



**LIVE**VOX

# Password Management Functionality

---

Support Contacts:

24 Hour Support Line: 888.477.3448

Support Email: [support@livevox.com](mailto: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This document is an unpublished work protected by the United States copyright laws and is proprietary to LiveVox, Inc. ("LiveVox").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 September 7, 2018

For Internal and Client Use Only

---

## Contents

---

<b>Introduction.....</b>	<b>4</b>
<i>Document Purpose.....</i>	<i>4</i>
<b>Password Management features .....</b>	<b>4</b>
<i>General Guidelines.....</i>	<i>4</i>
<i>Security Settings.....</i>	<i>6</i>
<i>Setting up Agents and Users.....</i>	<i>7</i>
<i>Logging In.....</i>	<i>9</i>
<i>Resetting Expired Password.....</i>	<i>10</i>
<i>Failed Logins.....</i>	<i>12</i>
<i>Dual Factor Authentication.....</i>	<i>15</i>
OTP Enrolment Status.....	20
Changing passwords.....	20
Resetting locked accounts.....	20
Setting up WinAuth Application for Dual Factor Authentication.....	21

# 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.

# Password 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)! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- Permitted voice portal users can set the account password temporarily and force the users or agents to change the password on the first login or when the password is updated. If permitted voice portal users change the password for their own user account, they are not prompted to change the password. This feature is configurable at the client level and applied to both users and agents.
- 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](mailto: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.

## Security Settings

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

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

- Password Expire Days - Set number of days for the password expiration. Applies to both users and agents.

**Note**  : *When implementing a password expire period for the first time or reducing the number of days in the current period, it is recommended that all agents be logged out to prevent any call interruption due to password expiration. In addition, if your portal uses any LiveVox Custom Applications (Scripter, for example) or you are unsure if you have integrated these types of apps, please reach out to your Account Management team before adding, removing or making any changes to the Password Expire Period as this may interrupt any active LiveVox Custom Applications.*

- Max Failed Login Attempts - Set number of password attempts after which the user or agent will be locked out. The value of **Max Failed Login Attempts LVP** and **Max Failed Login Attempts Agent** must be between 1 and 9. Zero, null, and characters are invalid.
- Browser Session Security - If selected, user will have to log back in any time the browser is closed.
- 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.
- Admin Set Passwords Are Temporary - If selected, then the system forces the users or agents to change the password on the first login or when the password is updated. Once they log in with the temporary password, they will be asked to change the password.

