correlation attribute**

**Token**

**Description**

There are following options in the basic settings:

- **Allowed** - only allowed synchronizations can be started, either manually or as [scheduled tasks](#)
- **Reconciliation** - if the synchronization should run in the "full" reconciliation mode regardless of the value of the last synchronization `_token_` (see [Reconciliation](#) for more details)
- **Name** - name of your choice
- **Set of mapped attributes** - those are attributes from [attributes mapping](#) prepared earlier.
- **Correlation attribute** - the attribute used for matching accounts and identities (i.e. finding the entities to be linked). The correlation attribute can be any attribute from the attribute mapping of the synchronization. The correlation attribute is always required in current version of CzechIdM, since the object vs entities states are computed before operations take place.
- **Token** - the value is the token of the last synchronization run. If the token is e.g. timestamp, the value can be time of last synchronization run. It is recommended to leave the option its current value.
- **Description** - optional description of the synchronization definition

## Synchronization states and actions

Linked
<div>Action *</div> <div>Update entity</div> <div>Workflow</div> <div>Select or type to search ...</div>
Not linked
<div>Action *</div> <div>Create link and update entity</div> <div>Workflow</div> <div>Select or type to search ...</div>
Missing entity
<div>Action *</div> <div>Create entity</div> <div>Workflow</div> <div>Select or type to search ...</div>
Missing account
<div>Action *</div> <div>Ignore</div> <div>Workflow</div> <div>Select or type to search ...</div>

During the process of synchronization, objects on connected system and entities in CzechIdM are compared and the state for every object is computed:

- **Linked** - Object and Entity has been previously (by synchronization or manually) linked. The following actions can be performed on object and entity in this situation:
  - **Update entity**: This updates the CzechIdM entity linked to the connected system object. The update is done on the basis of synchronization attribute mapping. After saving the entity, the standard provisioning is called.
  - **Update account**: This calls the standard provisioning. Synchronization only calls the event, it does not perform provisioning itself. So if the provisioning is asynchronous, the synchronization does not wait for the provisioning to finish.
  - **Remove link**: This deletes the link between the CzechIdM entity and connected system object. It does not perform editing of the CzechIdM entity itself, it does not call provisioning.
  - **Remove link and appropriate roles**: This removes the links, as in the previous case. In case of CzechIdM identity it also removes roles that are linked with this account.
  - **Ignore**: This action does not perform any active operation.
  - **Ignore and do not log**: This action does not perform any active operation. Additionally, it does not create a log entry in the synchronization log.
- **Not Linked** - This is a situation when there is no link between the entity in CzechIdM and object in connected system. Since the link does not exist yet, the identity has been found using a **correlation attribute**. The following actions can be performed in Not Linked situation:
  - **Create link**: This creates a link between CzechIdM entity and object. Editing of the identity itself is not done, provisioning is not called.
  - **Create link and update entity** (since 8.0): A link is created in the same way as in the previous case. In addition, the linked entity is updated on the basis of synchronization attribute mapping. After saving the entity, the standard provisioning is called.
  - **Create link and update account**: A link is created in the same way as in the previous case. In addition, the account on the end system is updated - an event for running provisioning is called.

- **Ignore:** This action does not perform any active operation.
- **Ignore and do not log:** This action does not perform any active operation. Additionally, it does not create a log entry in the synchronization log.
- **Missing Entity** - This is a situation when there is no entity in CzechIdM matching object in the connected system. The following actions can be performed in this situation:
  - **Create entity:** creates an entity in CzechIdM and a link it to object in connected system. The creation is done based on the attribute mapping chosen in synchronization configuration. The creation of entity calls provisioning.
  - **Ignore:** This action does not perform any active operation.
  - **Ignore and do not log:** This action does not perform any active operation. Additionally, it does not create a log entry in the synchronization log.
- **Missing Account** - This is a situation when there is no object on the end system matching the entity in CzechIdM. The following actions can be performed in this situation:
  - **Create account:** Synchronization calls entity provisioning, which leads to creation of an object on the connected system.
  - **Remove entity:** This deletes the entity in CzechIdM and the link to object in connected system.
  - **Remove link:** This deletes the link between the entity in CzechIdM and object in connected system. Editing of the entity itself is not done, provisioning is not called.
  - **Remove link and appropriate roles:** This removes the links, as in the previous case, however, it also removes the linked identity roles. In other words, it removes the roles which were assigned to the identity by the account.
  - **Ignore:** This action does not perform any active operation.
  - **Ignore and do not log:** This action does not perform any active operation. Additionally, it does not create a log entry in the synchronization log.

