

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This document is an unpublished work protected by the United States copyright laws and is proprietary to LiveVox, Inc. ("LiveVox").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
Document Purpose4
Management features
General Guidelines4
How does it work?
Setting up Agents and Users8
Resetting Expired Password9
Failed Logins
Security Settings
Dual Factor Authentication
OTP Enrolment Status18
Changing passwords
Changing passwords
Setting up WinAuth Application for Dual Factor Authentication



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:

- 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 - <u>client-services@livevox.com</u>.
 - 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).

	3
LIV	EVOX
Agent	t Sign In
Login ID:	
Password:	
Next	Clear

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:

	_IVEV	ΌΧ	
A	gent Si	gn In	
Logi	n failed: Invalid	password.	
Login ID:	Test_Agent		
Password:	•••••		
Next		Clear	

Figure 2: Agent login failed



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

Lľ	S VEVOX
Client Code	
User Name	
Password	
	LOGIN
	Please log in

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:

LIVEVOX
Client Code productmgmt
User Name manager7
Password
LOGIN
Unsuccessful login. Please try again.
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**.

💈 Agen	nts		C	Failed to save minimum leng		n : Password must r	meet				
General /	Agent Mapping Agen	t Team Mapping					_				
Filter : Activ	ve 🗸 Searc	h :	0								
ID	Logon ID	Agent Team	First Name	Last Name	Wrapup Time	Audio Path (Out)	Home Age	Extension	Active	Last Login	1
332934	ACONDE		AGUSTIN	CONDE	Unlimited	4156926963	*	1234	×	01/23/2014 12:21:01	-
324513	AGENT1	Kevin Team	AGENT	ONE	Unlimited	6783734052	-		*	11/09/2017 17:01:32	
			AGENT	TWO	Unlimited	2222				09/17/2015 23:14:04	T

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:

🛓 Agen	ts			Failed to save contain at leas		: Password must	×				
General A	Agent Mapping Agent 7	Feam Mapping					_				
Filter : Activ	e 🗸 Search		0								
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 6: Failure to save agent

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

🔽 Agen	nts				to save Agents st one character	. Reason : Passwo		×			
General	Agent Mapping Agent T	eam Mapping						_			
Filter : Activ	ve 🗸 Search :		0								
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 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**.

🖇 User					ewuser' : Failed to save Use ust meet minimum length st		d ×	
Role : All	✔ Se	arch:	0				_	
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	1	1
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 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

LIVEVOX	
Agent Sign In	
Expired Password.	
Change Password	
Enter current password	
Enter new password	
Re-type new password	
Submit Cancel	

Figure 9: Agent sing in for expired password



• Users

LI	VEVOX
Client Code ProductMgmi	t
User Name sysadmin1	
Old Password	
New Password	1
Retype Passwo	ord
	CHANGE
Your passwor	rd 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:

I	LIVE	VOX
Α	gent S	Sign In
Authent	ication faile	I: Account locked.
Login ID:	Agent	
Password:	•••••	
Next		Clear

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:

S LIVEVOX	
Client Code ProductMgmt	
User Name manager9	
Password	
LOGIN	
User Account Locked Out	



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.

General Agent Fortal Call Cen	iters Campaigns	Change History Phones	Job History Jobs	Messaging Por	rtal Customization Security	Settings Services	Voice Pool	
Security		LVP			Agent			
Password Expire Days		Max Failed Login /	Attempts LVP		Max Failed Login	Attempts Agent		
Browser Session Security								
Password Strength								
Subnet IP		Total Records: 0						
Subnet Mask								
No records found.								
« < > »								
+ Add X Delete								
		Export						

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:*

🂰 User		
Role : Manager	User - Manager_Trial2	٥
User Name Erwin		
manager	General Optional Powers Audit History Change History Profile Picture	
manager1	User ID: 137961	
manager2	User Name: * Manager_Trial2 Role: Manager V	
manager3	First Name: * Doc	
manager4	Password: * Password Confirm Password: * Confirm Password	
manager5	Email Address: Enrollment Successful	
Manager_Trial	Selected user has been enrolled. The next time the	
Manager_Trial'	DFA/OTP Enrollment Reset visuer logs-in (or changes his/her password) he/she will be taken through the OTP activation process.	
Manager_Trial2	ок	
NewManager		
PG_LIVEVOX nv_manager		
Tw_manager		
	Created By: Product Management/Doc, Sysadmin on 11/30/2017 02:24:43 Last Modified By: Product Management/Doc, Sysadmin on 11/30/2017 02:24:43	
<< <	Van Cancel / tal Recon	ds: 13
+ Add User	Celete User(s)	ancel

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.