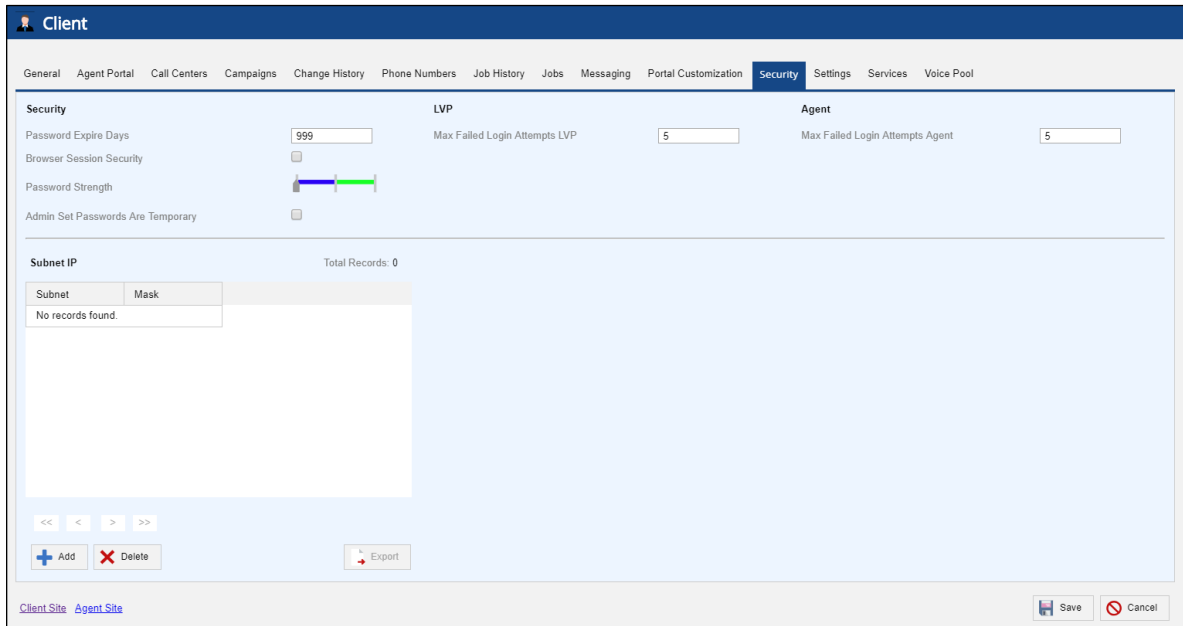


Figure 1: Client editor security tab

## 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**.

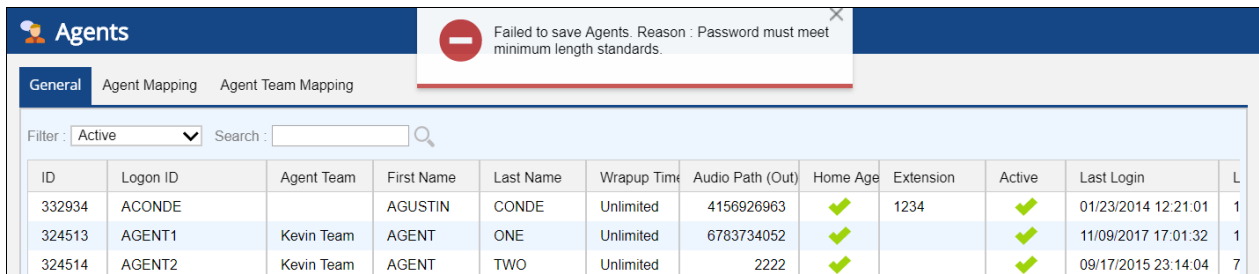


Figure 2: Failure to save agent

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

The screenshot shows the 'Agents' configuration interface. An error message is displayed at the top: "Failed to save Agents. Reason : Password must contain at least one digit." Below the error, there is a table of agents. The table has columns: ID, Logon ID, Agent Team, First Name, Last Name, Wrapup Time, Audio Path (Out), Home Age, Extension, Active, Last Login, and L.

ID	Logon ID	Agent Team	First Name	Last Name	Wrapup Time	Audio Path (Out)	Home Age	Extension	Active	Last Login	L
332934	ACONDE		AGUSTIN	CONDE	Unlimited	4156926963	✓	1234	✓	01/23/2014 12:21:01	1
324513	AGENT1	Kevin Team	AGENT	ONE	Unlimited	6783734052	✓		✓	11/09/2017 17:01:32	1

Figure 3: Failure to save agent

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

The screenshot shows the 'Agents' configuration interface. An error message is displayed at the top: "Failed to save Agents. Reason : Password must have at least one character." Below the error, there is a table of agents. The table has columns: ID, Logon ID, Agent Team, First Name, Last Name, Wrapup Time, Audio Path (Out), Home Age, Extension, Active, Last Login, and Last IP.

ID	Logon ID	Agent Team	First Name	Last Name	Wrapup Time	Audio Path (Out)	Home Age	Extension	Active	Last Login	Last IP
332934	ACONDE		AGUSTIN	CONDE	Unlimited	4156926963	✓		✓	01/23/2014 12:21:01	10.40.49.200
549765	AGENT	Kevin Team	agent	new	Unlimited	4158149720	✓	3333	✓	08/02/2017 01:48:14	115.248.129.122

Figure 4: 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**.

The screenshot shows the 'User' configuration interface. An error message is displayed at the top: "'newuser': Failed to save User. Reason : Password must meet minimum length standards." Below the error, there is a table of users. The table has columns: User Name, First Name, Last Name, E-Mail, Role, Last Login, Last IP, Services, and Analytics Dashboards.

User Name	First Name	Last Name	E-Mail	Role	Last Login	Last IP	Services	Analytics Dashboards
Sujith_sysadmin	Sujith_sysadmin	livevox123		Sysadmin	04/11/2016 02:42:17	106.51.39.123	✓	✓
superfelipe	Felipe	Super	fvega@livevox.com	Superuser	02/17/2016 10:40:58	190.7.146.242	✓	✓
super_jose	Jose	Borunda	jb@livevox.com	Superuser	12/20/2013 12:17:42	201.141.7.99	✓	✓
sysadmin1	Sys	Admin		Sysadmin	12/26/2016 13:49:15	10.40.234.73	✓	✓

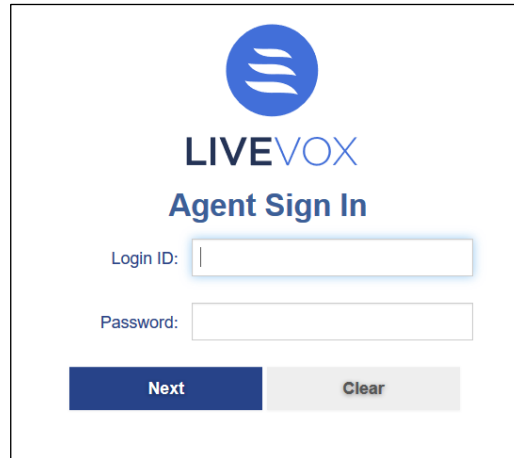
Figure 5: Failure to save new user



## Logging In

### Login

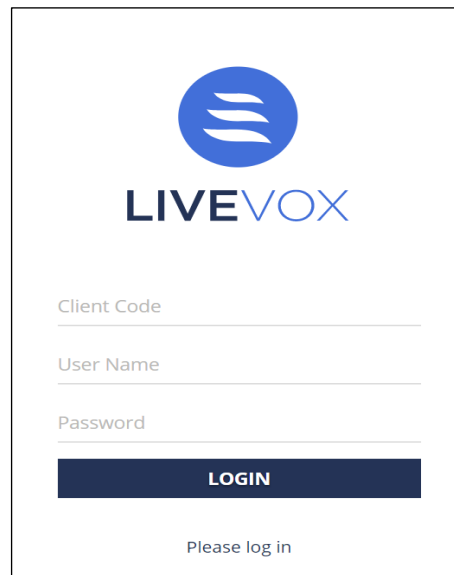
- Agent Login (via agent link provided by LiveVox). Enter Login ID and Password. Click **Next** button to log in.



The image shows a web form for Agent Sign In. At the top is the LiveVox logo, a blue circle with three white horizontal lines. Below the logo is the text "LIVEVOX" in blue and "Agent Sign In" in bold blue. There are two input fields: "Login ID:" followed by a white text box with a blue border, and "Password:" followed by a white text box with a blue border. At the bottom are two buttons: a dark blue button labeled "Next" and a light gray button labeled "Clear".

