Installation of CzechIdM - Final steps

installation, quickstart, configuration, userRole, email

We presume that CzechIdM is already installed as described in Installation of CzechIdM - Linux - CentOS8 or Installation of CzechIdM - Windows.

This tutorial contains some recommended steps to review and finalize the configuration for the production-ready version of CzechIdM.

Systems & Virtual systems

First of all, activate the module **acc** in **Settings → Modules** by clicking on the button **Activate**.

If you want to try CzechIdM account management without directly connecting some system, you could start with the Virtual systems. To use this, activate the module **vs** at **Settings → Modules** by clicking on the button **Activate**.

Notifications & e-mails

Sending of e-mails is turned off by default; the e-mails are only logged in the **Notifications → E-mails history**. However, when you start to use CzechIdM, some processes should be able to notify the users. Configure the following:

- Emailer - add the configuration properties for SMTP server and e-mail sending mode in the **Settings → Configuration**
- Review and adjust the standard notifications sent by CzechIdM according to your needs. **This is important so IdM behaves as you expect!**

Password policy

Go to Settings → Password policies and set the password policy according to your security standards.

It's recommended to set temporary blocking login after unsuccessful login attempts.

If you want to use **Maximum password age**, you will probably want to notify users when their passwords are going to expire. To do so, schedule the tasks PasswordExpirationWarningTaskExecutor (notify users before the password expiration) and PasswordExpiredTaskExecutor (notify users when their password expired).

Allow users into CzechIdM

Fix Me! For 10.5+, userRole is created by default - Init application and data. Change this section accordingly.

In the fresh installation, users without any assigned role can do nothing after logging into CzechIdM.

Typically, you want to enable the users to see their profile, request for roles or change their password. This is done by a special role called **userRole**. Create the role and add Permissions to it. Recommended settings is written in the example permissions for userRole.

Users may authenticate by their local CzechIdM password, or you may configure authentication against some of the connected systems - typically AD or LDAP (Authentication against end system). Or you may configure SSO.

Configure the approval process

Manual role assignment is always done by role requests. In the fresh installation, the requests will be automatically approved, because no approvers are set yet.

If you want to enable users to request a role change, you should also set some approval processes for their requests. The configuration options are described here.

Configure managers

Managers and guarantees of the contracts can be included in the approval process or they could manage their subordinates (if you set it in the userRole). If you use these features, make sure that CzechIdM uses a correct algorithm for evaluating managers and subordinates relationship.

The default algorithm evaluates the managers/subordinates by their position in the organizational structure and also includes directly set guarantees. This is set by DefaultManagersFilter and DefaultSubordinatesFilter.

Example:

```
## identity filters
## subordinates by standard tree structure (manager will be found by
contract on parent node)
idm.sec.core.filter.IdmIdentity.managersFor.impl=defaultManagersFilter
idm.sec.core.filter.IdmIdentity.subordinatesFor.impl=defaultSubordinatesFilt
er
```

If you don't want to use organizational structure for evaluating the managers - typically if it's the structure of departments and the managers and subordinates are at the same level in the structure - use rather GuaranteeManagersFilter and GuaranteeSubordinatesFilter.

Example:

```
## identity filters
idm.sec.core.filter.IdmIdentity.managersFor.impl=guaranteeManagersFilter
idm.sec.core.filter.IdmIdentity.subordinatesFor.impl=guaranteeSubordinatesFilter
```

Configure subordinates provisioning

Sometimes, we provision some details about the manager to the identity accounts. E.g. the attribute "manager" in Active Directory is the link to the user's manager. To make this link up-to-date, IdM does provisioning for new and original subordinates of the manager every time, when the manager's contract changes.

If you don't need this functionality, which can be time consuming, switch it off like this:

```
idm.sec.acc.processor.identity-contract-provisioning-processor.includeSubordinates=false
idm.sec.acc.processor.identity-contract-before-save-processor.includeSubordinates=false
```

Configure password reset for all systems including IdM

Please try check you project if you want reset password to all connected systems including CzechIdM after user's state will be evaluated from disable state to enabled state. This change is processed by processor **IdentitySetPasswordProcessor (acc-identity-set-password-processor)**. You can disable it by configuration property or GUI agenda of processors (it is equivalent).

Schedule the tasks

This section is obsolete, most important tasks are scheduled by default in newer versions of CzechIdM

Review the scheduled tasks in **Settings → Task scheduler**.

By default, connected system's synchronization is not scheduled. To do so, you have to add it. Add a new scheduled task SynchronizationSchedulableTaskExecutor, fill in the Synchronization Save the event and click Add under Scheduled starts. To run the event periodically, set a CRON trigger.

If you don't want to automatically delete old records in the provisioning archive, remove scheduled run from the DeleteProvisioningArchiveTaskExecutor.

If you want to use validity of the contracts and standard HR processes in CzechIdM, make sure that HR processes will be started every day. There are 2 options:

- Schedule the Hr…Process tasks.
- Ensure that synchronization of contracts from some resource will run every day and the "After end, start the HR processes" option is ticked in the configuration of this synchronization.

Start the 3 Hr...Processs tasks at least once **manually**, otherwise they won't be started after end of synchronization.

If you want to use the Account protection system for some connected system, you must schedule the AccountProtectionExpirationTaskExecutor to start once every day.

If you want to use **Maximum password age**, schedule the tasks mentioned in Password policy section to run once every day.