

MeemEnroller Plugin

MEEM is the *MFA Enrollment and Exemption Manager*. It is intended to coordinate enrollment in Multi-Factor Authentication. MEEM does not work with any specific technology, but is intended to work with Enrollment Flows and, indirectly, [Authenticators](#).

MEEM has various configuration points, but broadly it is intended to integrate with two Enrollment Flows:

1. A Self Signup or Invitation Flow (the "Initial" Enrollment Flow), used to perform general enrollment into the CO
2. An MFA Authenticator Enrollment Flow, used to set up a Multi-Factor Authenticator for the Enrollee

 The MeemEnroller Plugin is considered Experimental.

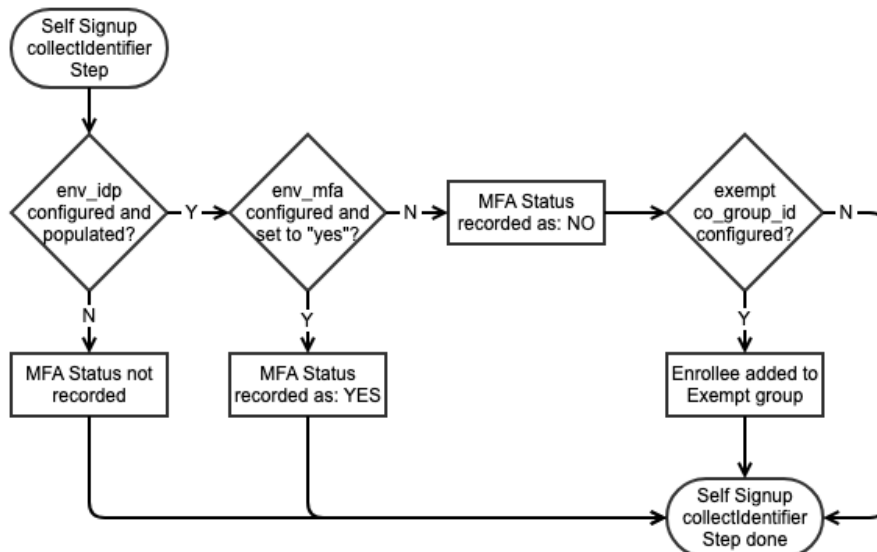
Initial Enrollment Flow

The Initial Enrollment Flow should be considered as usual for Self Signup or Enrollment, including whatever Enrollment Attributes are desired. Beyond that, *Email Confirmation* must be set to either *Automatic* or *Review*. Do *not* Establish Authenticators as part of this flow.

Once the Enrollment Flow is created, attach an Enrollment Flow Wedge using the MeemEnroller Plugin. The following configurations are supported:

- **IdP Identifier Indicator:** If set, this is the name of an environment variable that MEEM will examine during enrollment (after the *Collect Identifier* step) to determine the identifier of the Identity Provider that the Enrollee authenticated with. If this configuration is left blank, MEEM will not record MFA Status (see below).
- **MFA Assertion Indicator:** If set, this is the name of an environment variable that indicates that the Identity Provider asserted MFA. The value of the environment variable must be the literal string yes, though this is subject to change in a future release. This setting is only effective if the *IdP Identifier Indicator* is also set and populated.
- **MFA Exemption CO Group:** If set, this is the CO Group used to track which CO People are currently exempt from MFA. If *MFA Assertion Indicator* configure, and MFA was *not* asserted, the Enrollee will be added to this CO Group. Membership in this CO Group may also be manually managed.
- **Initial MFA Exemption:** If set, when a CO Person is automatically added to the *MFA Exemption CO Group*, the memberships will be set to expire the configured number of hours after being created, allowing for a "grace period" before MFA is required. Note a [Registry Job Shell](#) must be configured to ensure timely reprovisioning of expired CO Group Memberships. See also: [Registry Validity Dates](#).
- **MFA Enrollment Flow:** The Enrollment Flow that establishes an MFA Authenticator, described below.
- **Enable MFA Setup Reminder Splash Page:** Whether the MFA Setup Reminder Splash Page (described below) is enabled for this configuration.
- **Return URL Allow List:** If the *MFA Setup Reminder Splash Page* is enabled, a list of regular expressions (PHP syntax, including the delimiter, one regular expression per line) for permitted return URLs. Note that all Registry URLs are automatically considered valid, and so need not be added to this list. (ie: There is no need to adjust this setting to redirect into the *MFA Enrollment Flow*.)
- **API User:** If set, the API User granted access to the MEEM REST API, described below.