Figure 6: Agent login

- User login (via user link provided by LiveVox). Enter the Client Code, User Name, and Password. Click **Login** button to log in.



The image shows a web form for User login. At the top is the LiveVox logo, a blue circle with three white horizontal lines. Below the logo is the text "LIVEVOX" in blue. There are three input fields: "Client Code" followed by a white text box, "User Name" followed by a white text box, and "Password" followed by a white text box. At the bottom is a dark blue button labeled "LOGIN". Below the button is the text "Please log in".

Figure 7: User login

- For more information on failed login, see *Failed Logins* section.

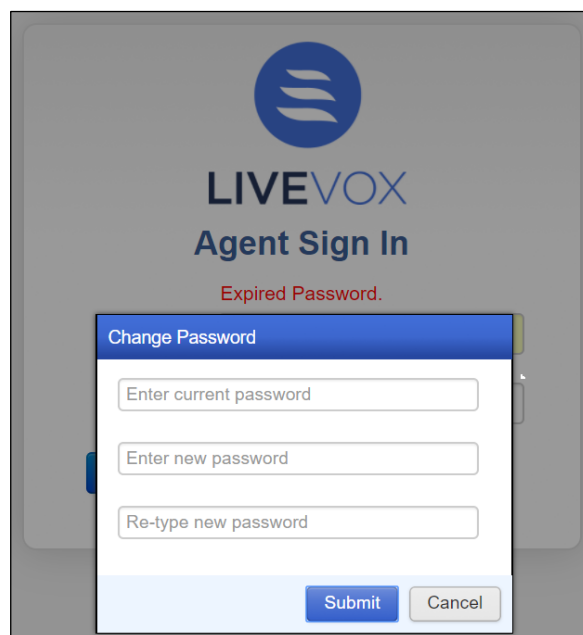
- If the account password is set temporarily, then the system forces the users or agents to change the password on the first login or when the password is updated. Once they log in with the temporary password, they will be asked to change the password. For changing the password, see *Resetting Expired Password* section. If the Dual Factor Authentication (DFA) is enabled, see *Changing passwords* section for more information.

○

## ***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.

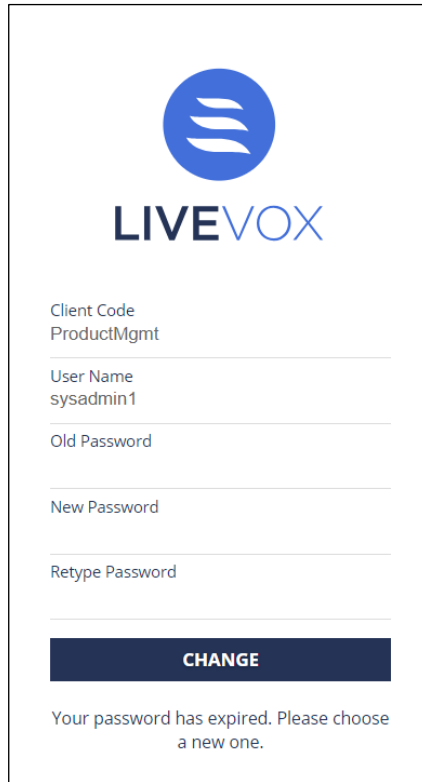
- Agents




The screenshot shows the LIVEVOX Agent Sign In interface. At the top, there is the LIVEVOX logo and the text "Agent Sign In". Below this, a red error message reads "Expired Password.". A modal dialog box titled "Change Password" is open in the center. It contains three input fields: "Enter current password", "Enter new password", and "Re-type new password". At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

*Figure 8: Agent sing in for expired password*

- Users



  
**LIVEVOX**

Client Code  
ProductMgmt

User Name  
sysadmin1

Old Password

New Password

Retype Password

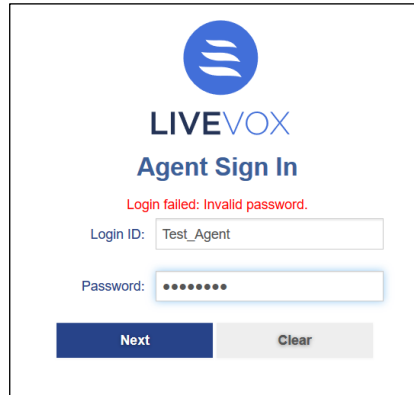
**CHANGE**

Your password has expired. Please choose a new one.

*Figure 9: User password expired*

## Failed Logins

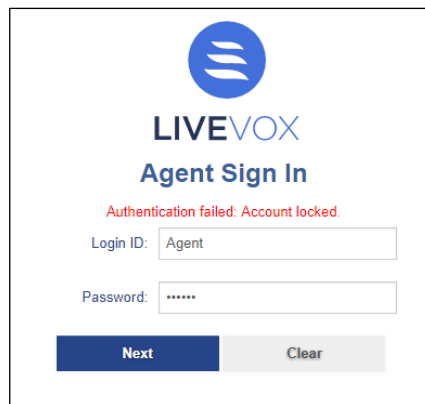
- Agents
  - The Agent login screen displays error message when an invalid password is entered by an agent.



The screenshot shows the LIVEVOX Agent Sign In interface. At the top is the LIVEVOX logo. Below it, the text "Agent Sign In" is displayed. A red error message reads "Login failed: Invalid password." Below the error message are two input fields: "Login ID:" with the value "Test\_Agent" and "Password:" with masked characters "\*\*\*\*\*". At the bottom are two buttons: "Next" (dark blue) and "Clear" (light gray).

