Recovery Dashboard Widget

The Recovery Dashboard Widget (RecoveryWidget) is a Registry Dashboard plugin that enables self service account recovery tools.

- Configuration
- Considerations
- Confirmation Resend Mode
- Identifier Lookup Mode
- Authenticator Reset Mode

Configuration

1. This is a non-core plugin, see Installing and Enabling Registry Plugins for more information.
2. The Recovery Widget supports several modes, each of which can be enabled independently of the others. See the description of the available modes, below. Links for each enabled mode will be presented when the Widget renders in the Dashboard.

Considerations

Because many of the recovery tools are designed to help a user regain access to services, the Dashboard to which they are attached should probably be configured with a Visibility of *Unauthenticated Users*.

Confirmation Resend Mode

Confirmation Resend Mode allows an Enrollee to request the resend of a confirmation email sent as part of an Enrollment Flow. It is enabled by ticking *Enable Confirmation Resend* in the Widget configuration.

The Enrollee is asked to provide an Email Address or the authenticated Identifier associated with their Petition record. Unlike the other modes, *Confirmation Resend* allows entry of an unverified Email Address because in general the confirmations are to verify an unverified Email Address. The authenticated Identifier, if provided, must be the exact string stored in the Petition's *authenticated identifier* field.

If a matching Email Address or Identifier is found, any pending confirmations on any matching Petitions will be resent. Confirmations are sent to the same address originally emailed as part of the Enrollment Flow. It is not currently possible to change the destination address.

Confirmation Resend only applies to enrollments started via an Enrollment Flow. It does not apply to Default Registry Enrollment.

Identifier Lookup Mode

Identifier Lookup Mode allows a user to request an email containing an Identifier, such as their login username.

To enable this mode, first define a Message Template. The Message Template should have a *Message Context* of either *Authenticator* or *Plugin*. The desired Identifier can be incorporated into the outgoing message using the `(@IDENTIFIER:x)` Message Substitution. (Multiple Identifiers can be incorporated using this technique.)

Select the Message Template in the Widget's *Message Template for Identifier Lookup* configuration.

The user is asked to provide a verified Email Address or any Identifier associated with their CO Person record. If a matching Email Address or Identifier is found, a message (using the Message Template) will be sent to all verified Email Addresses associated with the CO Person. The CO Person record must be in either Active or Grace Period status.

Identifier messages will only be sent to CO People in Active or Grace Period status.

Authenticator Reset Mode

Authenticator Reset Mode allows a user to reset an Authenticator without logging in to Registry.

To enable this mode, first define a Message Template. The Message Template should have a *Message Context* of either *Authenticator* or *Plugin*. The Message Template should include the Message Substitution `(@RESET_URL)`, which will contain the link the recipient should click in order to continue the Authenticator reset process. Identifiers may also be used, as described in Identifier Lookup Mode, above.

In the Dashboard Widget configuration, there are several options to set:

- **Self Service Reset Authenticator**: The instantiation of the desired Authenticator to provide reset services for. Currently, only instances of the Password Authenticator Plugin are supported.
- **Message Template for Self Service Reset**: The Message Template created above.

- **Self Service Reset Token Validity**: The duration of the reset token validity, after which the token will expire and a new token must be requested.
- **Redirect on Self Service Reset**: A URL to redirect the user to after completing the Self Service Reset process.

When *Authenticator Reset Mode* is enabled, two links are generated in the dashboard widget: The first is the link into the Authenticator Reset process, the second is a direct link to the Authenticator management (in case the user still has control of the Authenticator.) Upon clicking the first link, the user is asked to provide a verified Email Address or any Identifier associated with their CO Person record. If a matching Email Address or Identifier is found, a message (using the Message Template) will be sent to all verified Email Addresses associated with the CO Person. The CO Person record must be in either Active or Grace Period status.

If *Authenticator Reset Mode* is subsequently disabled, any pending reset requests will remain active for the duration of their token validity. The only way to bulk invalidate such tokens is to delete them from the database table (`cm_authenticator_reset_tokens`).

Locked Authenticators cannot be reset. Similarly, Authenticators cannot be reset for CO People not in Active or Grace Period status.