Configuration Flow Diagram



MFA Status

If MEEM is configured to record MFA Status, a database entry will be made recording the MeemEnroller configuration, the CO Person ID, the IdP Identifier, and whether or not MFA was asserted. Note MEEM does not currently update MFA Status outside of the Initial Enrollment Flow.

MFA Status may be examined using the REST API, below.

MFA Authenticator Enrollment Flow

The primary task of the MFA Authenticator Flow is to set up an Authenticator Plugin for use as a second factor. The flow should be configured as follows:

- **Petitioner Enrollment Authorization:** CO Person
- **Identity Matching:** Self
- **Require Approval:** No
- **Email Confirmation Mode:** None
- **Establish Authenticators:** Yes, with the desired Authenticator for MFA *Required*

Do not attach any Enrollment Attributes to the flow.

Once the Enrollment Flow is created, attach an Enrollment Flow Wedge using the MeemEnroller Plugin. Leave all configuration options blank except *MFA Exemption CO Group*, which should be set to the same group as in the MeemEnroller configuration attached to the Initial Enrollment Flow. If the Enrollee successfully establishes the MFA Authenticator, the membership in the exemption group will be removed.

MFA Setup Reminder Splash Page

The MFA Setup Reminder Splash Page is a simple page that can be rendered to remind the Enrollee of the need to set up MFA. The page does not require authentication, as it does not access or display privileged information. The page will render when *Enable MFA Setup Reminder Splash Page* is enabled, and can be accessed using a URL of the form

`https://myserver/registry/meem_enroller/meem_reminders/remind/<n>?countdown=<c>&return=<r>`

where

- **n:** The MeemEnroller configuration ID (ie: `cm_meem_enrollers:id`).
- **c:** The amount of time in seconds before MFA Exemption expires. This value may be obtained using the MEEM REST API, below.
 - The value 0 (zero) should be used to indicate that the exemption period has expired, and the Enrollee must set up MFA.
 - The value -1 should be used to indicate that the exemption period does not have a scheduled end.
- **r:** A % encoded URL to redirect the Enrollee to after passing through the splash page. This URL must be permitted by the *Return URL Allow List*.

If the Enrollee is still exempt (C is greater than 0), a choice will be provided to enroll now or later. If the Enrollee is no longer exempt, only an *Enroll Now* option will be presented (though of course the Enrollee could simply close the page).

The Splash Page will automatically render during the Initial Enrollment Flow (after the *Provision* step) when the following conditions are met:

1. An *MFA Exemption CO Group* is set.
2. An *MFA Enrollment Flow* is configured.
3. The *MFA Setup Reminder Splash Page* is enabled.

REST API

MEEM provides a simple REST API to obtain information about a CO Person's MFA status. Access to the API is granted to the API User set in the Initial Enrollment Flow MeemEnroller configuration. The API is accessed at the endpoint

`https://myserver/registry/meem_enroller/v1/status/<n>/<identifier>`

where

- **n:** The MeemEnroller configuration ID (ie: `cm_meem_enrollers:id`).
- **identifier:** Any valid Identifier attached to the CO Person record

On success, a 200 OK response will be generated with a JSON object holding two members:

- **mfa_status:** An array of MeemMfaStatus objects, corresponding to the contents of the `cm_meem_mfa_statuses` table
- **mfa_exempt:** A timestamp in database format (and local to the server time) indicating when the CO Person's MFA exemption is valid through, or *false* if the CO Person is not exempt

Example MEEM API Response

```
{
  "mfa_status": [
    {
      "MeemMfaStatus": {
        "id": 4,
        "meem_enroller_id": 1,
        "co_person_id": 2528,
        "idp_identifier": "https://remote-user.test.idp",
        "mfa_asserted": false,
        "created": "2020-09-16 17:39:00",
        "modified": "2020-09-16 17:39:00",
        "meem_mfa_status_id": null,
        "revision": 0,
        "deleted": false,
        "actor_identifier": "danielbmorningstar"
      }
    }
  ],
  "mfa_exempt": "2020-09-19 17:39:00"
}
```