*Figure 10: Agent login failed*

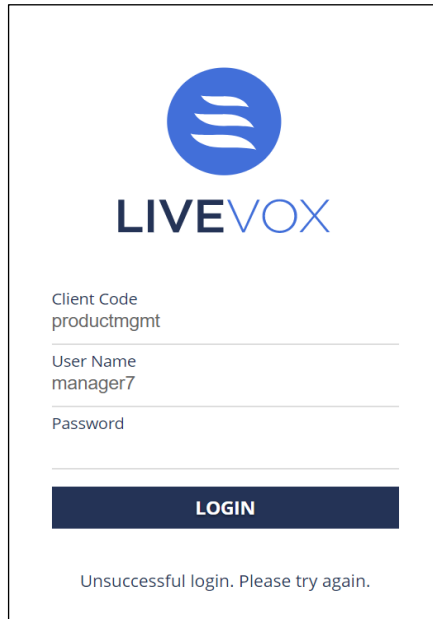
- If an agent attempts to log in with the wrong password more times than the site's configured limit, the agent will be locked out and presented with the following screen:



The screenshot shows the LIVEVOX Agent Sign In interface. At the top is the LIVEVOX logo. Below it, the text "Agent Sign In" is displayed. A red error message reads "Authentication failed: Account locked." Below the error message are two input fields: "Login ID:" with the value "Agent" and "Password:" with masked characters "\*\*\*\*\*". At the bottom are two buttons: "Next" (dark blue) and "Clear" (light gray).

*Figure 11: Agent account locked*

- Users
  - The login screen displays the following message when an invalid password is entered by the user.



The screenshot shows the LIVEVOX login interface. At the top center is the LIVEVOX logo, consisting of a blue circle with three white horizontal lines and the text "LIVEVOX" below it. Below the logo are three input fields: "Client Code" with the value "productmgmt", "User Name" with the value "manager7", and "Password" which is empty. A dark blue "LOGIN" button is positioned below the password field. At the bottom of the form, the message "Unsuccessful login. Please try again." is displayed.

*Figure 12: Unsuccessful user login*

- 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:

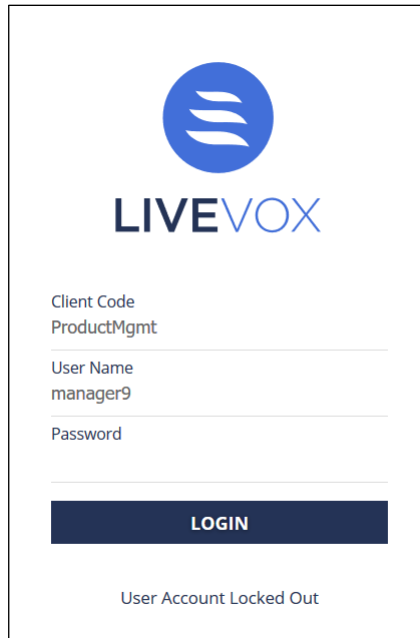


Figure 13: User account locked

- To unlock the user or agent, permitted user can double click on the lock icon and confirm the action from User or Agents editor.

The screenshot shows the 'Agents' management interface. A table lists various agents with columns for ID, Logon ID, Agent Team, First Name, Last Name, Wrapup Time, Audio Path (Out), Home Age, Extension, Active status, Last Login, Last IP, and Email. A 'Confirm' dialog box is overlaid on the table, asking for confirmation to unlock an agent's account due to 5 consecutive unsuccessful login attempts. The dialog has 'OK' and 'Cancel' buttons.

ID	Logon ID	Agent Team	First Name	Last Name	Wrapup Time	Audio Path (Out)	Home Age	Extension	Active	Last Login	Last IP	Email
332934	ACONDE		AGUSTIN	CONDE	Unlimited	4156926963	✓		✓	01/23/2014 12:21:01	10.40.49.200	2444@100.64.19
549765	AGENT	Kevin Team	agent	new	Unlimited	4158149720	✓	3333	✓	08/02/2017 01:48:14	115.248.129.122	
521091	AGENT1		agent	bond	Unlimited	555	✓	123123	✓	08/04/2016 16:01:01	187.237.14.230	
521092	AGENT#.?		agent	bourne	Unlimited	555	✓	22222	✓	08/04/2016 16:05:09	187.237.14.230	
513804	AGENT-ANINDITA	Kevin Team	Anindita	password123	Unlimited	6503517454	✓	0123	✓	12/14/2016 02:10:21	182.75.26.194	12345@100.64.1.09
523329	AGENT-ONE	Kevin Team	AGENT	ONE	Unlimited	6503517454	✓	650	✓	08/23/2016 05:06:07	182.75.26.194	
523288	AGENT001		Agent001	password123					✓	09/19/2017 15:30:13	12.151.97.234	
324513	AGENT1	Kevin Team	AGENT	ONE			✓		✓	07/16/2018 14:59:01	201.103.241.142	
324514	AGENT2	Kevin Team	AGENT	TWO			✓		✓	10/02/2017 13:19:44	189.146.243.177	
324515	AGENT3	Kevin Team	AGENT	THREE			✓		✓	05/19/2017 18:50:11	189.146.225.138	
324516	AGENT4	Kevin Team	AGENT	FOUR			✓		✓	03/31/2014 15:35:01	10.40.2.210	
324517	AGENT5	Kevin Team	AGENT	FIVE			✓		✓	08/03/2016 10:01:44	187.237.14.239	
324518	AGENT6	Kevin Team	AGENT	SIX	Unlimited	6666	✓		✓	01/30/2017 11:08:00	12.127.62.202	
592546	AGENT7		Agent	One	Unlimited	6783634060	✓		✓	08/14/2018 06:22:58	115.248.129.122	
394752	AGENT_AT		Arlan	Tokugawa	Unlimited	4156716004	✓		✓	04/26/2018 18:38:01	206.15.76.98	
394751	AGENT_HCI		Arlan	Tokugawa	Unlimited	4156716004	✓		✓			
544599	AGENT_SH		123		Unlimited	5555			✓	03/21/2018 11:57:54	206.15.76.98	
526888	AMALLOY	Demo	Agent		Unlimited	4048626497			✓	01/25/2017 15:56:36	73.54.142.166	
526656	AMALLOYCLOSER	Demoq	Closer		Unlimited	6786991219			✓			
526654	AMALLOYINIT	Demo	Initiator		Unlimited	4048626497			✓	10/07/2016 10:10:18	50.160.232.212	
560048	ASHAW		pass	livevox1	Unlimited	6503517454	✓		✓	05/31/2018 02:52:17	182.75.26.194	
549874	AVINASH		avinash	shivaswamy	Unlimited	6503517536	✓		✓	01/18/2017 08:24:53	182.75.26.194	
539055	BATMAN	Erwins Team	Bruce	Wayne	Unlimited	12345	✓	5555	✓	11/01/2016 16:02:32	206.15.76.98	

