



LIVEVOX

Password Management Functionality

Support Contacts:

24 Hour Support Line: 888.477.3448

Support Email: support@livevox.com

This document is an unpublished work protected by the United States copyright laws and is proprietary to LiveVox, Inc. ("LiveVox"). Disclosure, copying, reproduction, merger, translation, modification, enhancement, or use by anyone other than authorized employees, clients or licensees of LiveVox, and its affiliate companies, without the prior written consent of LiveVox, is prohibited. This document is intended as a guide to assist users of systems provided by LiveVox, and does not constitute the provision by LiveVox of any legal or compliance advice. Compliance by authorized clients or licensees of LiveVox with any and all applicable local, state, federal, or foreign laws and regulations is the sole responsibility of those authorized clients or licensees. Further, features and services that rely on third party performance are subject to the errors and omissions of those third parties, over which LiveVox has no control. LiveVox therefore disclaims any and all liability resulting from or arising out of any services supplied by or through any third party vendor or any acts or omissions of the applicable third party vendor. Additionally, LiveVox makes no representations or warranties with respect to the accuracy of content supplied by parties other than LiveVox.

This document last revised August 14th, 2018

For Internal and Client Use Only

Contents

Introduction.....	4
<i>Document Purpose.....</i>	<i>4</i>
Management features.....	4
<i>General Guidelines.....</i>	<i>4</i>
<i>How does it work?.....</i>	<i>6</i>
<i>Setting up Agents and Users.....</i>	<i>8</i>
<i>Resetting Expired Password.....</i>	<i>9</i>
<i>Failed Logins.....</i>	<i>11</i>
<i>Security Settings.....</i>	<i>12</i>
<i>Dual Factor Authentication.....</i>	<i>13</i>
OTP Enrolment Status.....	18
Changing passwords.....	18
Resetting locked accounts.....	18
<i>Setting up WinAuth Application for Dual Factor Authentication.....</i>	<i>19</i>

Introduction

Document Purpose

This document provides an overview of the LiveVox password management functionality. It also includes general guidelines for the client level SFTP credentials.

Management features

General Guidelines

LiveVox portal and agent portal access:

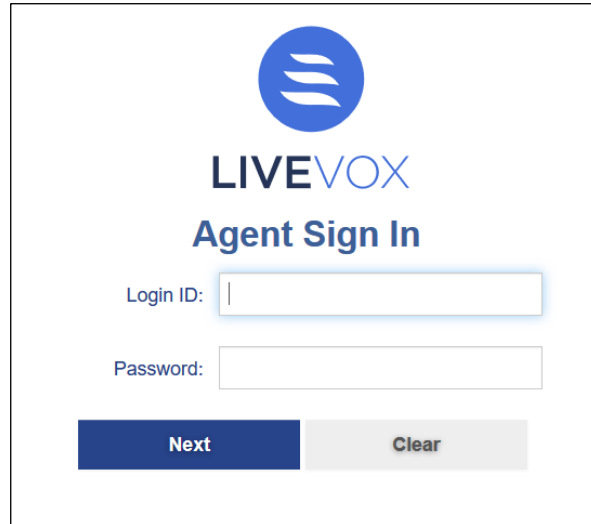
- Username and password are case sensitive. With the password management feature enabled, the following restrictions are implemented.
 - Password strength is selectable at three levels:
 - Medium: User and agent passwords must be a minimum of eight characters in length containing at least one digit, one letter, and must not match the previous four passwords for that user or agent credential.
 - Strong: User and agent passwords must be a minimum of eight characters in length containing at least one digit, one letter, one special character, and must not match the previous four passwords for that user or agent credential.
 - Very Strong: User and agent passwords must be a minimum of twelve characters in length containing at least one digit, one letter, one special character, and must not match the previous four passwords for that user or agent credential.
 - Special characters supported are the ASCII printable characters:
 - (space)! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~
- User and agent passwords expire after a specified period. The timeframe is configurable at the client level, is set to 90 days by default, and applied to both users and agents. Password management will lock out users and agents after a number of failed login attempts. The allowed number of failed logins is configurable at the client level for users and agents. By default, both users and agents are allowed 5 failed logins. Passwords are encrypted for all users, meaning that passwords are not stored in clear text anywhere in the system including the database. This is configurable at the client level.
 - LiveVox uses AES-256 encryption.

- SFTP site access:
 - Users can upload campaign files or retrieve generated reports from their LiveVox SFTP site. LiveVox uses the SFTP protocol by default. If you require FTP instead, please contact Client Services - client-services@livevox.com.
 - If utilizing the voice portal's integrated FTP Browser, a user's voice portal credentials are used (password requirements described above).
 - If utilizing a 3rd party SFTP browser application, specific SFTP credentials provided by LiveVox are used. These credentials adhere to the following standards:
 - SFTP usernames and passwords are case sensitive.
 - SFTP passwords must be a minimum of eight characters in length and contain at least 1 digit.
 - SFTP passwords do not expire.
 - SFTP encrypts commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network.

How does it work?

Login

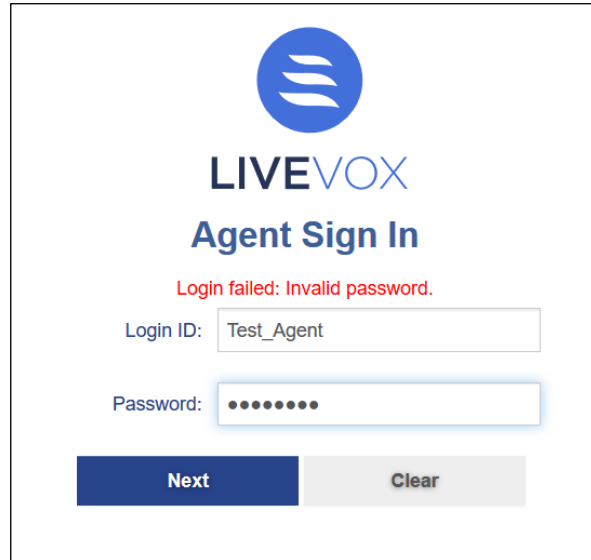
- Agent Login (via agent link provided by LiveVox).



