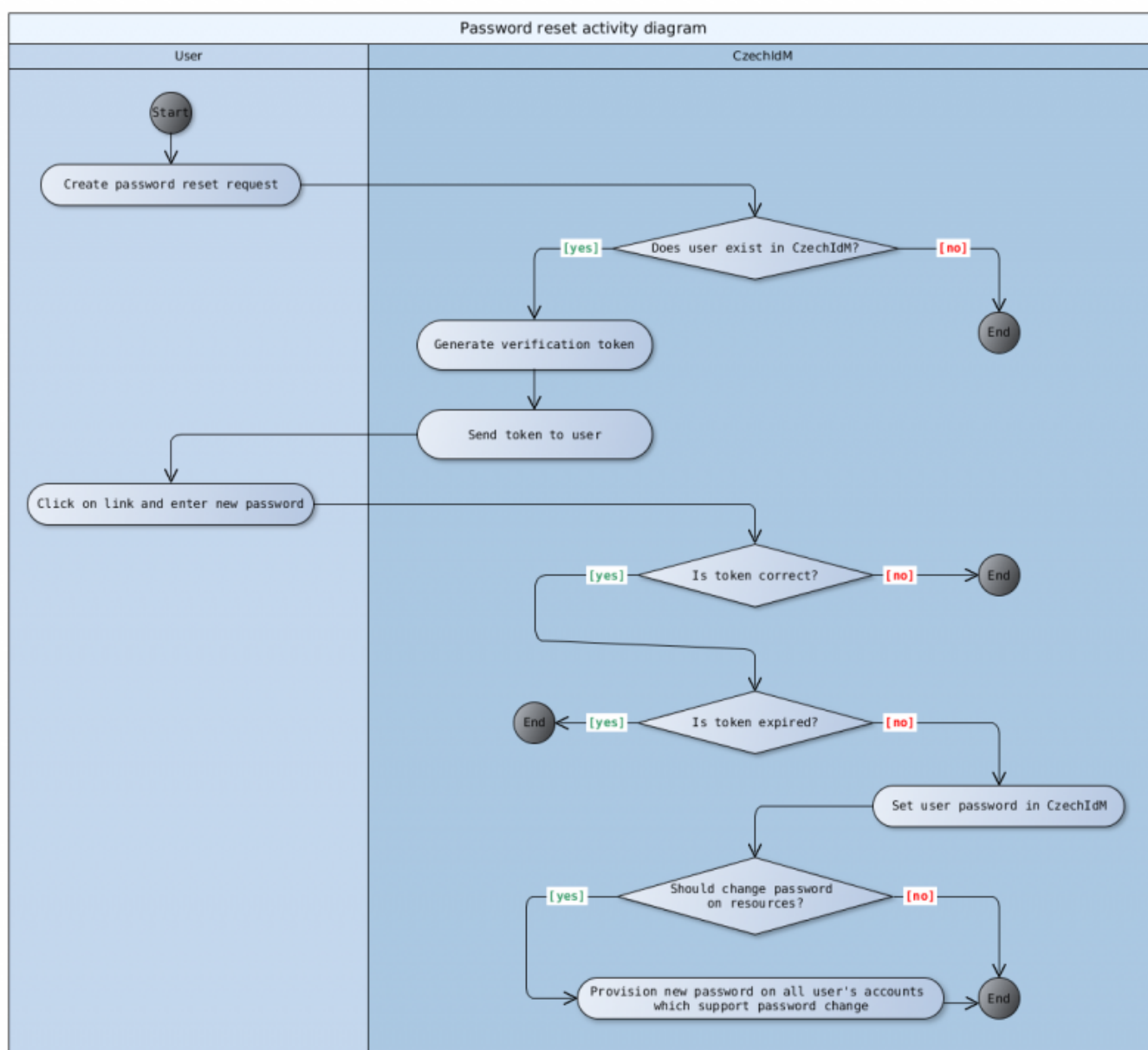# Modules - pwd-reset: How to reset forgotten password?

This module provides the functionality of password reset or, in other words, the recovery of a forgotten password.

How does it work?

Process of restoring your forgotten password

Users can restore their forgotten password via the password reset module. User can start the process on CzechIdM´s login page by clicking on "Forgotten password" link. In next step user it is required to

enter an account identifier.

