Security built-in

Password Policies (recommended)

TS No-code Platform allows you to setup and enforce the use of strong passwords through an appropriate password policy. Specify attribute requirements that control complexity and lifetime of passwords such as:

- Minimum password length
- Special characters
- Maximum password age
- Maximum number of tries

The structural restrictions will be honored when

- The user changes his password
- A new random password is generated and sent

Passwords can also be set to expire after an amount of time.

How to: The polices can be changed in server configurations in the group *Password policies*

Note: The password polices will have no impact on SSO authentication

Multi-factor Authentication (recommended)

Device MFA

TS No-code Platform offers native Multi-factor Authentication to protect against unauthorized access by requiring a user to provide multiple authentication factors to prove their identity. At present two different options are available:

- MFA using session-specific, one-time-passcodes sent to the users mobile phone via regular or Flash SMS
  - You will need to create an account for sending SMS
  - Cost is approx. 0,30 DKK per message)
- MFA using a dedicated app from

    - Apple
    - Google
    - Microsoft

SMS requires very little of the users, while App based MFA is considered (slightly) more secure.

Note: If using singlesignon (SSO) the MFA will not be used

Location MFA

IP can be used as factor. In some cases slightly less secure, but much easier for the user.

Options include

- Country whitelisting (via IP)
- Static whitelisting of IP's
- Adaptive whitelisting of IP's

Adaptive whitelisting happens when the same user logs in from the same IP multiple times (typically 5).

IP MFA can be used together with normal MFA, so that SMS/App check is only required in case the IP is not whitelisted.

Geolocation blocking (optional)

Geoblocking will allow the servers to deny requests from certain countries.

The geoblocking will match the clients IP against a Geo service. The county will be matched to the servers whitelist of country names.

How to: Change the system configurations starting with *ipBlocker*

- Activate setting **ipBlockerActive**
- Set allowed countries in **ipBlockerAllowedCountries**

Request throttling (optional)

As specified in OWASP v4 system should be able to limit the amount of request a user can carry out in a system.

Limitations can be set on

- Pages hit

- WebDAV requests
- Upload (size/count)
- REST operations

How to: Edit server configurations starting with *limit*

Brute force prevention (optional)

This protection is handled by not serving too many requests to the login page, regardless of the source in question. This will prevent brute force attacks on distributed accounts using multiple machines. In case the detection triggers, login requests will be ignored for at set amount of time, while already logged in users can continue their work.

How to: Define systems configurations starting with *brute force*

Additional configurations

- File whitelisting (uploadWhitelist)
- OWASP compliance (owaspCompliance)

Revision #4
Created 3 April 2025 13:20:46 by Theis Villumsen
Updated 13 October 2025 13:18:10 by Max Gøtske