The image shows the 'Agent Sign In' form. At the top is the LIVEVOX logo. Below it, the text 'LIVEVOX Agent Sign In' is displayed. There are two input fields: 'Login ID:' and 'Password:'. Below the input fields are two buttons: 'Next' (dark blue) and 'Clear' (light grey).

Figure 1: Agent login

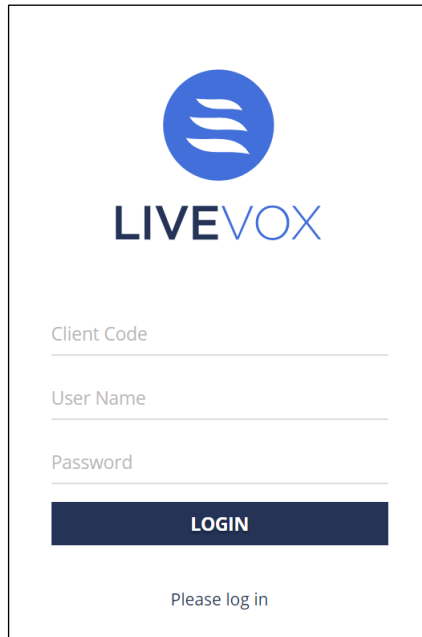
- The Agent login screen displays error message when an invalid password is entered by an agent. Click **Next** and the following screen is displayed:



The image shows the 'Agent Sign In' form after a failed login attempt. The LIVEVOX logo and 'Agent Sign In' text are at the top. A red error message 'Login failed: Invalid password.' is displayed above the input fields. The 'Login ID:' field contains the text 'Test_Agent'. The 'Password:' field is filled with dots. Below the input fields are two buttons: 'Next' (dark blue) and 'Clear' (light grey).

Figure 2: Agent login failed

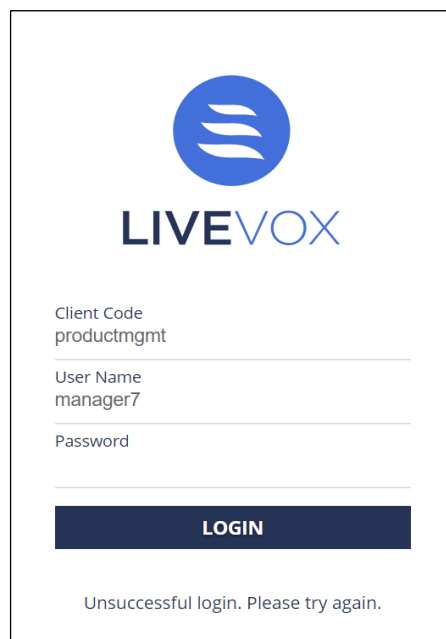
- User login (via user link provided by LiveVox).



The image shows a user login screen for LiveVox. At the top center is the LiveVox logo, which consists of a blue circle containing three white horizontal lines, with the word "LIVEVOX" in blue capital letters below it. Below the logo are three input fields: "Client Code", "User Name", and "Password". Each field has a horizontal line underneath it. Below the input fields is a dark blue rectangular button with the word "LOGIN" in white capital letters. At the bottom center of the screen, the text "Please log in" is displayed.

Figure 3: User login

- The login screen displays the following message when an invalid password is entered by the user. Click **Login** and the following screen is displayed:



The image shows the user login screen after an unsuccessful login attempt. The layout is identical to Figure 3, but the input fields now contain text: "Client Code" is "productmgmt", "User Name" is "manager7", and "Password" is empty. The "LOGIN" button is still present. At the bottom center, the message "Unsuccessful login. Please try again." is displayed.

Figure 4: Unsuccessful user login

Setting up Agents and Users

- Adding a new agent:
 - If the password is not 8 characters or greater, does not contain a mixture of characters and numbers, or matches one of the previous four passwords, the user configuring a new agent will get the following error, after clicking **Save**.

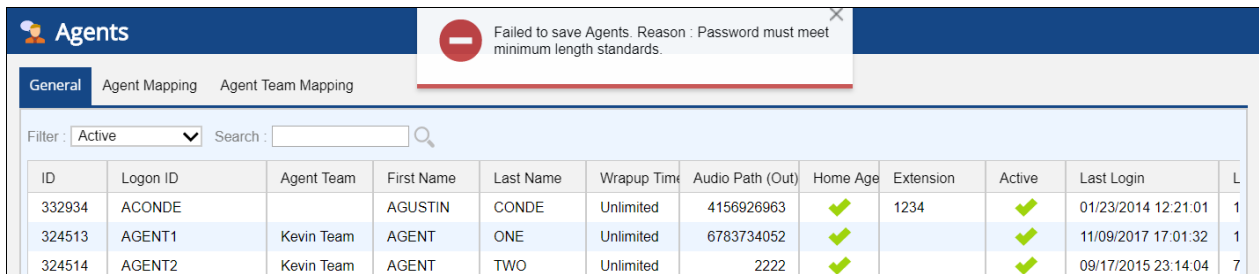


Figure 5: Failure to save agent

- If the password has no digits but characters only, the user configuring new agent will get the following error:

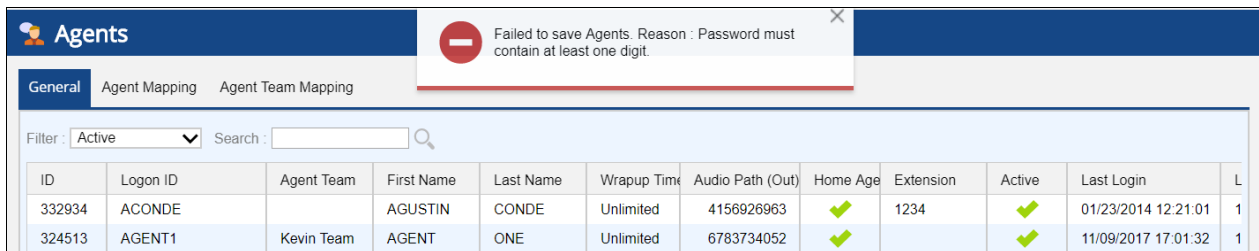


Figure 6: Failure to save agent

- If the password has no characters but digits only, the user configuring new agent will get the following error:

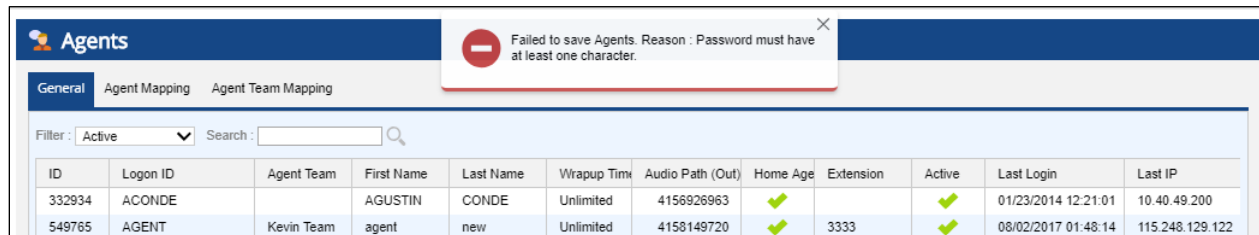


Figure 7: Failure to save agent

- Similarly, adding a new user.
 - If the password is not 8 characters or greater, or does not meet the password requirements; the user configuring new user will get the following error, after clicking **Save**.

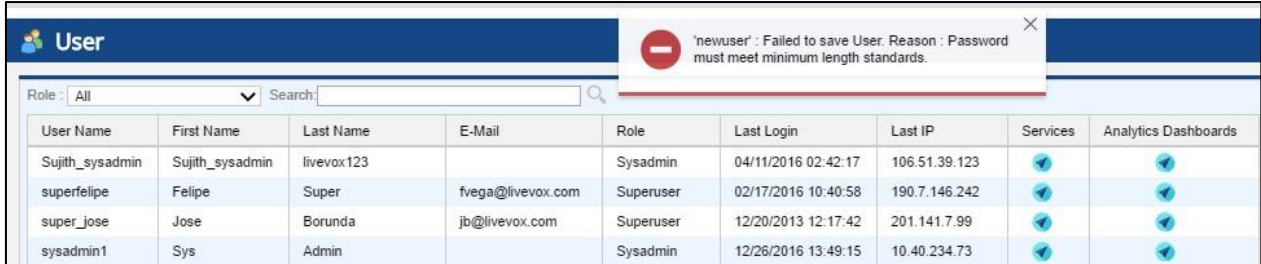


Figure 8: Failure to save new user

Resetting Expired Password

When the password expires, agents and users will get an error on their screen as they try to log in. New password cannot be the same as the last four passwords.

- Agents

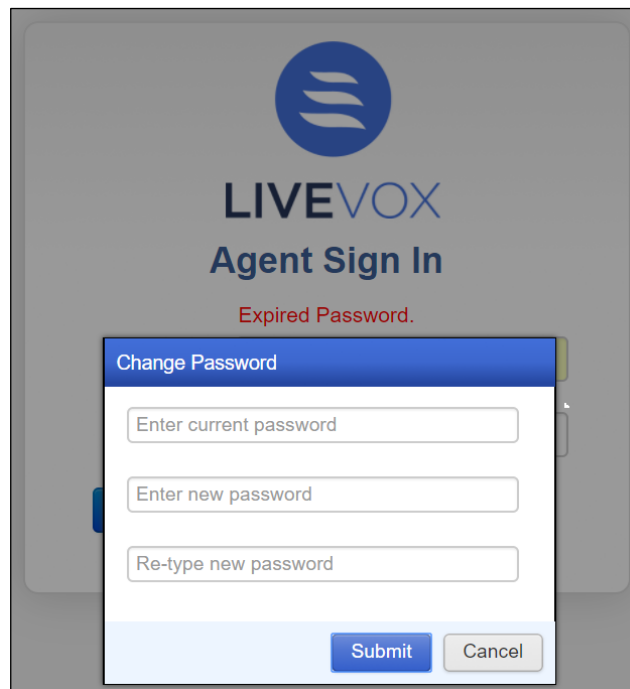
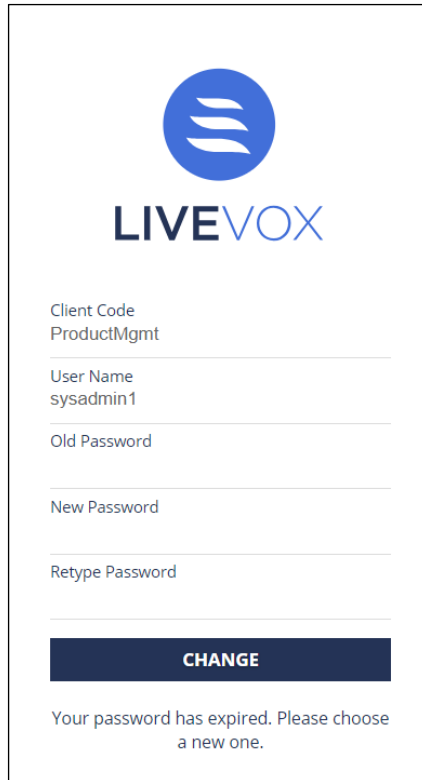



Figure 9: Agent sing in for expired password

- Users




LIVEVOX

Client Code
ProductMgmt

User Name
sysadmin1

Old Password

New Password

Retype Password

CHANGE

Your password has expired. Please choose a new one.

Figure 10: User password expired

Failed Logins

- Agents
 - If an agent attempts to log in with the wrong password more times than the site's configured limit, the agent will be locked out:

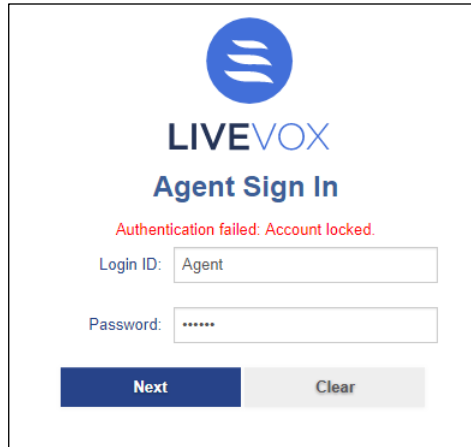


Figure 11: Agent account locked

- Users
 - If a user attempts to log in with the wrong password more times than the site's configured limit, the user will be locked out and presented with the following screen:

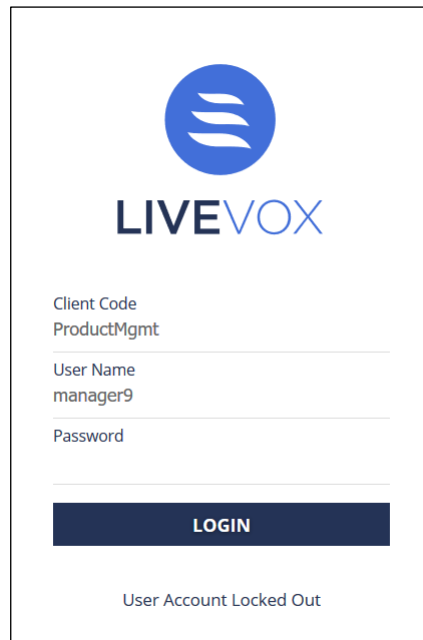


Figure 12: User account locked

Security Settings

Users in Sysadmin role can manage LVP and Agent password security settings in the **Security** tab in the Client editor.

Sysadmins have the option to configure the following for LVP users and agents:

- Password Expire Days
- Max Failed Login Attempts
- Browser Session Security
- **Password Strength.** Slide the arrow on the bar to select one of the following levels:
 - Medium - Password must be a minimum of eight characters in length containing at least one digit, one letter, and must not match the previous four passwords.
 - Strong - Password must be a minimum of eight characters in length containing at least one digit, one letter, one special character, and must not match the previous four passwords.
 - Very Strong - Password must be a minimum of 12 characters in length containing at least one digit, one letter, one special character, and must not match the previous four passwords.

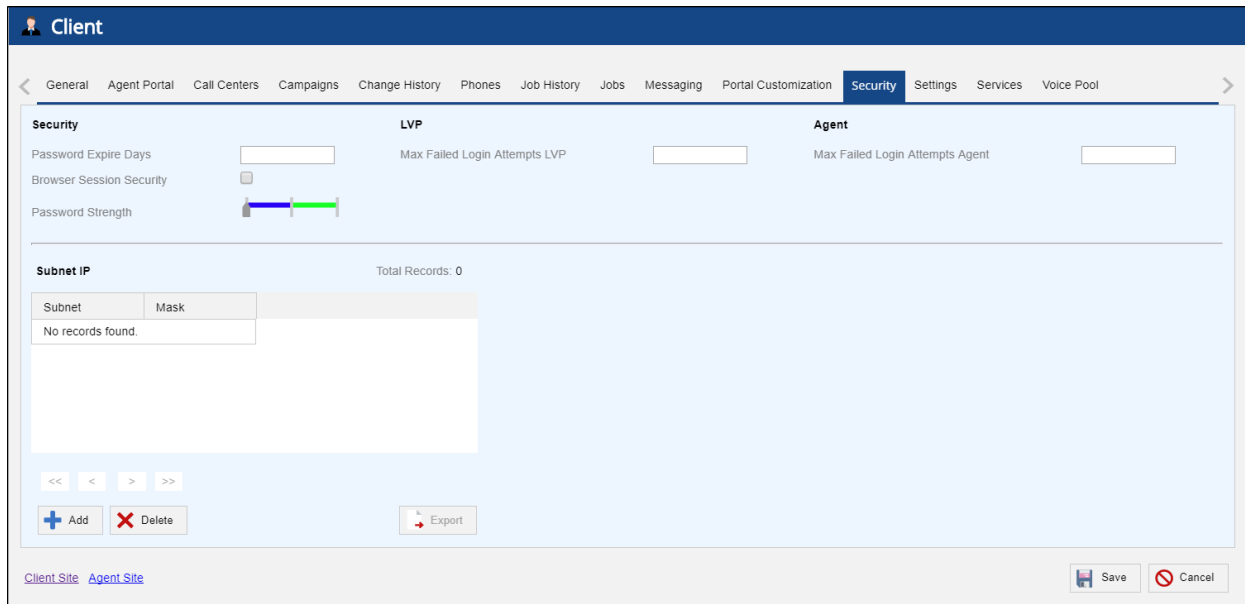


Figure 13: Client editor security tab

Dual Factor Authentication

Dual Factor Authentication (DFA) is a type of Multi Factor Authentication, where essentially second level of authentication by user is required for a successful login, and this second password is an OTP (One Time Password).

An Admin can enrol a user for dual factor authentication. To enrol the user for DFA, navigate to *Configure > System > Double click the user > General Tab*:

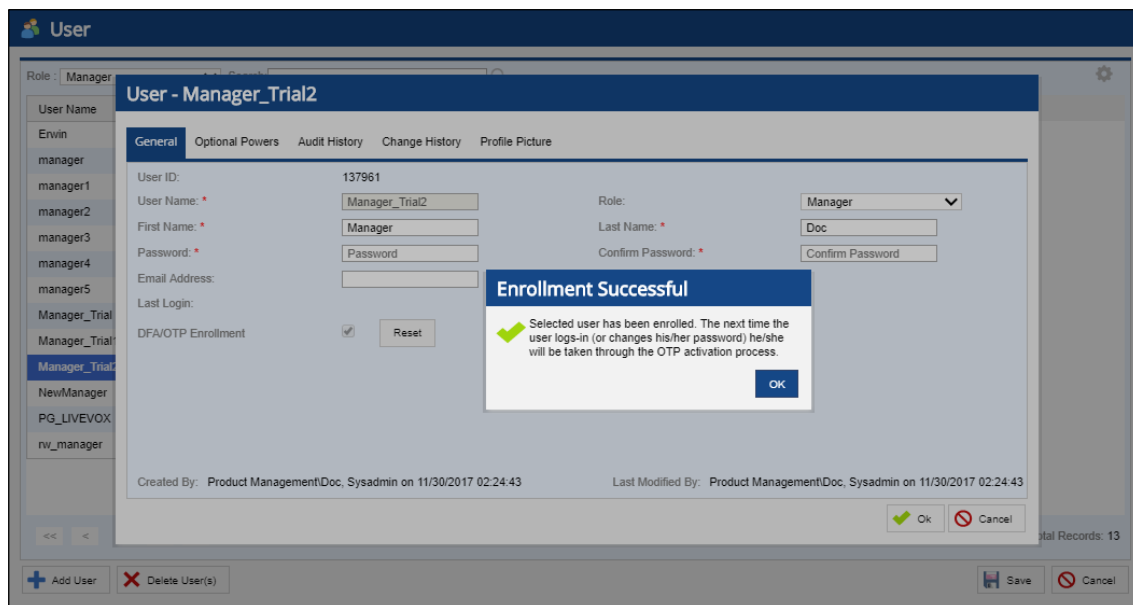


Figure 14: DFA Enrollment for User

Once the enrollment option is enabled by Admin, the user's enrollment will be in pending activation status which is displayed in the OTP column of User editor.