Forgotten password

For now, the identity's email or login are supported and admin can use a configuration property to select which of these (or both) can be used. User then confirms password reset request by clicking on submit button. CzechIdM then generates validation token and stores it in the password reset request along with the time of creation. Validation token is then being sent to user via notification. Administrator can edit the notification using standard CzechIdM notification functionality. Notification is sent to topic "passwordResetRequestCreated" with SUCCESS level.

After clicking on the link, which contains verification token in GET parameters, user is asked to fill in new password. If the password change succeeds (password validation is OK and user can change their own password), then the user can log in to CzechIdM with a new password.

New password

                                                                 *

Re-enter new password

                                                                 *

Cancel   Set password

Password generating

Password reset module has a process for generating new password by default based on a password policy for IdM. The form for password generating is a part of the password change component. To generate password to an end system it is necessary to enable the event type PASSWORD_GENERATE for processor in acc (processor.identity-password-provisioning-processor).

Password generating is available by permission IDENTITY PASSWORDRESET (and also APP_ADMIN).

> ⚠ By default, the "Password generate" form displays all end system accounts, but the password **will not** be provisioned to the end system accounts. So remember to add the event type PASSWORD_GENERATE to the configuration property `idm.sec.acc.processor.identity-password-provisioning-processor.eventTypes` (as written above) to avoid confusion.

Reset password in user´s system accounts

Password reset module changes user's passwords only to their CzechIdM account. To reset passwords to end system accounts you need to have the acc module enabled and do a little bit of configuration. You need to set IdentityPasswordProvisioningProcessor and PasswordValidateProcessor to respond to PASSWORD_RESET event type. You can do it by setting

```
idm.sec.acc.processor.identity-password-provisioning-
processor.eventTypes=PASSWORD,PASSWORD_RESET,PASSWORD_GENERATE
idm.sec.acc.processor.identity-password-validate-
processor.eventTypes=PASSWORD,PASSWORD_RESET
```

After the password reset, notification is sent to user with system names and accounts, where password has been changed. This processor has to be enabled with setting

```
idm.sec.core.processor.identity-password-change-
notification.eventTypes=PASSWORD,PASSWORD_RESET
```

Now IdM will also reset password on all user accounts which support it.

Installation

Download the module distribution package. The package contains a backend folder. Your IdM Tomcat installation we call IDM in the following example.

1. Copy the content of the backend folder into your tomcat IdM installation - [IDM]/WEB-INF/lib
2. Set correct access rights to the files if needed (`chown tomcat:tomcat [IDM]/WEB-INF/lib/*`)
3. Restart the IdM application server (`service tomcat restart`)
4. Log in to CzechIdM as a privileged user and go to Settings → Modules and enable the pwd-reset module.
5. Go to the configuration and configure required properties (see below).
6. Add the event types PASSWORD_RESET and PASSWORD_GENERATE for processors as [described above](), if you want to reset and provision generated passwords for end system accounts (typically, you do).

Configuration

The module provides following configuration properties:

Property	Description
idm.pub.pwdreset.allowed.attrs	REQUIRED. List of identity attributes (separated by comma) which can be used by user to identify their account when reseting password (username, email and personal number are available for now)
idm.sec.pwdreset.token.ttl	How many minutes is verification token valid (default is 60 minutes)
idm.pub.pwdreset.identity.passwordReset.public.idm.enabled	Boolean value to enable/disable password reset and password generate for CzechIdM system. Default value is true (password reset and password generate is enabled).
idm.sec.pwdreset.debug	Debug password reset, if value is true token will be visible in notification in IdM.
idm.sec.pwdreset.token.length	Length of generated verification tokens - Default is 25

Video Guide

[How to reset password]() - czech language

FAQ

How to allow password reset in CAS?

For CAS docker set env variables:

```
- CAS_CUSTOM_FRONTEND_PASSWORDRESET_DISPLAY=true
- CAS_CUSTOM_FRONTEND_PASSWORDRESET_LINK=<idm url>/#/password-reset
```

From:
 https://wiki.czechidm.com/ - **CzechIdM Identity Manager**

Permanent link:
https://wiki.czechidm.com/tutorial/adm/modules_pwdreset

Last update: **2023/11/09 11:57**