Figure 14: Example of unlocking the locked agent

## 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*:

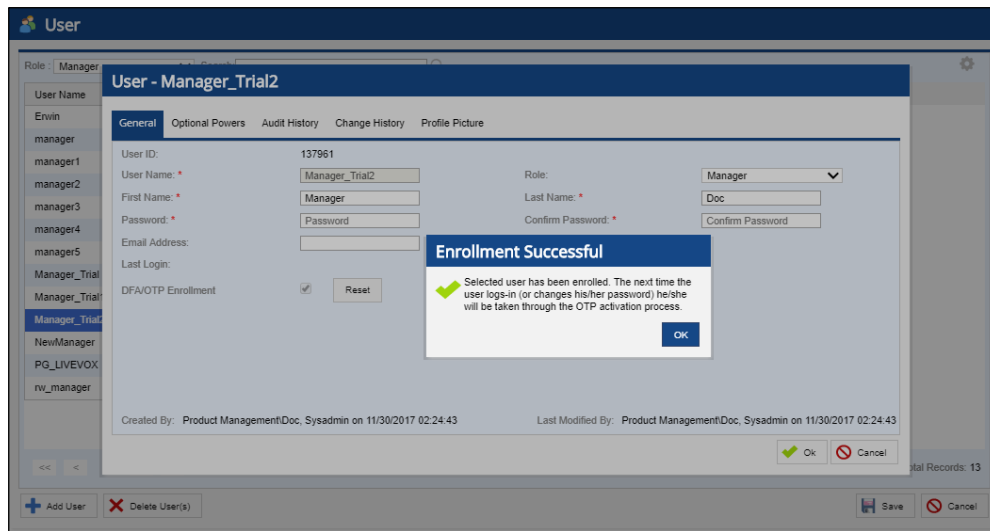
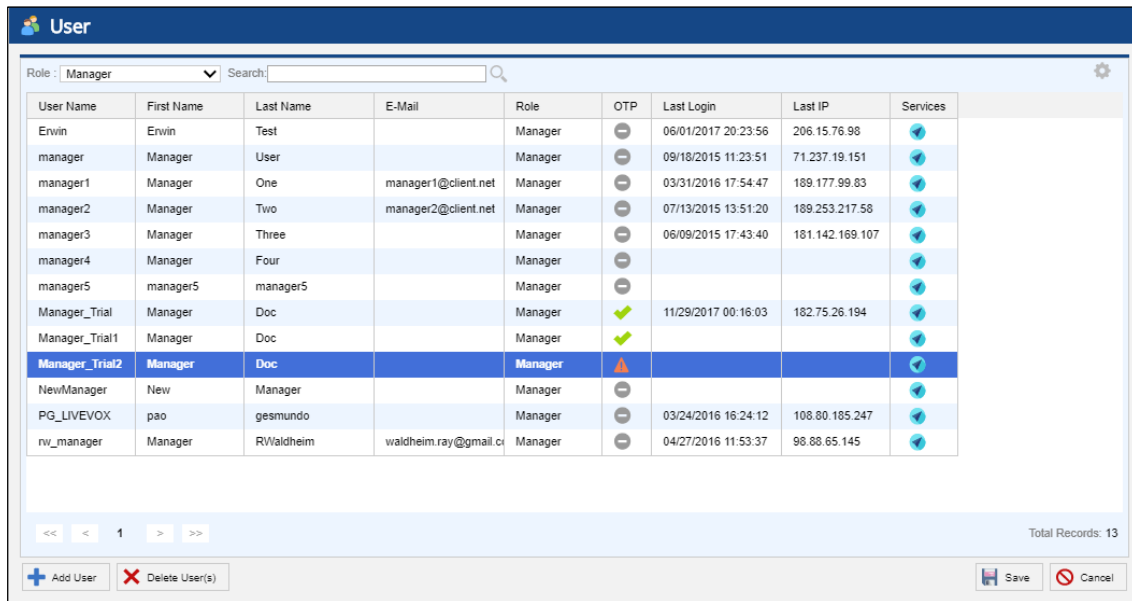


Figure 15: DFA Enrollment for User

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	✔
rv_manager	Manager	RWaldheim	waldheim.ray@gmail.c	Manager	—	04/27/2016 11:53:37	98.88.65.145	✔