User Name	First Name	Last Name	E-Mail	Role	OTP	Last Login	Last IP	Services
Erwin	Erwin	Test		Manager	⊖	06/01/2017 20:23:56	206.15.76.98	✔
manager	Manager	User		Manager	⊖	09/18/2015 11:23:51	71.237.19.151	✔
manager1	Manager	One	manager1@client.net	Manager	⊖	03/31/2016 17:54:47	189.177.99.83	✔
manager2	Manager	Two	manager2@client.net	Manager	⊖	07/13/2015 13:51:20	189.253.217.58	✔
manager3	Manager	Three		Manager	⊖	06/09/2015 17:43:40	181.142.169.107	✔
manager4	Manager	Four		Manager	⊖			✔
manager5	manager5	manager5		Manager	⊖			✔
Manager_Trial	Manager	Doc		Manager	✔	11/29/2017 00:16:03	182.75.26.194	✔
Manager_Trial1	Manager	Doc		Manager	✔			✔
Manager_Trial2	Manager	Doc		Manager	⚠			✔
NewManager	New	Manager		Manager	⊖			✔
PG_LIVEVOX	pao	gesmundo		Manager	⊖	03/24/2016 16:24:12	108.80.185.247	✔
nv_manager	Manager	RWaldheim	waldheim.ray@gmail.c	Manager	⊖	04/27/2016 11:53:37	98.88.65.145	✔

Figure 15: User Account Pending Activation

The user is required to complete this activation process upon login.

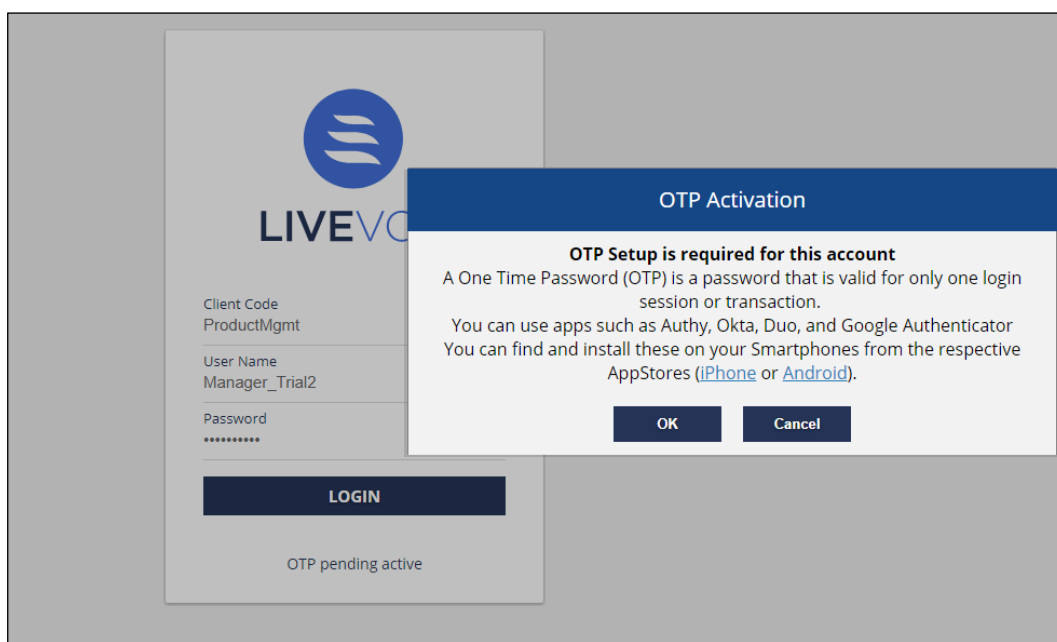


Figure 16: User login for Dual Factor Authentication

Users must authenticate their login with an OTP generated via Desktop Application (WinAuth), mobile application (Google Authenticator, OKTA etc.) or hardware token.

- User login (User's enrolled for DFA only).

- The following screen displays when the user enrolled for DFA submits the login credentials:

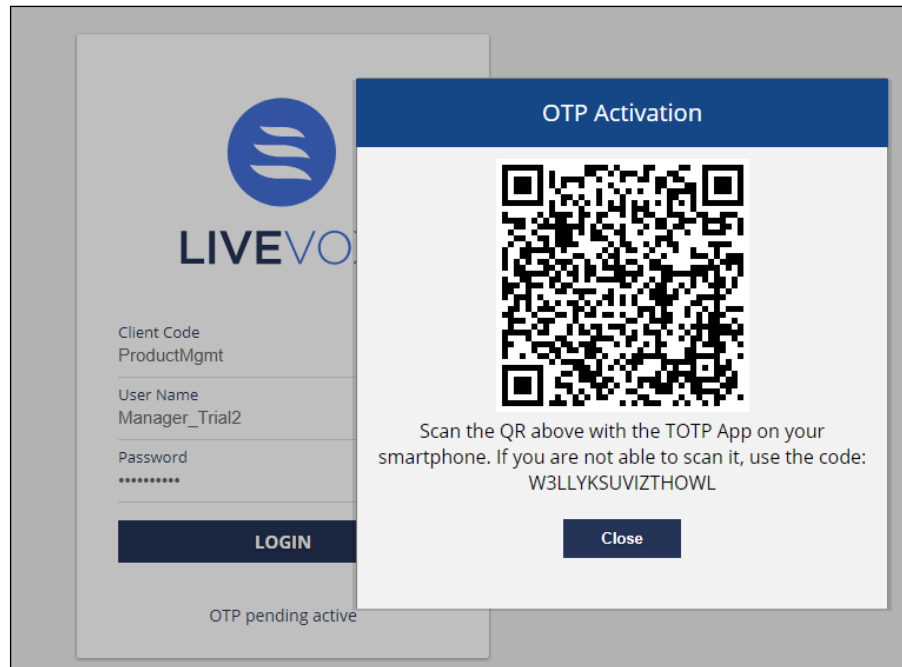


Figure 17: QR Code for OTP Activation

- Desktop Users
 - Users are required to add the QR code in WinAuth to generate the OTP. Enter the OTP obtained via WinAuth application to continue the login process. For details on the usage of WinAuth see *Setting up WinAuth Application for Dual Factor Authentication* section.

