

Create MFA policies

Description

This wizard will help you to configure multi-factor authentication in order to expand security. This process requires users to provide two or more forms of identification before being granted access to a system or application.

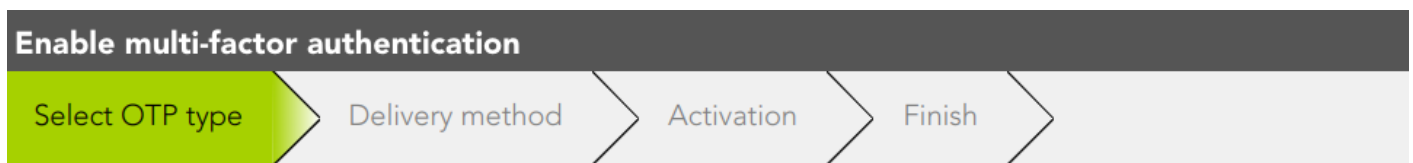
For more information, you can visit [the Two-factor authentication \(2FA\) book](#).

Step-by-step

1. If you have not previously installed the Federation Addon, the first time you select the *Create MFA policies* option, Soffid will require to **install the Federation and the OTP Addons**.

The screenshot shows the Soffid Configuration wizard interface. The breadcrumb navigation is: [Main Menu](#) > [Administration](#) > [Configuration](#) > [Global Settings](#) > Configuration wizard. The wizard is divided into four quadrants: AM (Authentication Management), IGA (Identity Governance and Administration), PAM (Privileged Access Management), and IRC (Identity Risk & Compliance). The AM quadrant is highlighted in green and contains steps: 01. Connect Soffid syncserver to your on-prem network (checked), 02. Create identities (checked), 03. Add applications, and 04. Create adaptive authentication rules. The IGA quadrant is highlighted in blue and contains steps: 01. Connect Soffid syncserver to your on-prem network (checked), 02. Create identities (checked), 03. Add applications, and 04. Sign user lifecycle flows. The PAM quadrant is highlighted in red and contains steps: 01. Create MFA policies, 02. Create monitoring and recording, and 03. Create MFA policies. The IRC quadrant is highlighted in grey and contains steps: 01. Create SoD matrix and 02. Schedule weekly risk. A warning dialog box is displayed over the AM quadrant, stating: "This option is not available. Please, install the federation and OTP addons". The dialog box has an "OK" button.

2. First, you must select the authentication factor to use



Select the strong authentication factor type to use

- Email
- SMS
- Time-based HMAC OTP
- Event-based HMAC OTP
- Security PIN
- Certificate
- FIDO Token



3. Second, you must select the delivery method to use. If you select the second option, you have to select the users to whom the instructions will be sent.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Select the desired method to provision the strong authentication factor.

- Send instructions by email to everyone
- Send instructions by email to some selected users
- Do not send it yet

Email message :

Dear \${fullName},

Please, follow this [link](#) to register your authentication email address.
It will be used by Soffid to verify your identity.

Sincerely yours, Gabriel Buades

← Undo

→ Next

4. Next, you must select which users will have the second authentication factor activated.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Select which users will be required to use its second authentication factor

- Everyone
- Only users that have completed the enrollment process.
- No one yet

← Undo

→ Next

5. Finally, the changes will be applied and the process will be finished.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Applying changes

 Finish

Revision #5

Created 22 February 2023 13:59:48

Updated 12 February 2025 12:05:16