OTAC auth Install and Design Guide

V 1.2.0

swIDch Ltd.

swIDch
Address: 1st floor, 3 More London Pl, London SE1 2RE
Tel: +44 (0) 2032834081
Mail : developer@swidch.com

Contents

Release Notes

Version	Date	Notes
0	2024-01-24	Initial Release
1.0	2024-01-26	Added support for EPC 1522 Bug fixes and stability improvements.
1.1	2024-03-22	Refreshed UI for the Admin Portal. Bug fixes and stability improvements.
1.2	2024-03-27	Simplified the menu layout in the Admin Portal. Added support for AXC F 3152 (Due to the memory limitation, an SD card is required to install OTAC auth).

Introduction

This document is intended for administrators who will be using the OTAC auth app available on the PLCNext Store and the mobile app on Google Play store and Apple Apple store. This mobile app works together with the backend OTAC service that typically protects web applications such as a PLC application. The mobile app generates a One Time Authentication Code (OTAC) which is the world's first one-way dynamic authentication technology that enables users to authenticate to PLC devices via their phone.

- **App Details**: Experience rapid and secure user/device authentication through OTAC's 8-character code.
- **Quick and Easy, No Registration**: Streamlined authentication without the hassle of sign-up or login processes. Your privacy is paramount; no personal information required.
- **Secure Authentication with OTAC Code**: Ensure robust security with time-sensitive OTAC codes. Safely access your accounts using a code that expires after a specific duration.
- **Manage Multiple Accounts Easily**: Effortlessly authenticate multiple accounts using a single OTAC auth app. Register and manage up to 20 accounts securely.

Download the App

PLCNext Store
You can download the OTAC auth app from the PLCNext Store:

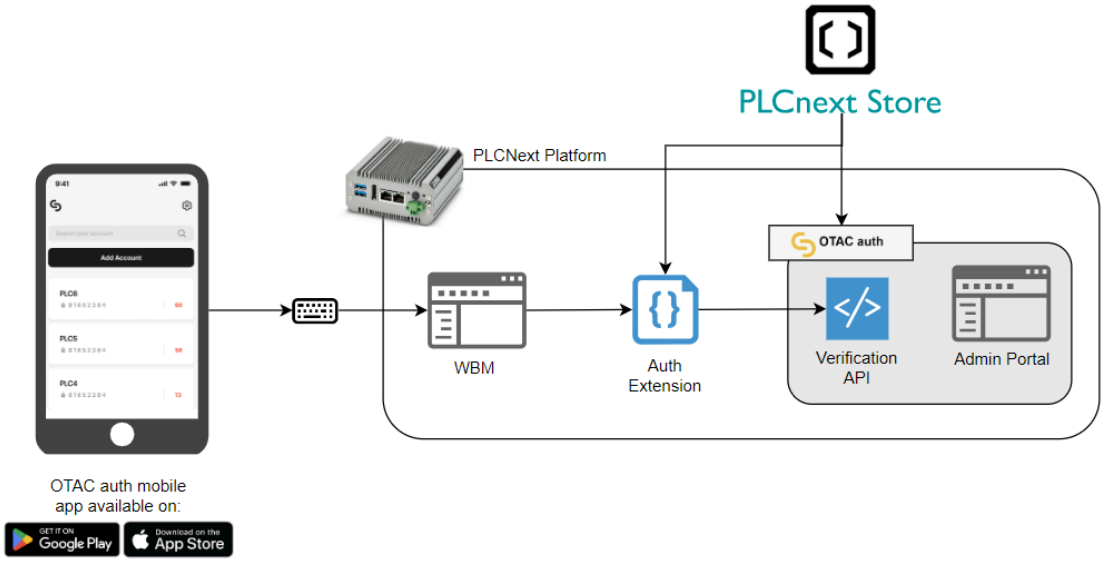
OTAC auth - MFA for PLCnext

Mobile App
You can download the OTAC auth app from the respective Google and Apple app stores:

Design

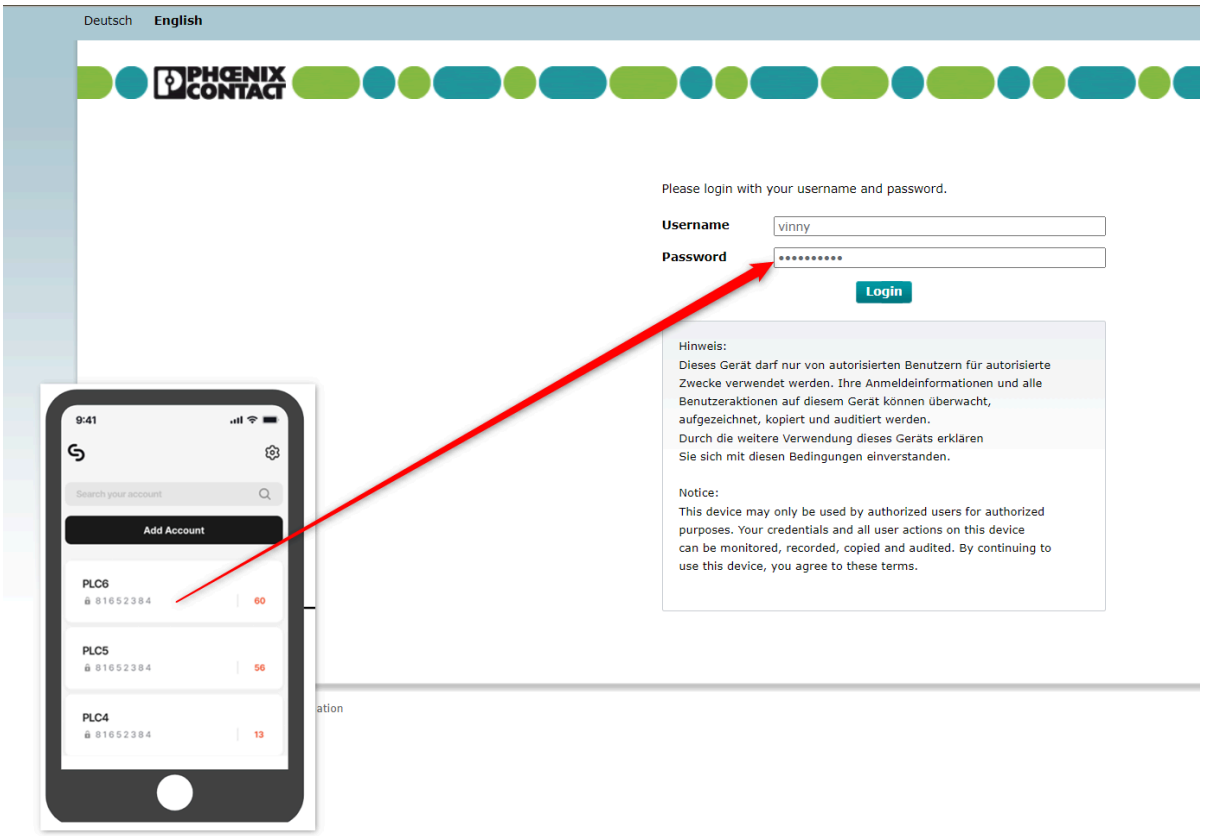
The purpose of the app is to secure the PLC web login with single step Multi Factor Authentication. Once a PLC is protected with our solution, users can authenticate to PLC utilizing our dynamic 'one-time authentication code' (OTAC) technology. The code is generated on our mobile app (available on Google Play and Apple App store), is valid for a short period of time and even works offline. OTAC combined with device biometrics and/or PIN provides a highly optimized and secure authentication solution specifically for ICS/OT security challenges.

The diagram below illustrates the design of the solution and the various components involved.



- **Mobile App**: This is responsible for generating the OTAC running on android or iOS.
- **Admin Portal**: This is a web server that runs the management portal and is also used for the registration.
- **Verification API**: This is the back end service responsible for verification and securely storing the user secrets.
- **Auth Extension**: This is a library that redirects the user's username and password from PLC's WBM the verification service.