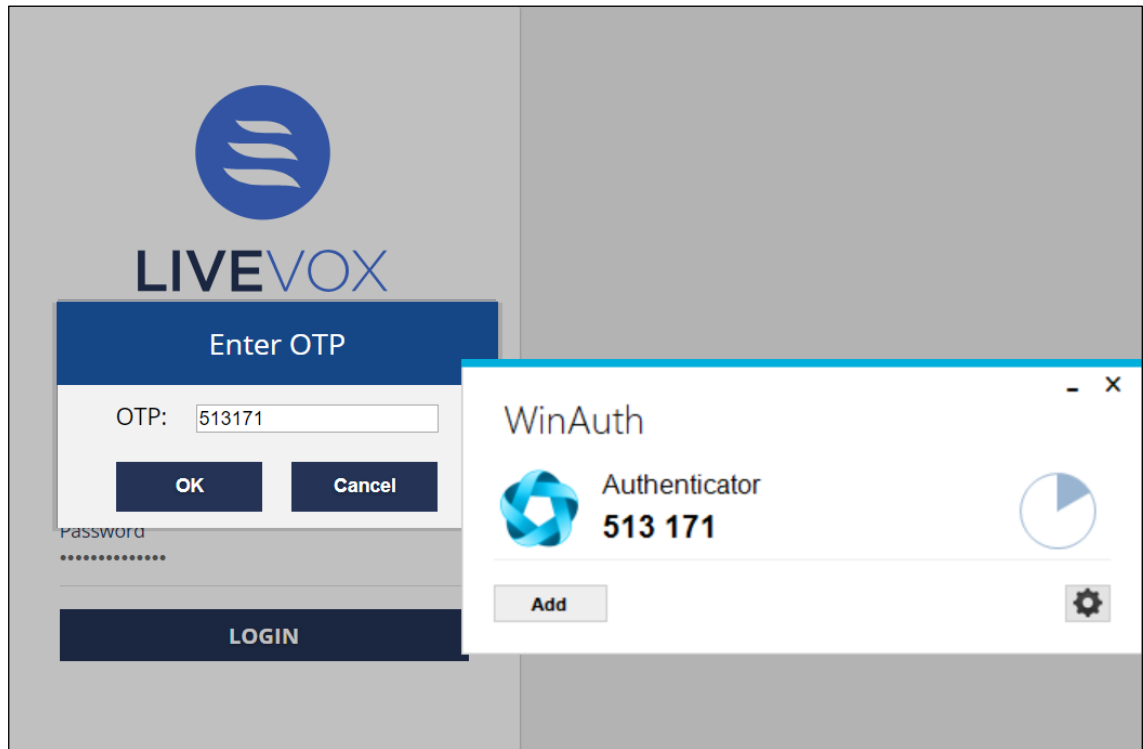
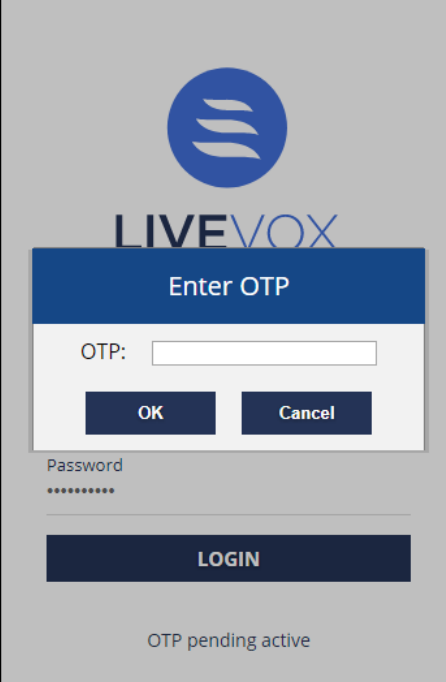


Figure 18: OTP verification via WinAuth

- Mobile Users
 - Users are required to scan the QR code to continue the login process. The user receives OTP via a mobile application (Google Authenticator, OKTA etc.) and is presented with the following screen:



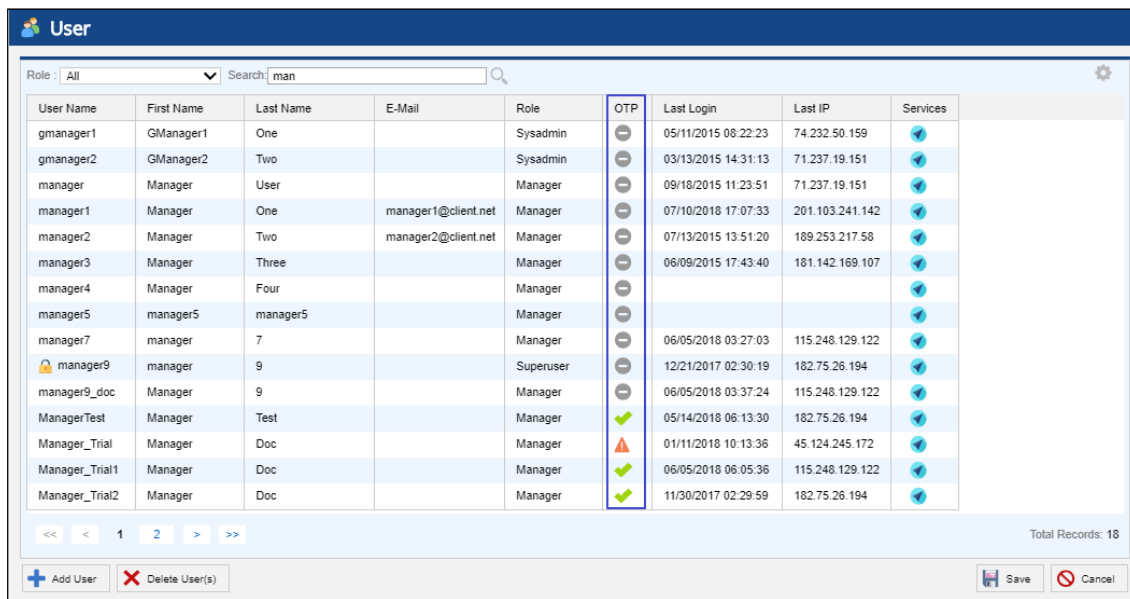
The screenshot displays the LIVEVOX login interface. At the top, the LIVEVOX logo is visible. Below it, a blue header bar contains the text "Enter OTP". Underneath this bar is a white input field labeled "OTP:" with a small white rectangle next to it. Below the input field are two dark blue buttons: "OK" and "Cancel". Below these buttons is a "Password" field with a masked password represented by seven dots. At the bottom of the form is a large dark blue button labeled "LOGIN". Below the "LOGIN" button, the text "OTP pending active" is displayed.

