OTAC auth Install and Design Guide



V 1.2.0

swIDch Ltd.

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

Contents



Release Notes	3
Introduction	3
Download the App	3
Design	5
User Login Experience	6
User Registration	7
User Authentication	9
Prerequisites	10
Installation	11
Logging into the Admin Portal	13
Applying the License	14



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:



Mobile App

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



SWIDCH LIMITED Registered in England and Wales with Company Number 11711049

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)

Registered in England and Wales with Company Number 11711049

- 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 <u>license@swidch.com</u> 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.

<complex-block></complex-block>			Europe					
<complex-block></complex-block>		APP = OTAC AUTH - MFA	FOR PLCNEXT					
<complex-block></complex-block>			AC auth - M	FA for				
<complex-block></complex-block>								
<complex-block></complex-block>			.next					
<complex-block></complex-block>		swIDch						
<complex-block></complex-block>		🖂 Contac	t 📽 Share App					
<complex-block></complex-block>		Developer						
winiming Image: Statuling Image:								
<complex-block></complex-block>		Version: 1.1	~		Exter	nal fee		
Control Con					The deve	loper may charge	a fee for this app	
Control of the probability of the work of the two of the first one-work of quantic authentication technology that enables MM for PL Cneed devines in a second segmentated on our mobile apply of page stere is, shall for a short period PL Cneed MM of the circle home in the circl				alo	outside t	he PLCnext Store.	For more information,	
PICTURE Picture				- (p.	see the a	pp description.		
bit is in the activation code (QTAC) is the world's first one way dynamic authentication technology that enables MFA for PLC enter diversion is autoes remained on the molecular to PLC utilizing our dynamic to ne-time authentication code' (QTAC) technology to autoes		DESCRIPTION						
With series smartphones. Once as PLC is protected with our solution, the user can authenticate to PLC utilizing our dynamic 'one time authentication code' (OTAC) technology, is signerated on our mobile app (asailable on Google PLA) and Apple App story, is valid for a short period of time and even works offline (Le. a) apple amought divele biometrics and/or PHJ provides a highly optimized and secure authentication solution specifically for Comparison on the AppLe App story, is valid for a short period of time and even works offline (Le. a) apple amought divele biometrics and/or PHJ provides a highly optimized and secure authentication solution specifically for Comparison on the AppLe App story, is valid for a short period of time and even works offline (Le. a) apple amought divele biometrics and/or PHJ provides a highly optimized and secure authentication solution specifically for Comparison on the AppLe App story, is valid for a short period of time and even works offline (Le. a) apple amought divele biometrics and/or PHJ provides a highly optimized and secure authentication solution specifically for Short apple amought divele biometrics and/or PHJ provides a highly optimized and secure authentication solution specifically for Comparison on the AppLe App story is valid for a short period of time and even works offline (Le. a) apple amought divele biometrics and or PHJ provides a highly optimized and secure authentication solution specifically for Comparison on the AppLe App story is valid for a short period for the store of the store apple		swIDch's One Time Authenti	cation Code (OTAC) is the world'	's first one-way dynamic auth	nentication technology tl	nat enables MFA f	or PLCnext devices	
Image: Control of the control of t		via users smartphones.			0,1			
Consistent of the spectrate of the sp								
Addition of the second state of the s		Once a PLC is protected with The code is generated on our	our solution, the user can authors on Coord	enticate to PLC utilizing our o	iynamic 'one-time authe	ntication code' (C) IAC) technology.	
Con Download to download the app file. Con Download to download the app file. Con Download to download the app file. Con to WBM of the PLC Con to the transfer of the second the secon		airplane mode). OTAC combi	ined with device biometrics and	/or PIN provides a highly opt	imized and secure authe	ntication solution	n specifically for	
		ICS/OT security challenges.						
Image: services Constructions <								
a on Download to download the app file. The Werk area and a set of the PLC Contract of the		0710						(?)
Project Name: Net of Name: Net of Service	on Dowr	otac resolves:	lload the app	file.				
PC 1502 185416 PCmattan Construct PCmattan PCmattan Construct Page management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Page management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Page management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Page management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Page management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Pape management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation: Construct Pape Mane App 1D Version Manufacturer License Status App Status Configuration Reformance Pape Mane Pape Manegement can adversely affect the real-time behavior of the system. Pape Management can adversely affect the real-time behavior of the system. Pape Management can adversely affect the real-time behavior of the system. Configuration Reformance Pape Manegement can adversely a	on Dowr n to WBN rtsch English Help	other resolves: hload to down A of the PLC	load the app	file.				Logout i
PPC 1502 1185416 Construction Overview Overview Control Data Codopt Product Apps Daspottics Notifications Product Product Services System Services Networks Reformance Product Services Product Services System Services Networks Reformance System Services System Services Networks Reformance System Services Sy	on Dowr n to WBN usch English Help	otac resolves: hload to down A of the PLC	load the app	file.	Proje	tt Name:	_	Logout I HW: 03 FW: 2023.0.6
Configuration Records Agre Records	ON DOWR N tO WBN JISCH ENGLISH HELP CONSERVATION	other resolves: nload to down A of the PLC	load the app	file.	Proje	tt Name:	_	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10-48:D
System Message Information The App container is being transferred to the Controller: 1% Verview App management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation. Concel Data That Data One Palpontics App Name App 10 Version Manufacturer Uccess Status App Status Pagapontics Thotal Data The App Container is being transferred to the Controller: 1% The App Name App 10 Version Manufacturer Uccess Status App Status On Dagnotics The App Name App 10 Version Manufacturer Uccess Status App Status Configuration Reference App Status For Status App Status App Status For Status App Status Particular Services Particular Services Particular Services For Status	on Dowr n to WBN atsch English Help CECHSON EPC 1502 EPC 1502	otter resolves: hload to down A of the PLC C C C C C C C C C C C C C C C C C C	load the app	file.	Proje	t Name:	_	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Information The App container is being transferred to the Controller: 1% • Overview App amagement can adversely affet the real-time behavior of the system. Therefore, do not manage any apps during productive operation: • Overview Intel de D. Context Apps • Overview App Name App D Version Manufacturer License Status App Status • Dagnostics Notifications Pointer Notifications Notifications Notifications • Configuration Network Notifications Notifications Notifications Notifications • Configuration Network Notifications Notifications Notifications Notifications • Configuration Network Notifications Notifications Notifications Notifications • Condextories Notifications Notifications Notifications Notifications • Condextories Notifications Notifications Notifications Notifications • Robust Services Date and Time Notifications Notifications Notifications • Statist Services Date and Time Notifications Notifications Notifications • Statist Services Notifications Notifications Notifications Notifications • Statist Service	on Down n to WBN disch English Help CECCENT	otter resolves: hload to down A of the PLC C Administrat PLCnext Apps	load the app	file.	Proje	t Name:		Logout I HW: 03 FW: 203.0.6 MAC: A8:74:10:48:D