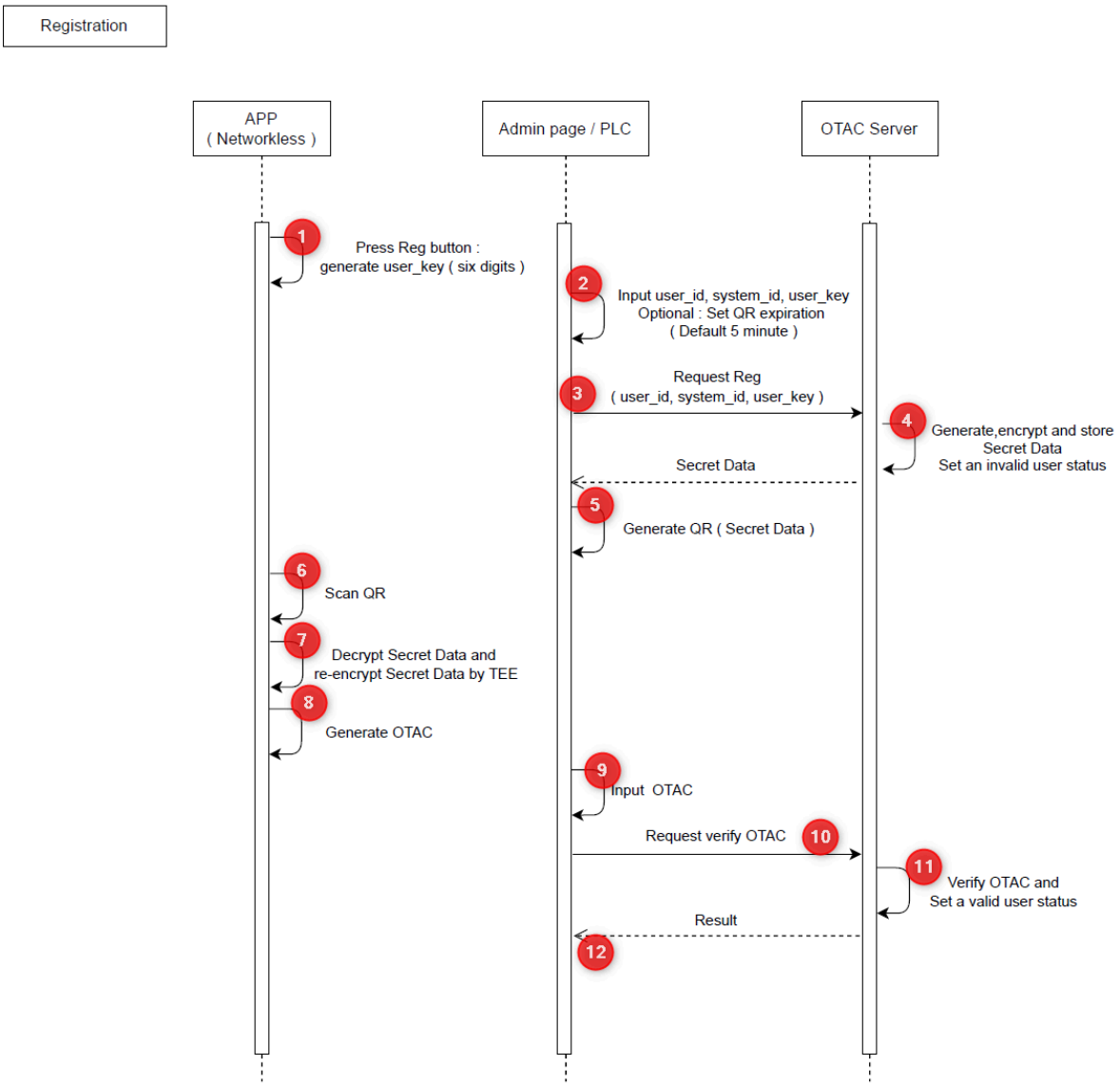
User Login Experience



Once the PLC is protected by OTAC auth, the user will not have to remember any passwords. They simply use the mobile app that generates one time-use OTAC valid for a few seconds as their password.

User Registration

The standard registration process happens in combination with the end user and admin user, the detailed steps are described below the diagram.