Figure 19: One Time Password verification

- Once the OTP is entered by the user the login process continues.
- If there are failures, they are counted against the maximum OTP failure count and eventually the account gets locked and the user needs to contact the Admin to unlock the account.

OTP Enrolment Status

The User editor's User Grid displays a column to indicate the OTP (One Time Password) Enrolment Status. Hover the mouse over the icon displayed in the OTP column to get the description of the OTP Enrolment Status.



User Name	First Name	Last Name	E-Mail	Role	OTP	Last Login	Last IP	Services
gmanager1	GManager1	One		Sysadmin	⊖	05/11/2015 08:22:23	74.232.50.159	✔
gmanager2	GManager2	Two		Sysadmin	⊖	03/13/2015 14:31:13	71.237.19.151	✔
manager	Manager	User		Manager	⊖	09/18/2015 11:23:51	71.237.19.151	✔
manager1	Manager	One	manager1@client.net	Manager	⊖	07/10/2018 17:07:33	201.103.241.142	✔
manager2	Manager	Two	manager2@client.net	Manager	⊖	07/13/2015 13:51:20	189.253.217.58	✔
manager3	Manager	Three		Manager	⊖	06/09/2015 17:43:40	181.142.169.107	✔
manager4	Manager	Four		Manager	⊖			✔
manager5	manager5	manager5		Manager	⊖			✔
manager7	manager	7		Manager	⊖	06/05/2018 03:27:03	115.248.129.122	✔
manager9	manager	9		Superuser	⊖	12/21/2017 02:30:19	182.75.26.194	✔
manager9_doc	Manager	9		Manager	⊖	06/05/2018 03:37:24	115.248.129.122	✔
ManagerTest	Manager	Test		Manager	✔	05/14/2018 06:13:30	182.75.26.194	✔
Manager_Trial	Manager	Doc		Manager	⚠	01/11/2018 10:13:36	45.124.245.172	✔
Manager_Trial1	Manager	Doc		Manager	✔	06/05/2018 06:05:36	115.248.129.122	✔
Manager_Trial2	Manager	Doc		Manager	✔	11/30/2017 02:29:59	182.75.26.194	✔

Figure 20: User editor - enrolment status

Changing passwords

The users enrolled for Dual Factor Authentication require a valid OTP token to change the password. The login process continues upon successful validation. The OTP token validation failure is counted against the maximum OTP failure count.

Resetting locked accounts

The User editor displays a "Lock" icon for a user locked due to exceeding the maximum attempts of password or OTP. The unlocking process is the same as described under *Failed Logins* section.

Note  :

- Please contact LiveVox Client Services to enable Dual Factor Authentication option and specify Max Failed Login OTP Attempts.
- Dual Factor Authentication is not available for agent login.
- Second-factor authorization is not supported via email, SMS and voice message.

Setting up WinAuth Application for Dual Factor Authentication

WinAuth application can be used by Desktop users to generate OTP for second level verification. Follow the below procedure for initial set up of the WinAuth Authenticator.

Download the WinAuth app by clicking <https://winauth.github.io/winauth/>.

Once downloaded, double click the WinAuth application to set up a new Authenticator:

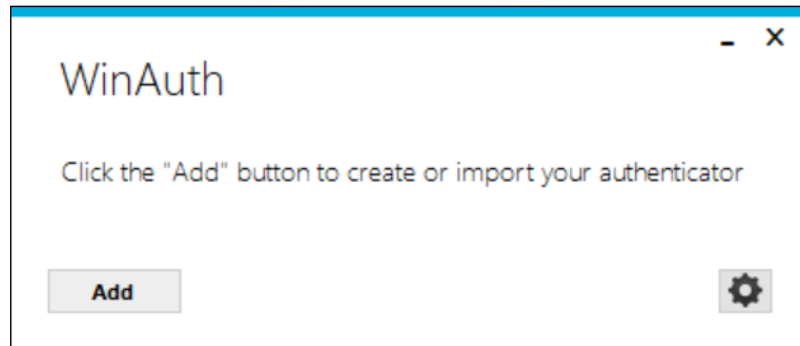


Figure 21: WinAuth Application

Click the **Add** button to set up an Authenticator and you will be presented with the Add Authenticator window.