• Waning Apps management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation. • Overview	on Dowr n to WBN toch English Help CECCESSI 1185416	otter resolves: hload to down A of the PLC Cost Apps System Message	load the app	file.	Proje	it Name;	_	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Instalced PCCreat Apps Instalced PCCreat Apps Second Data App Name App Da Version Manufacturer License Status App Status Cockyot Install Apps Second Status Second Status <td>on Dowr n to WBN tsch English Help CEC 1502 1185416</td> <td>otter resolves: hload to down A of the PLC Administrat PLCnext Apps System Message Information</td> <td>lload the app tion</td> <td>file.</td> <td>Proje</td> <td>it Name;</td> <td></td> <td>Logout / HW: 03 FW: 2023.0.6 MAC: A8:74:10:46:D</td>	on Dowr n to WBN tsch English Help CEC 1502 1185416	otter resolves: hload to down A of the PLC Administrat PLCnext Apps System Message Information	lload the app tion	file.	Proje	it Name;		Logout / HW: 03 FW: 2023.0.6 MAC: A8:74:10:46:D
App Name App D0 Version Manufacturer License Status App Status CodoR Install App Install App Install App Install App Install App Install App o Dagnostics Notifications Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App o Configuration Install App Install App Install App Install App Install App </td <td>on Dowr n to WBN etch English Netr CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC</td> <td>otter resolves: hload to down A of the PLC * * Administrat PLCnext Apps System Message Information Warning</td> <td>lload the app</td> <td>file.</td> <td>Proje</td> <td>tt Name; nage any apps during</td> <td>productive operation1</td> <td>Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D</td>	on Dowr n to WBN etch English Netr CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	otter resolves: hload to down A of the PLC * * Administrat PLCnext Apps System Message Information Warning	lload the app	file.	Proje	tt Name; nage any apps during	productive operation1	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Codqbt Textall App • Degnostics Notifications Profinet Configuration Network Profinet Proficious Services Date and Time System Services System Services Service Services Services Service Services Service Servic	on Down n to WBN etch English Help CECCSCC 1185416 UCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	Administrat PLCnext Apps System Message System System Syst	lload the app	file.	e system. Therefore, do not ma	tt Name: nage any apps during	productive operation!	Logout / HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Degnostics Notifications Profinet Configuration Network PCnext Store Proficdud Services Date and Time System Services Web Services	on Down n to WBN etch English Help CONCENTION EPC 1502 1185416 UCCONCENTION C	Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name	Iload the app	file.	Proje	tt Name: nsge any apps during License Status	productive operation! App Status	Logout // HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:0
Profinet Configuration Profinet Profinet Proficul Services Date and Time System Services Web Services	on Down n to WBM itsch English Netgr DECLISS2 1185416 Contention General Data Cockyt	Administrat PLCnext Apps System Message Installed PLCnext Apps Marning Installed PLCnext Apps App Name Installed PLCnext Apps	load the app tion	file.	system. Therefore, do not ma Manufacturer	it Name: nage any apps during License Status	productive operation1 App Status	Logout / HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Configuration Network PCicest Store Proficioud Services Date and Time System Services Web Services	on Down n to WBN rest English Heg DECESSA EEPC 1502 1185416 Codept Overview Codept Data	Administrat Picnest Apps System Message Information Warning Installed Picnest Apps App Name Install App	tion No.400 The App container is being transf App ID Version	file.	e system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation! App Status	Logout HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Configuration Network Proficious Services Date and Time System Services Web Services	on Down n to WBN Constant Cons	Administrat PLCnext Apps PLCnext Apps PLCnext Apps Information Warning Installed PLCnext Apps App Name Installed PLCnext Apps	tion The App container is being transf Apps ID Versio	file.	Proje	tt Name: nage any apps during License Status	productive operation!	Legout HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
Computation Network PLCheck Store Proficious Services Date and Time System Services Web Services	on Down n to WBN Carlier Carlier Carlier Correction Cor	Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name Installed PLCnext Apps	tion The App container is being transf App ID Version	file.	Proje	tt Name: nage any apps during License Status	productive operation!	Legout HW: 03 FW: 2023.0.6 MAC: A8:74:10-48:D
Network PLCnest Store Proficuld Services Date and Time System Services Vesservices	on Down n to WBN Constant Cons	Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name Trottall App	Iload the app	file.	e system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation!	Legout HW: 03 FW: 2023.0.6 MAC: A8:74:10-48:D
PLCheck Store Proficioud Services Date and Time System Services Web Services	Configuration	Administrat Pload to down A of the PLC Administrat Plcnext Apps System Message Information Warning Installed Pl.Cnext Apps App Name Installed Pl.Cnext Apps	Iload the app	file.	* system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation!	Legout HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:0
Date and Time System Services Web Services	Configuration	Administrat PLCnext Apps System Message Information Verning Tistalled PLCnext Apps App Name Install App	Iload the app	file.	system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation! App Status	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10-48:D
System Services Web Services	on Dowr n to WBN tack English Rep Cockpt Cockpt Cockpt Cockpt Cockpt Configuration Network Runeat Store	Administrat PLCnext Apps System Message System Message Sys	Iload the app	file.	* system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation! App Status	Logout I HW: 03 FW: 2023.0.6 MAC: A8:74:10:48:D
years and a second with a second s	Configuration	Administrat Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name Installed PLCnext Apps	lload the app	file.	e system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation1	Logout I HW: 03 FW: 2023.0.6 MAC: A8:774:10:48:D
	on Down n to WBN I endie Eccipion Configuration Professional Configuration Configuration Configuration Profession Pro	Administrat Piccext Apps System Message Information Warning Installed Piccext Apps App Name Installed Piccext Apps App Name Installed Piccext Apps	lload the app	file.	Proje	tt Name: nage any apps during License Status	productive operation!	Logout I HW: 03 FW: 2023.0.6 MAC: A8:774:10:48:00
	Configuration	Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name Testalled PLCnext Apps	lload the app tion	file.	Proje	tt Name: nage any apps during License Status	productive operation!	Logout I HW: 03 FW: 2023 0.6 MAC: A8:74:10-48:D
	Configuration Configu	Administrat PLCnext Apps System Message Information Warning Installed PLCnext Apps App Name Installed PLCnext Apps	Iload the app	file.	* system. Therefore, do not ma Manufacturer	tt Name: nage any apps during License Status	productive operation!	Logott HW: 03 FW: 2023.0.4 MAC: A8:74:10:48:0