Figure 16: User Account Pending Activation

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

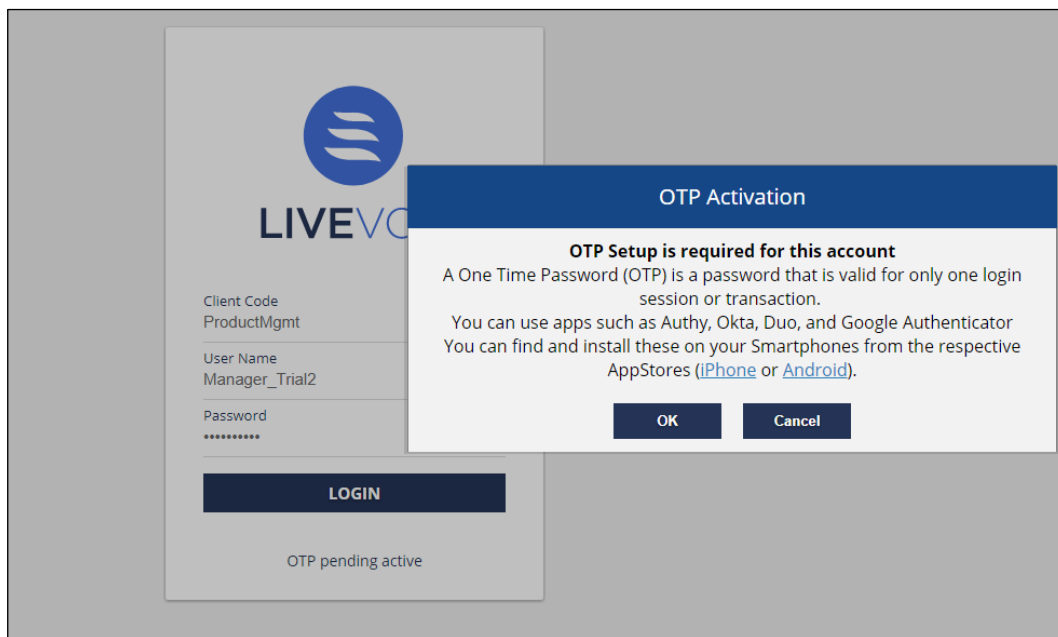
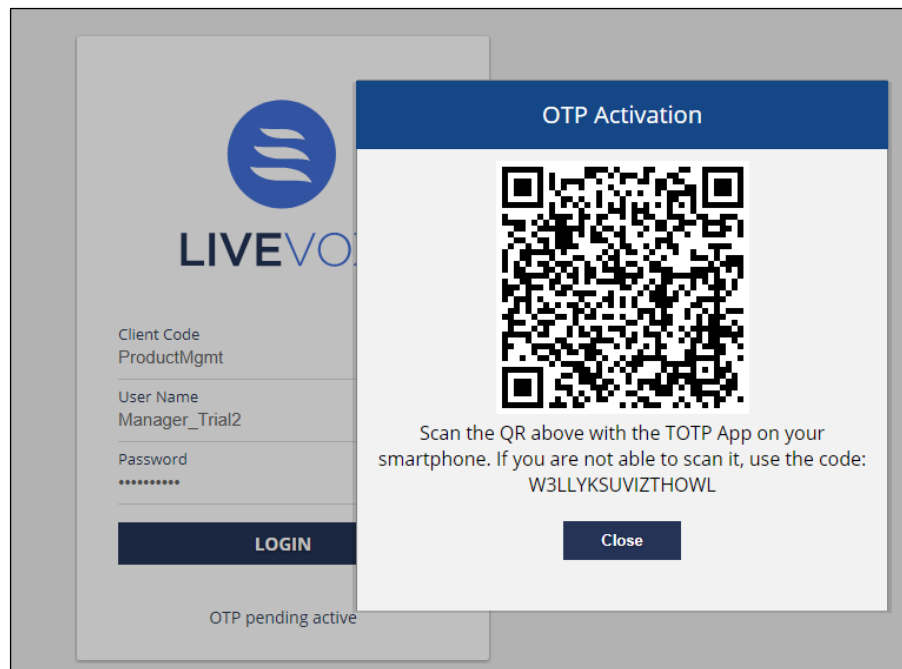


Figure 17: User login for Dual Factor Authentication



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 18: 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.