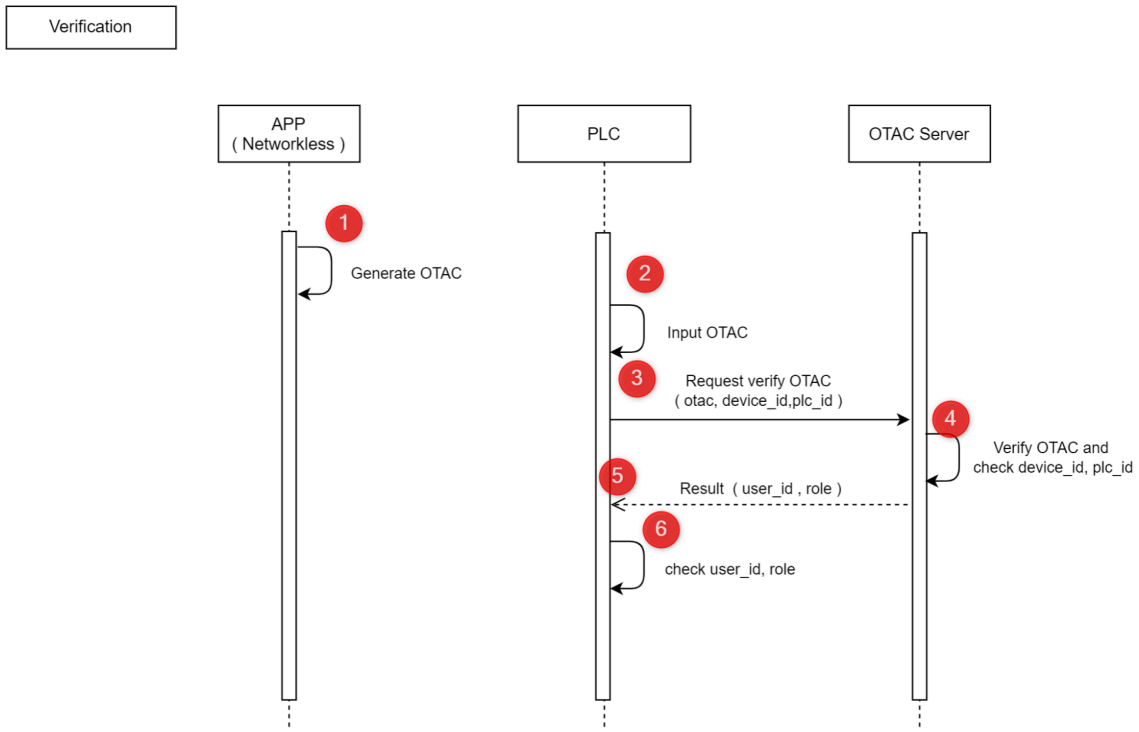


1. The first time the user opens the mobile app, they are guided through a registration process. The app first generates a random 6 digit user_key. This key is used later to encrypt and decrypt (in step 4 & 7) the secret data during transit.
2. On the Admin Portal and administrator starts the onboarding process by creating a user object and providing the following details:
    - user_id (username)
    - system_id (this is ID of the PLC device they are allowed to login in to, this parameter is optional)

    - the user_key generated on the users mobile device
3. The user_id, system_is and user_key are sent to the OTAC Server
4. The OTAC server generates a secret key for the user and encrypts it with the user_key. At this point the user status is set to invalid
5. The encrypted secret data is shown as a QR code on the admin portal.
6. The user on their mobile app can now either scan the QR code via the camera or input the secret data manually via the keyboard.
7. The secret data is decrypted using the user_key and the user secret is extracted. The user secret is then re-encrypted with a new private key and the private key is stored securely on the devices TEE (Trusted Execution Environment)
8. This finishes the pairing process, but to finish the registration process the user is asked to generate an OTAC code.
9. The administrator on the admin portal inputs the first time generated OTAC code from the user mobile.
10. The OTAC is passed to the OTAC server
11. The server verifies the OTAC and sets the user status to valid and
12. returns a successful message back.

User Authentication

While logging into the PLC, the user is prompted for a username and password. In the password field the user has to input the OTAC generated on their mobile phone. The detailed steps are described below the diagram.



1. The user opens the OTAC auth mobile app on the phone.
2. The user inputs their username and the OTAC from the mobile phone as the password.
3. The PLC passed the username, OTAC, PLC id and the device id to the OTAC Server.
4. The OTAC Server verifies the OTAC, PLC id and the device id and…
5. …returns the result along with the user id and users roles back to PLC
6. The PLC checks the result along with the user id and the roles to allow user access.