Syslog C

Firewall

- 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

.

						Project Name:		MAC: A8:74:1D:4B:D1:F5
556 4 563	Δdministr	ration						
1185416	Administr	ation						
	PLCnext Apps							
and the second s	System Message							
=1== &	Information	-						
Conservation of the second sec	Warning	Apps management	can adversely affect	the real-time behavior of	the system. Therefore, do i	not manage any apps during	productive operation	ml
Overview	Installed PLCnext A	pps						
General Data	App Name	App ID	Version	Min FW Version	Manufacturer	License Status	App Status	
Cockpit	OTACauth	60002172000829	1.0	23.0.6	Swidch	License free		Start Uninstall
Notifications Profinet Configuration								
Network								
Professional Convision								
Date and Time								
System Services								
Web Services								
 Security 								
Certificate Authentication								

• 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 <u>http://192.168.1.10:8443/otacadm</u> 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

6	vinnyAdminEPC1522(Vinny) ~
OTAC auth	License Management
vinnyAdminEPC1522(Vinny) ~	Your hostild : 007f0101
Administration Management ~	Choose file No file chosen
OTAC Management ^	
User Management	* Please contact license@swidch.com to obtain a new license
Policy Management	
Device Management	
Role Management	
Server IP Management	
License Management	Copyright @2023 sulDcb, All right reserved.
S Audit Logs ~	
A My info	

Please contact <u>license@swidch.com</u> 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.