

Multi factors authentication

Contents

- What is a Multi factors authentication?
- Existing 2nd factors on Trustelem
- Possible authentications depending on the protocols
- Setup
- Create an access-rules for MFA

What is a Multi factors authentication?

There are 3 kinds of authentication factors:

- Something you know --> password, pin...
- Something you possess --> smartphone, security key, certificate...
- Something you are --> fingerprint, face, eye iris, voice...

A Multi factors authentication is the combination of 2 factors. *Example: login + password + email one time password = MFA*

BUT a strong authentication is the combination of 2 different kinds of factors.

The previous example is not a strong authentication

Example: login + password + mobile phone application one time password = strong authentication

Existing 2nd factors on Trustelem

Trustelem factors, used in addition to the password, are:

- **SMS:** users receive a SMS with a code on their mobile phone - additional cost, not available by default
- **TOTP Authenticator:** user can use any kind of Time based One Time Password (TOTP) which is a code provide:
 - by an **application** (Google Authenticator, Microsoft Authenticator...)
 - or a **device** (usually setup with NFC).
- **WALLIX Authenticator:** the mobile (IOS/Android) and desktop application made by Trustelem; if the network is up the user receives a push notification, otherwise he can use a TOTP



- **Security key:** user has to plug a fido key. The fido key can be for example: <https://www.yubico.com/fr/works-with-yubikey/catalog/trustelem/>
- **Email:** a code is sent using an email address to be used a second factor. *This is not a strong authentication, so it is disable by default*

Notes:

- The desktop version of WALLIX Authenticator can be downloaded in the Microsoft store only.
It uses a specific Microsoft protocol for push notification named **WNS**.
It can be necessary to open some flow for this protocol in the firewall.
The needed URLs can be found here <https://learn.microsoft.com/fr-fr/windows/apps/design/shell/tiles-and-notifications/firewall-allowlist-config>
- TOTP codes are calculated using a secret and the time of the device. If the time is incorrect, the code will not work.

Possible authentications depending on the protocols

Web logging - Admin page + SAML / OpenID Connect applications

The user provides his Trustelem login + password, then the 2nd factor.
If he has multiple 2nd factors, he can choose to use another one:

WALLIX Authenticator

Waiting for device approval

Cancel



[Use a generated code from the application](#)

Alternatives

Use a security key

Ask for a rescue code (if no other method can be used)

Connect using another identity

LDAP applications

The LDAP protocol is not designed to do MFA. But with Trustelem, there are 2 ways of doing it:

- You can use push notifications with LDAP.
*The user provides his Trustelem login + password in the application, then Trustelem sends a push notification and answer to the LDAP request after the notification validation.
To make it works, be sure to set a response time / timeout long enough on your application.*
- You can use a code with LDAP (TOTP or OTP).
The user provides his Trustelem login, and in the same form the password and the code sticked together.
- You can't use security keys: the protocol can't read USB device.

Radius applications

Radius authentications have lot of possibilities:




- login + password + 2nd factor using Radius
The user provides his Trustelem login + password, then his 2nd factor
- login + password using another protocol + 2nd factor using Radius
The user provides a login + password from another source, then Trustelem 2nd factor
- login + password then no answer from Trustelem before the validation of a push notification
The user provides his Trustelem login + password then validate a push notification
- login + password and the code sticked together
The user provides his Trustelem login + password and code sticked together
- You can't use security keys: the protocol can't read USB device.

Setup

To setup the allowed factors, , go on Trustelem admin page, **Security settings** and **Authentication factors**

The first part, **Manage authentication factors**, has 2 parameters: **Login**, and **User can reset token**

Security (Trustelem Demo)

General			Password management	Authentication factors	Application certificates	Social Login	Emails	Service providers
Manage authentication factors								
 Edit								
		Login		User can reset token				
SMS		<input type="button" value="No"/>		<input type="button" value="No"/>				
TOTP Authenticator 		<input checked="" type="button" value="Yes"/>		<input checked="" type="button" value="Yes"/>				
WALLIX Authenticator		<input checked="" type="button" value="Yes"/>		<input checked="" type="button" value="Yes"/>				
Security Keys	User Verification: discouraged 	<input checked="" type="button" value="Yes"/>		<input checked="" type="button" value="Yes"/>				
User certificates		<input type="button" value="No"/>						
Email		<input type="button" value="No"/>						

Login parameter

For a chosen factor, you can activate the option **login** for all users or for specific users.
When it's done:

- Users can use the selected factor for a multi factors authentication.
- An administrator can do a manual enrollment for users.

User can reset token parameter

For a chosen factor, you can activate the option **User can reset token** for all users or for specific users.
When it's done, the defined users can use their dashboard to reset this factor:

`https://mydomain.trustelem.com/#security`

Security parameters

Password

Google Authenticator
No device registered

Security key
No device registered

+

Trustelem Authenticator

samsung SM-G950F (Android 9, v2.1.9) - Added: 2020-06-25 13:25

+

Close

When you have enabled the chosen factors, you can start the enrollment.