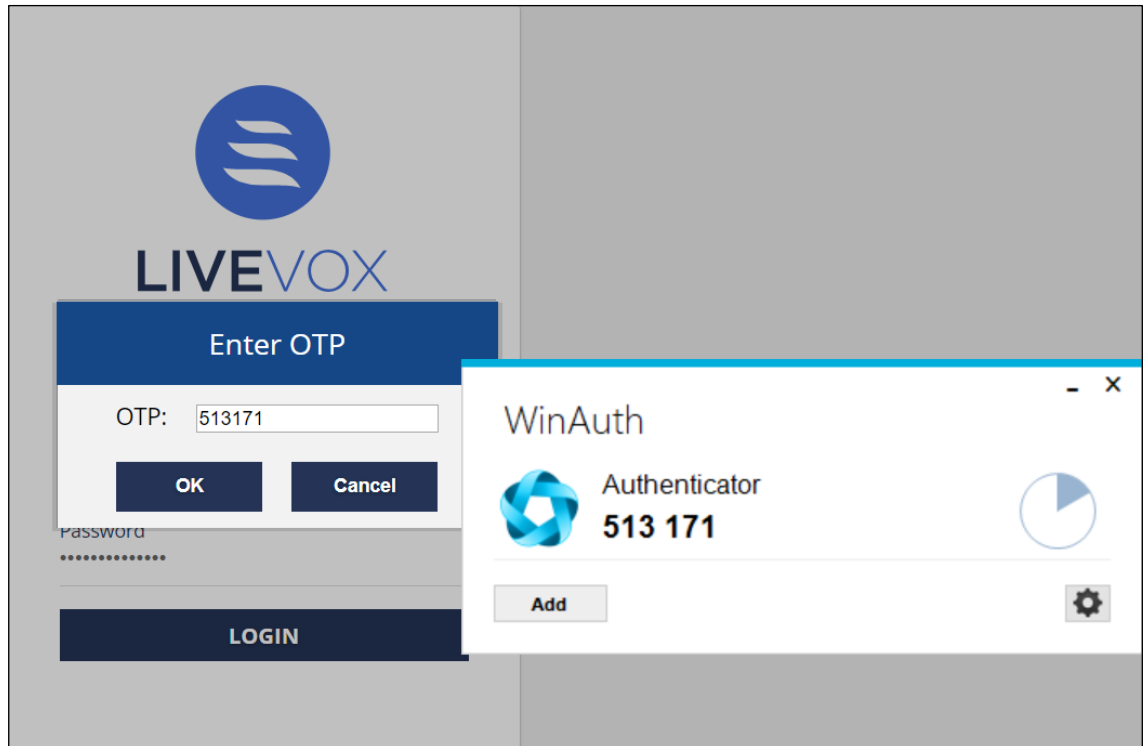
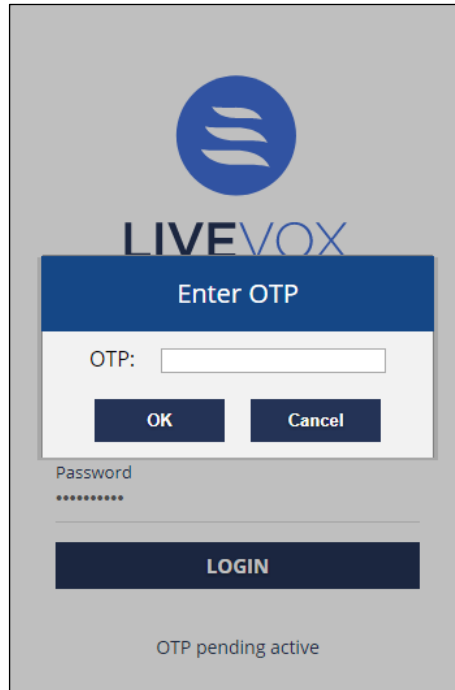


Figure 19: OTP verification via WinAuth

- 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:

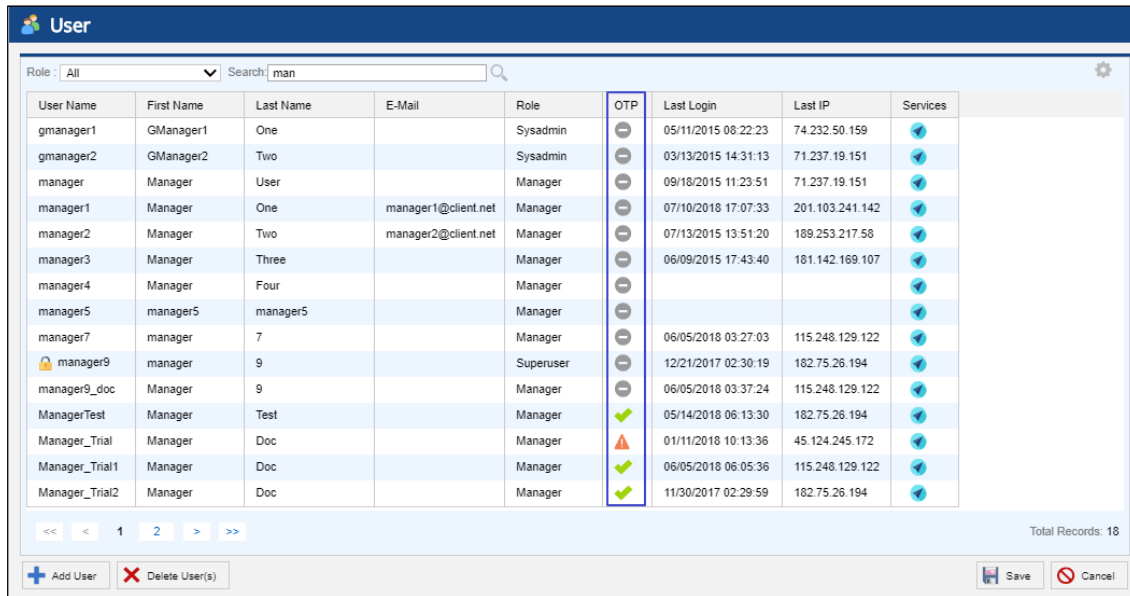


*Figure 20: One Time Password verification*

- 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 21: 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. To unlock the user, permitted user can double click on the lock icon and confirm the action.