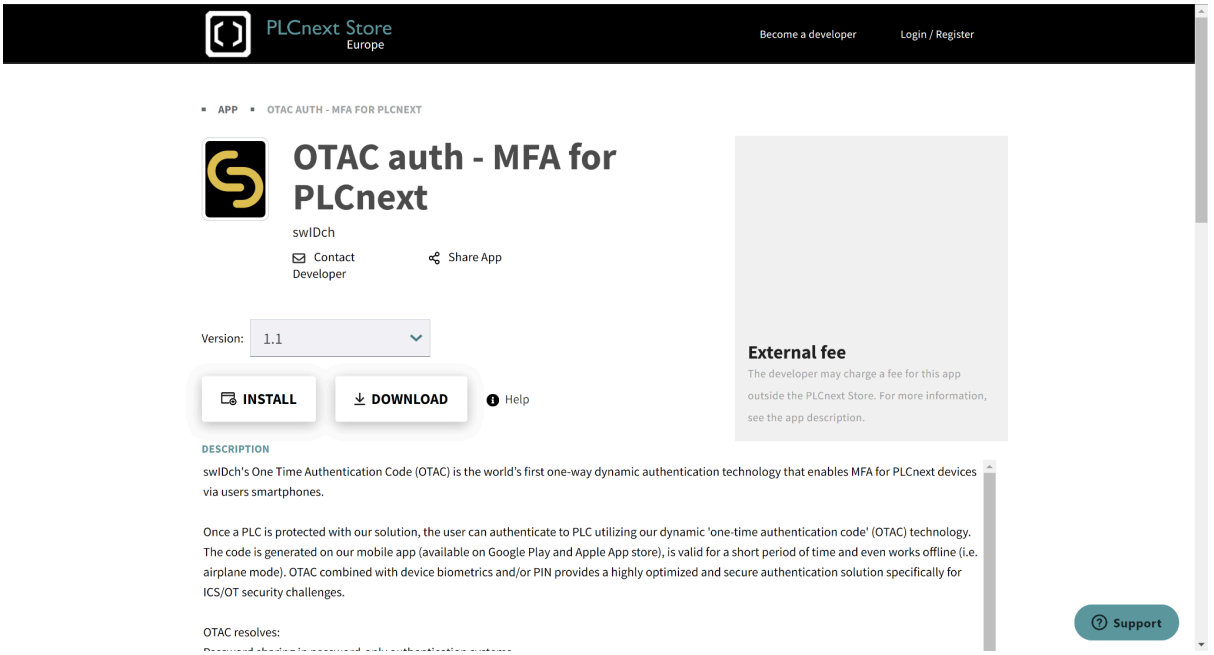
Prerequisites

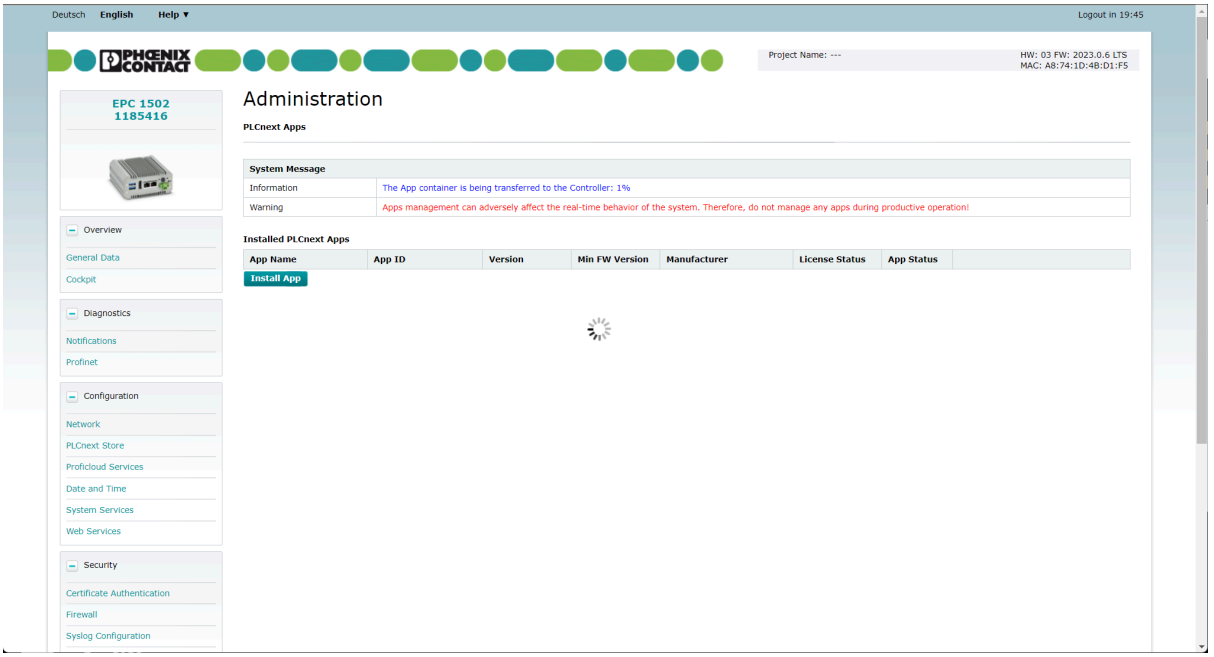
Before you can install the app from the PLCNext store you need to make sure:

- The firmware version is 2023.0.6 or above
- The date time and are set correctly on the PLC
- You have a license file available from swIDch.
- For a user to login, you need to make sure the same user does not exist in the PLC's WBM user management. The Auth Extension first checks if the user exists in the local WBM's repository and only if it cannot find the user, the authentication is redirected to OTAC auth service.

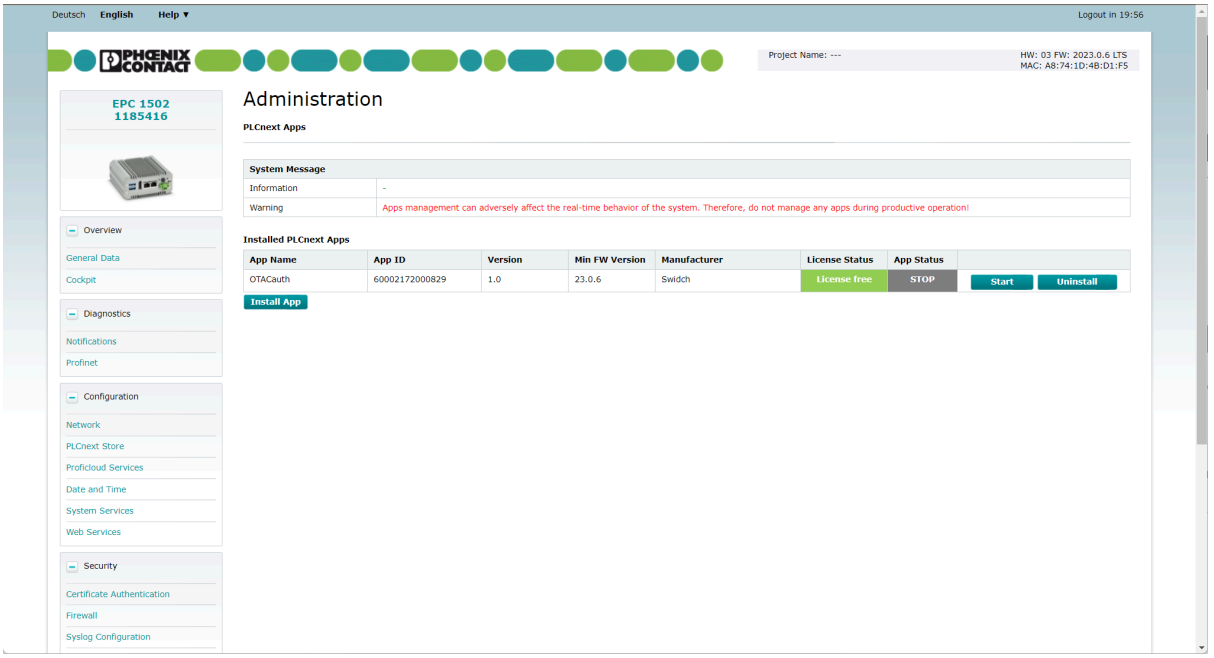
Obtaining a license file: Please contact license@swidch.com to obtain a license file. You will need to provide us the hostid of the PLC which can be found on the Admin Portal under OTAC Management > License Management

Installation

- Goto the PLCNext store and search for [OTAC auth - MFA for PLCnext](#).
- 

- Click on Download to download the app file.
- Logon to WBM of the PLC
- 

- Navigate to Administration > PLCnext Apps and click on install app. Browse for the app file you downloaded from the store.
- The app will take a few minutes to transfer, after which click on start

