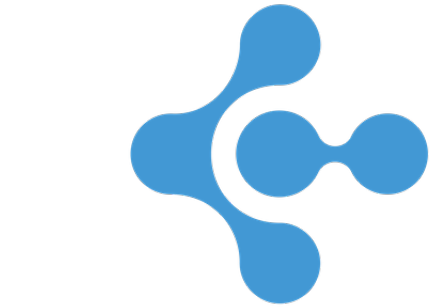

cockpit
IT Service Manager

Two-factor authentication

FAQ document

Table of contents

Introduction

I. Objective

The purpose of the document is to present the configuration and operation of strong authentication.

II. Operation

In order to increase the security level of portal access, it is possible to set up double factor authentication, based on the TOTP protocol (Time-based One-Time Passwords).

When the user activates strong authentication, a secret code is generated and encoded in BASE32 format. A 6-digit authentication code is generated from this secret code and a timestamp. This code, plus the username and password, will be requested when connecting to the portal.

III. Prerequisites

A. User

Double factor usage is available only for "Cockpit" connection mode.

B. Mobile application

To generate the 6-digit code it is necessary to use a mobile authentication application such as "Google Authenticator", "LastPass Authenticator" or "Free OTP".

Configuration

I. Enabling double factor authentication

Menu: My Parameters > Authentication

Principle: The setting of the double factor authentication is personal, so it must be done by the user, whether this is an end-user or operator, and cannot be imposed.

Operation:

To enable the "Double factor" option, a window with a QR-code and a "6-digit code" field appear.

Open the mobile authentication application ("Google Authenticator" in this example) and scan the QR-code displayed.

A line with a code updated every 30 seconds appears in "Google Authenticator".

Enter the code in the "6-digit code" field and click on "Save".

> Note: The temporary code generated by "Google Authenticator" will be required during each portal authentication, so the user will need access to their mobile phone to log in.

II. Adding a device

Menu: My parameters > Authentication

Operation: When double factor authentication is enabled, the "Add a device" button is used to obtain the identification code on another device with a mobile authentication application.

The temporary 6-digit code is required.

III. Disabling double factor authentication

Menu: My parameters > Authentication

Operation:

To disable the "Double factor" option, the temporary 6-digit code is required.

Document end