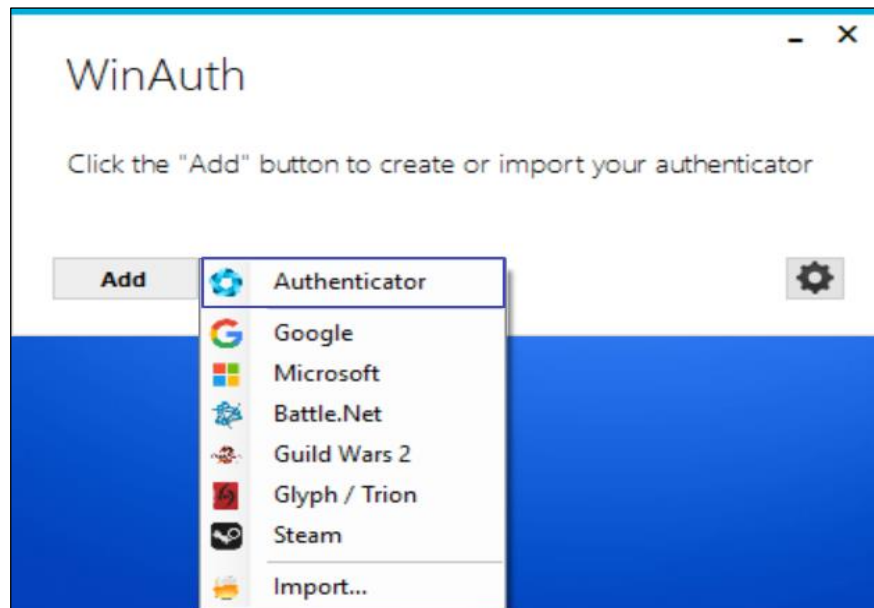


Figure 22: Adding a new Authenticator

The Add Authenticator window allows you to configure the following:

- Enter the name of the Authenticator in the Name field.
- Copy the QR code displayed on OTP Activation screen into WinAuth.
- Set the authenticator type as time-based.
- Click the **Verify Authenticator** button in order to preview the first generated code.
- Do not click Ok button on the Add Authenticator window at this point.

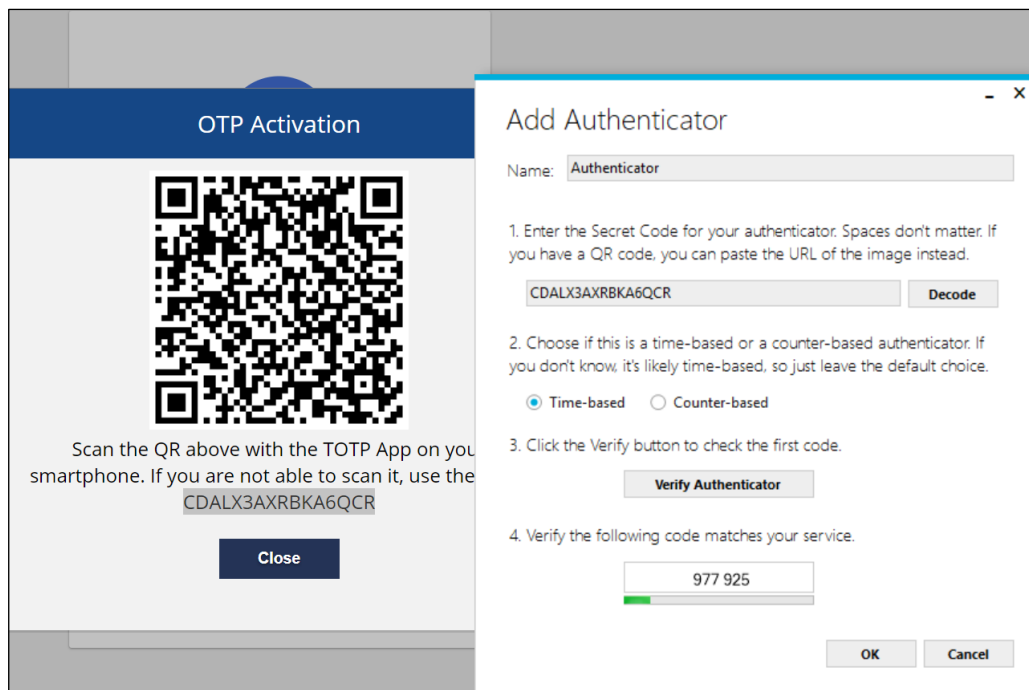


Figure 23: Configuring Authenticator details

Close the OTP Activation window and you will be prompted with Enter OTP window as shown in Figure 17, where you can enter the code presented on the WinAuth.

Once done, click Ok button on the Add Authenticator screen of WinAuth and you will be presented with the following screen to lock the WinAuth app, if you wish to lock the app.

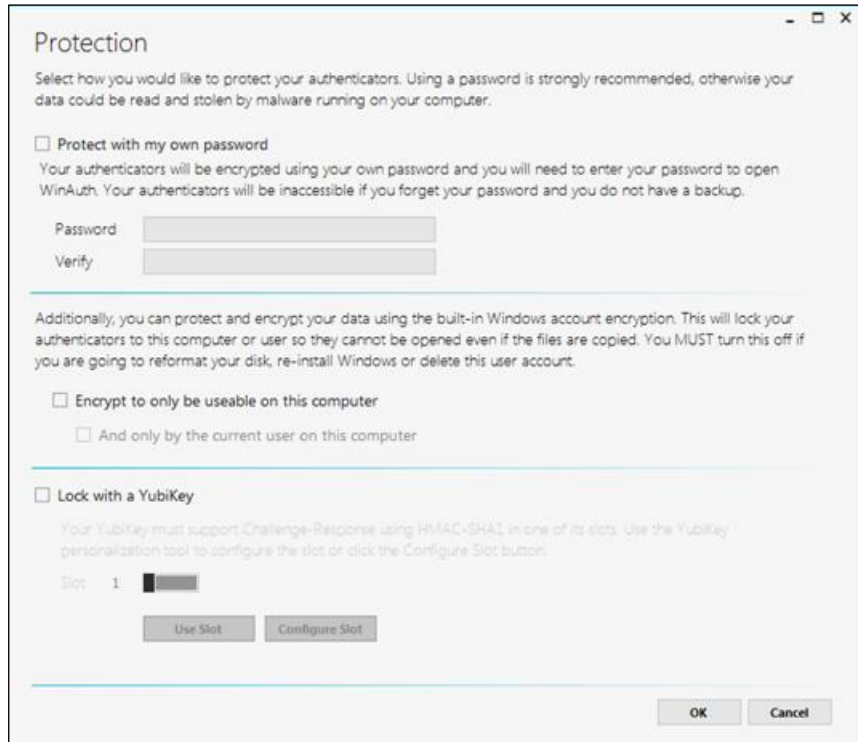


Figure 24: Protection config

Set the required Password and click Ok button on the Protection config and use WinAuth to verify OTP as normal.