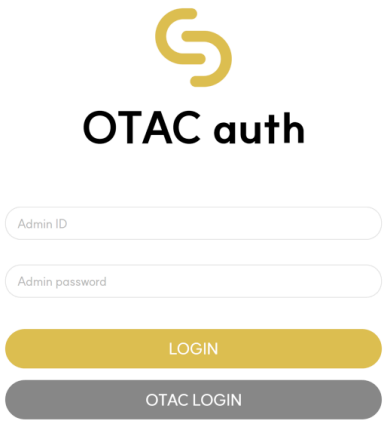


- Once the app is installed, the PLC will reboot.

Logging into the Admin Portal

Once the PLC has rebooted, you should be able to access the OTAC auth Admin Portal

---

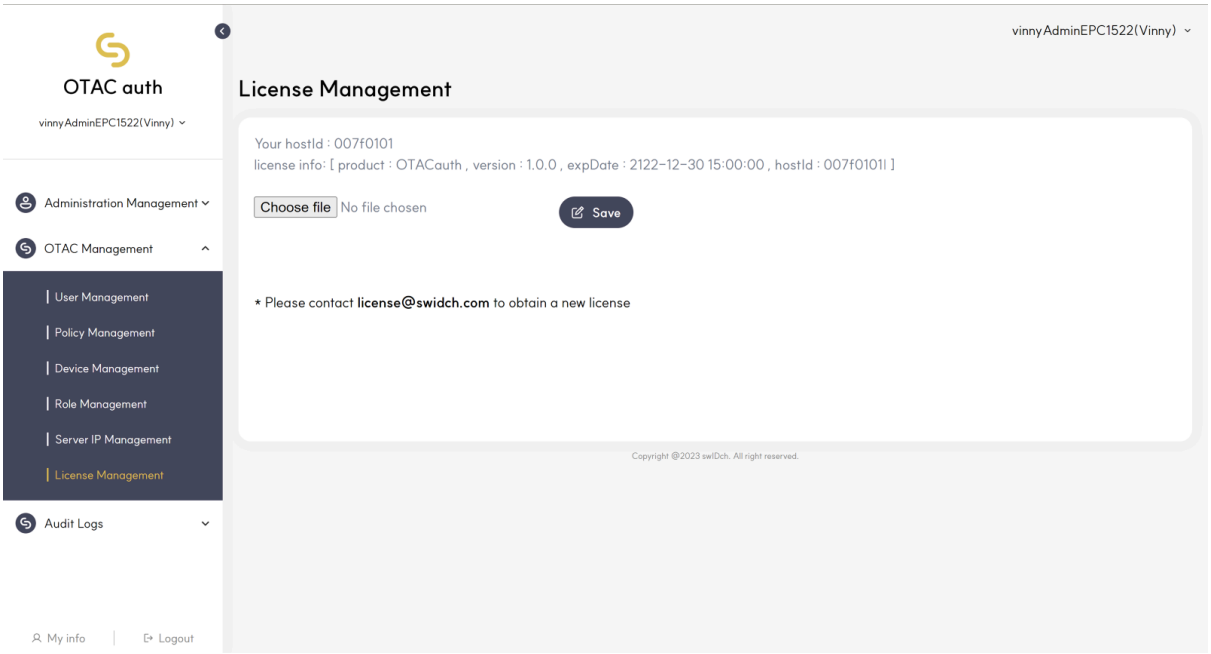


To log on as administrator on the default IP address goto http://192.168.1.10:8443/otacadm and follow these steps :

1. Admin ID “otac_admin”
2. The password is “@TACaUth!12”
3. 'Login'. Press the button.
4. You will be prompted to change the password.
5. Please set a new password

Applying the License

Once you have logged into the Admin Portal navigate to System Management > License Management



Please contact license@swidch.com to obtain a license file. You will need to provide us the hostid of PLC visible on this page above. Once you have received and applied the license, please reboot the PLC.

Please Note: Once the PLC has been rebooted, it may take up to 2 minutes for the OTAC service to start. The license is a one-time fee per PLC device, starting at £95 per PLC. License is valid for the lifetime of the device, regardless of number of registered users or number of authentication requests. License is non-transferrable.
Maintenance is available at 20% per annum - covers software upgrades, patches and technical support.