## Specific synchronization options

### Synchronization details

Settings
Specific settings
Filter
Logs

**Default role**  

AD user

×

If the synchronization creates a link between an Identity and an account, this role will be assigned to the Identity. This assignment will be linked to the main contractual relationship of the Identity.

**Behavior of the default role for inactive identities**  

DO\_NOT\_LINK - Don't link the account and end its processing, if there is no valid contract for the default role

×

How to behave if the identity doesn't have any valid contract for assigning the default role.

☐ After end, start the automatic role recalculation  
 After successful synchronization will be start recalculation of all automatic role by attribute.

☐ Create default contracts for new Identities  
 During the creation of new Identities, will be also created default contract. For create new default contract must be enabled function 'Creating default contracts' in application configuration.

Back
Save and continue

You can configure additional synchronization options for specific uses:

- **Default role** - The value can be any role in CzechIdM. This value is used in the case that the synchronization links an existing system account to an existing or a new identity in CzechIdM. If the default role is specified, this role will be assigned to the identity for its main valid contractual relationship. Then the link to the account will be created with the property **Assigned by role** set to the default role. If the default role is empty, the link to the account will be created as well, only without the property "Assigned by role".
  - The main use-case for this option is **initial linking of accounts during the reconciliation** of a system, where the accounts will be further managed by CzechIdM - e.g. LDAP, AD. The default role will be usually configured for provisioning on this system, see [Provisioning - role and queue configuration](#).
  - This option is supported in the following actions of the synchronization: Missing Entity → Create entity, Not Linked → Create link, Create link and update entity, Create link and update account.
  - The role assignment skips an approval process - the corresponding role request will be processed **Without approval**.
  - If the identity doesn't have any valid contractual relationship, the synchronization will take action based on the **Behavior of the default role for inactive identities** option (see below).
  - Note that the role will be assigned to the identity regardless of other role assignments of the identity. So even if the identity already had the same role assigned, the role would be assigned again and the created account's link will be related to this new assignment.
- **Behavior of the default role for inactive identities** (since 9.3.0): This option is required in the case that a **Default role** (see above) is specified for the synchronization. If the synchronized identity doesn't have any valid contract, then the default role can't be assigned to it. So you must specify by choosing one of the following options, how the synchronization should behave in such situations:
  - **DO\_NOT\_LINK**: The account won't be linked and the identity won't be updated or created at all. The result of processing this item is **Ignore**. Typically, you will use this option when you connect a system to IdM in which you expect some old unwanted accounts, and you don't want to manage them anymore.
  - **LINK\_PROTECTED**: The account will be linked to the identity without the property "Assigned by role", but it will be put into the [protected state](#). The length of the protection is based on the last expired contract of the identity and the **Length of protection interval** configured in the provisioning mapping for this system. Note that this can be in the past if you have a short protection interval, so the account can be deleted as soon as the task for deleting expired accounts ([AccountProtectionExpirationTaskExecutor](#)) starts. If the identity doesn't have any expired contract (it has no contracts, or only future contracts), the current date is used as the start of the protection. Typically, you will use this option if you connect a system to IdM in which you intentionally keep old accounts, and you want to have some control over these accounts by IdM (e.g. if the original owner got a new valid contract, the original account should be reused). This option requires an existing [provisioning mapping](#) with **Account protection** enabled, otherwise the synchronization wouldn't start.
  - **LINK**: The account will be just linked to the identity without the property "Assigned by role". The result of processing this item is **Warning**, because such account is not managed by role assignment - it will exist as long as the corresponding identity exists regardless of its (in)activity. This option is for backward compatibility mainly, because such was the behavior in the versions < 9.3.0.
- **After end, start the automatic role recalculation** - After synchronization correctly ended recalculation of automatic role will be started.
- **Create default contracts for new identities** (since 8.2.0) - If a new identity is created

during synchronization, a default contract will be created for the identity. To use this feature, you must also enable creating default contracts in the [application configuration](#) (`idm.pub.core.identity.create.defaultContract.enabled=true`). Note that default contracts weren't created in the versions 7.6 - 8.1.x.

From:

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

Permanent link:

<https://wiki.czechidm.com/tutorial/adm/synchronization>

Last update: **2022/04/29 07:13**