Manual enrollment using dashboard

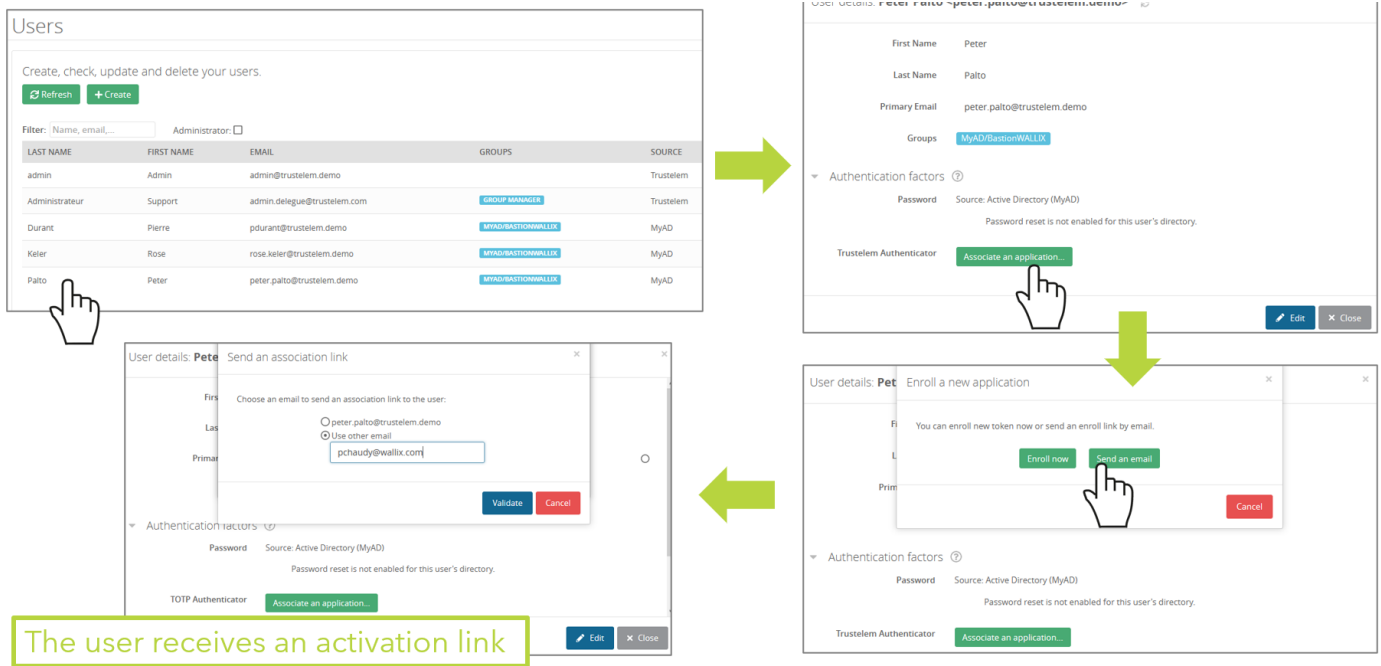
This has to be done by a Trustelem administrator

The diagram illustrates the manual enrollment process for a user in the Trustelem dashboard. It consists of the following steps:

- Users Dashboard:** A table of users is shown. The user **Peter Palto** (email: `peter.palto@trustelem.demo`) is selected.
- User Details Page:** The details for Peter Palto are shown, including his primary email and groups. Under the **Authentication factors** section, the **Trustelem Authenticator** is associated.
- Enrollment Modal:** A modal titled "Enroll a new application" is displayed. It provides instructions on how to enroll the user's mobile device.
- Enrollment Options:** The modal offers two ways to enroll:
 - Enroll now:** A button to start the enrollment process immediately.
 - Send an email:** A button to send an enrollment link via email.
- QR Code Enrollment:** A separate window shows a QR code that the user's mobile device can scan to complete the enrollment. It also provides an alternative code: `ESHWZZP-268CAD`.

Manual enrollment using email


This has to be done by a Trustelem administrator. You can send the enrollment link to Trustelem **Primary Email** or choose another one.



Enrollment campaign

- The enrollment can be using campaigns.
- Users in the selected groups will be involved in the enrollment process only if they don't already have a 2nd factor.
- If you select multiple factors, users will have a selector to enroll only one of them.
- if you enable **Automatic enroll by email** emails with the enrollment link are sent automatically. If you don't, you have buttons to do it manually.
- If you enable the **Automatic enroll during login**, every time users authenticate on Trustelem login page, they will have a window asking them to enroll a new factor. They can skip the enrollment, but the window will continue to appear after the next authentications until they do the enrollment.



 Amy Farrer
(amy.farrer@mycompany.com)

Please proceed to associate **Trustelem Authenticator** with your Trustelem account.

- Install Trustelem Authenticator on your mobile device. Once started, select 'Add an Account'
- Use your device camera to scan the following barcode:



- As an alternative, you may use the following code to register your device: 6XLVRHDH-24LC2B

Waiting for device registration

Cancel

Register later



Create an access-rules for MFA

If you already have users and applications, you can now create access-rules in order to force multi factors authentication.

You can find the detail using the URL: [access rules](#)

Revision #17

Created 1 July 2022 08:24:56 by WALLIX Admin

Updated 11 March 2025 08:15:09 by WALLIX Admin