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:

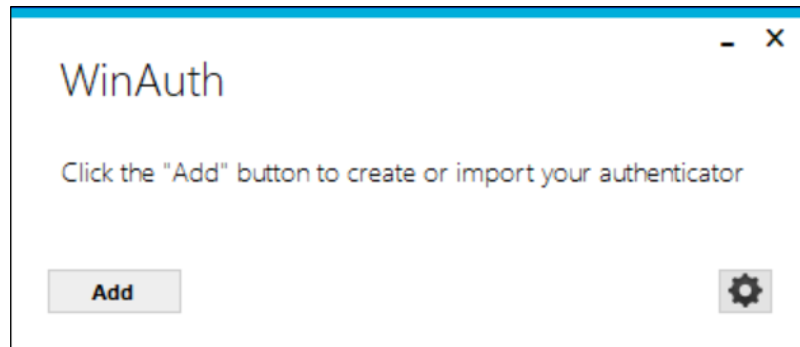


Figure 22: WinAuth Application

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

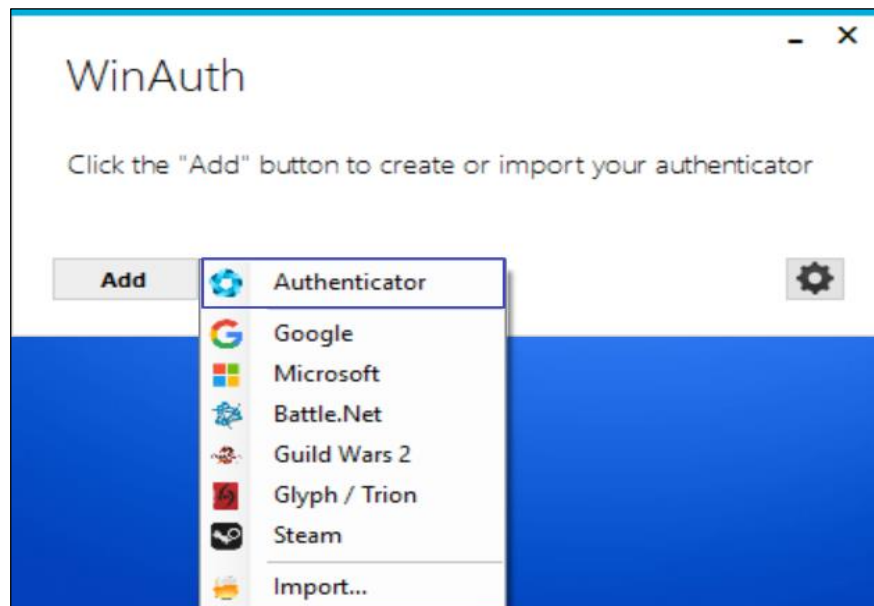
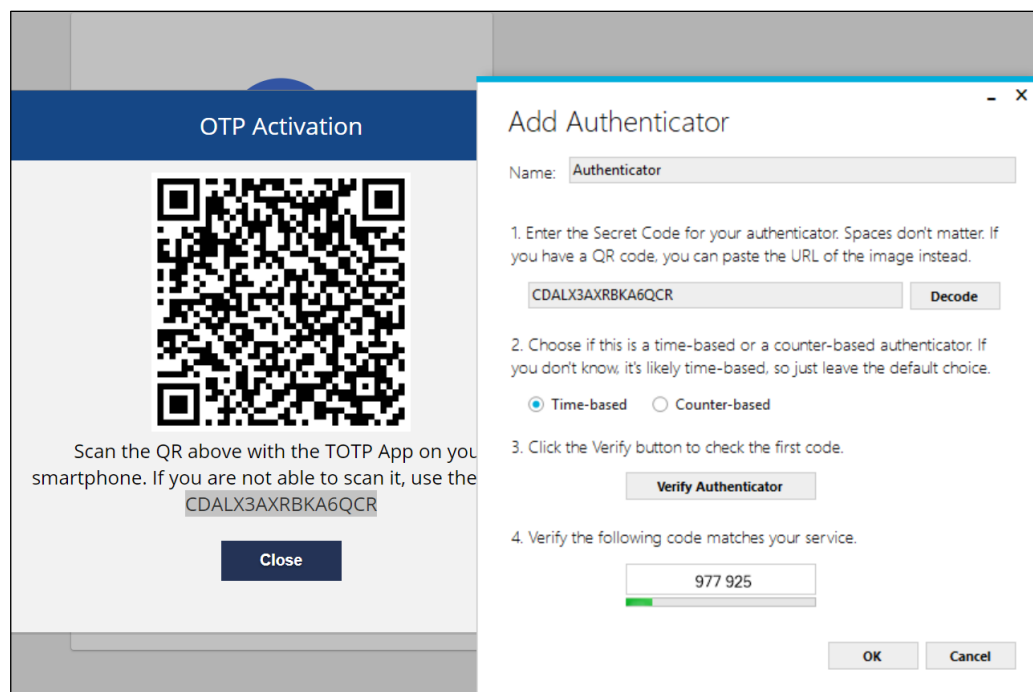


Figure 23: Adding a new Authenticator

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 24: 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.

Protection

Select how you would like to protect your authenticators. Using a password is strongly recommended, otherwise your data could be read and stolen by malware running on your computer.

Protect with my own password  
Your authenticators will be encrypted using your own password and you will need to enter your password to open WinAuth. Your authenticators will be inaccessible if you forget your password and you do not have a backup.

Password

Verify

Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You MUST turn this off if you are going to reformat your disk, re-install Windows or delete this user account.

Encrypt to only be useable on this computer  
 And only by the current user on this computer

Lock with a YubiKey  
Your YubiKey must support Challenge-Response using HMAC-SHA1 in one of its slots. Use the YubiKey personalization tool to configure the slot or click the Configure Slot button.

Slot: 1

Use Slot    Configure Slot

OK    Cancel

*Figure 25: Protection config*

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