Draft for:

1/4

Authentication via OTP

This feature is available for server firmware 1.1.10.22 and above, configurator version 1.3.0.24 and above, and client version 1.2.24 and above.

Instead of sharing a username and password to allow users to authenticate with the server, it is possible to generate a one-time password (OTP) and send it to the client. The code generated is valid for 2 hours, after which it will no longer work.

Generating the OTP

• Only an Admin user can generate an OTP. The code is generated directly from the client application. To define an authenticated user as Admin, go to the server's webpage under Licenses and Codes, and make sure to enabled the Admin option for the admin user.

Clients codes:				
A unique code is associated to inserted into the list of server to enabled clients.	any running client (Ipad, Touch Sc known codes and has to be enable	reen, PC). This (d. Server ensure	code m conne	ust be ction just
Maximum allowed client: 999				
Last connected client code:				
Last connected client IP: 192	.168.3.118			
	1			
Show 10 v entries	Search:			
	Desc.			Admin
Android	ID: ************************************		4.40	
EnvisionClient	ID:""		-	
Windows_10_(10.0)	ID:"CT00000.0000000000000000000000000000000		0707	
•				•
Showing 1 to 3 of 3 entries		Previous	1	Next
Insert client code				
	Add Client Code			

Figure 16: Admin Configuration

• In the configurator, click on System and enable "Use OTP Authentication".

Password	••••
VNC password	
ThinknxCloud	Enabled
Password for ThinknxCloud	•••••
Automatic server update	Enabled
Automatic authentication	Enabled
Use OTP authentication	Enabled
Automatic connection	Enabled
Cloud connection policy	Local and Cloud

Figure 17: Enable OTP Authentication

• Open the project using the Admin profile, and access the advanced settings window as seen in the picture below.



Figure 18: Project Settings

• Click on Manage Clients, and add a new user. Configure your preferences for this user and save it.





• The user created is now visible in the Users list with the OTP displayed as the user label. The admin can now share this OTP with another user to authenticate with the server.

Manage clients	
Android Enabled always, push notifications are disabled.	Î
EnvisionClient Enabled always, push notifications are enabled.	
Windows_10_(10.0) Enabled always, push notifications are enabled.	
OTP: 77244244 Code valid for: 01 h. 59 min. 48 sec.	
Ð	

Figure 20: OTP created

Using the OTP to authenticate

- Any user wanting to authenticate with the server should ask the Admin for the OTP.
- Download the project on the user's device using one of the methods explained above.
- Open the project downloaded. A popup shows up, asking the user to authenticate. A toggle button on the extreme right of the popup gives the option to authenticate using username and password, or OTP. Select the OTP view mode, and enter the OTP generated by the Admin.

Client's authentication required Type OTP to authenticate the device in the ThinKnx server.	
OTP	
Authenticate Settings	
Client's authentication required Type username and password to authenticate the device in the ThinKnx server.	Toggle View
Username	
Decement	
Password	
Authenticate Settings]

Figure 21: OTP Authentication