irst Name rwin	Last Name	E-Mail	Role	OTP				
	Test		Manager	0	Last Login 06/01/2017 20:23:56	Last IP 206.15.76.98	Services	
lanager	User		Manager	0	09/18/2015 11:23:51	71.237.19.151	•	
lanager	One	manager1@client.net	Manager	-	03/31/2016 17:54:47	189.177.99.83	•	
lanager	Two	manager2@client.net	Manager		07/13/2015 13:51:20	189.253.217.58	•	
lanager	Three		Manager	0	06/09/2015 17:43:40	181.142.169.107	•	
lanager	Four		Manager	0			•	
anager5	manager5		Manager	0			•	
lanager	Doc		Manager		11/29/2017 00:16:03	182.75.26.194	•	
lanager	Doc		Manager				•	
lanager	Doc		Manager				Ø	
ew	Manager		Manager	•				
ao	gesmundo		Manager	•	03/24/2016 16:24:12	108.80.185.247		
lanager	RWaldheim	waldheim.ray@gmail.co	Manager	•	04/27/2016 11:53:37	98.88.65.145	<	
la la la la la a la a	nager nager nager nager nager nager w w o	nager One nager Two nager Three nager Four nager5 manager5 nager Doc nager Doc w Manager o gesmundo	anger One manager1@client.net nager Two manager2@client.net nager Three Tanger Four Three nager Four Canager5 manager5 manager5 Canager Doc Canager Doc Canager Doc Canager Doc Canager Doc Canager Doc Canager Sub Canager S	One manager1@client.net Manager nager Two manager2@client.net Manager nager Three Manager2@client.net Manager nager Three Manager2@client.net Manager nager Four Manager Manager nager Four Manager Manager nager Doc Manager Manager nager Doc Manager Manager w Manager Manager Manager p gesmundo Manager Manager	nager One manager1@client.net Manager nager Two manager2@client.net Manager nager Three Manager O nager Four Manager O nager5 manager5 Manager5 Manager nager Doc Manager ✓ nager Doc Manager ✓ nager Doc Manager ✓ nager Doc Manager ✓ w Manager Manager ✓ o gesmundo Manager ✓	nager One manager1@client.net Manager Ome 03/31/2016 17:54 47 nager Two manager2@client.net Manager Ome 07/13/2015 13:51:20 nager Three Manager Ome 06/09/2015 17:43:40 nager Four Manager Ome 06/09/2015 17:43:40 nager Four Manager Ome 06/09/2015 17:43:40 nager Four Manager Ome 0 nager Doc Manager Ome 11/29/2017 00:16:03 nager Doc Manager Ome 0 nager Doc Manager Ome 0 w Manager Imager Manager Ome w Manager Manager Ome 0 gesmundo Image Manager Ome 0	nager One manager1@client.mt Manager Imager 03/31/2016 17.54.47 189.177.99.83 nager Two manager2@client.mt Manager Imager 0/11/32015 13.51.20 189.253.217.58 nager Three Manager Imager Imager2@client.mt Manager Imager2@client.mt Manager2@client.mt Manager2@client.mt	nager One manager@client.net Manager 03/31/2016 17:54-47 189.177.99.83 Imager nager Two manager@client.net Manager 07/13/2015 13:51:20 189.253.217.58 Imager nager Three Manager Imager 06/09/2015 17:33:40 181.142.169.107 Imager nager Four Manager Imager 06/09/2015 17:33:40 181.142.169.107 Imager nager Four Manager Imager 06/09/2015 17:33:40 181.142.169.107 Imager nager Four Manager Imager Imager

Figure 15: User Account Pending Activation

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

LIVEVO	OTP Activation
Client Code ProductMgmt User Name Manager_Trial2 Password	OTP Setup is required for this account A One Time Password (OTP) is a password that is valid for only one login session or transaction. You can use apps such as Authy, Okta, Duo, and Google Authenticator You can find and install these on your Smartphones from the respective AppStores (iPhone or Android).
LOGIN OTP pending activ	e

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:

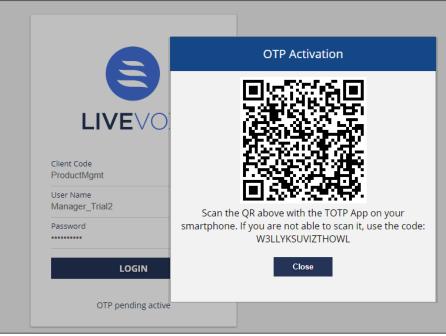


Figure 17: QR Code for OTP Activation



- 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.

Enter OTP		
OTP: 513171 OK Cancel Password LOGIN	WinAuth Authenticator 513 171	- ×

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:

Enter OTP	
OTP:	
Password LOGIN	
OTP pending active	

Figure 19: One Time Password verification

- \circ $\,$ 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.

Jser Name	First Name	Last Name	E-Mail	Role	OTP	Last Login	Last IP	Services	
gmanager1	GManager1	One		Sysadmin	0	05/11/2015 08:22:23	74.232.50.159	<	
gmanager2	GManager2	Two		Sysadmin	0	03/13/2015 14:31:13	71.237.19.151	•	
manager	Manager	User		Manager	0	09/18/2015 11:23:51	71.237.19.151	•	
manager1	Manager	One	manager1@client.net	Manager	0	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	0				
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.



- 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 <u>https://winauth.github.io/winauth/</u>.

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

WinAuth	-	x
Click the "Add" button to create or import your authentic	ator	
Add	¢	ł

Figure 21: WinAuth Application



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

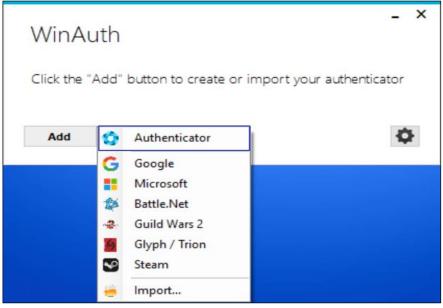


Figure 22: Adding a new Authenticator



The Add Authenticator window allows you to configure the following:

- $\circ~$ 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.
- $\circ~$ Do not click Ok button on the Add Authenticator window at this point.

OTP Activation	Add Authenticator
	Name: Authenticator
	 Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.
	CDALX3AXRBKA6QCR Decode
	Choose if this is a time-based or a counter-based authenticator. If you don't know, it's likely time-based, so just leave the default choice.
	 Time-based Counter-based
Scan the QR above with the TOTP App on you smartphone. If you are not able to scan it, use the	3. Click the Verify button to check the first code.
CDALX3AXRBKA6QCR	Verify Authenticator
Close	4. Verify the following code matches your service.
	977 925
	OK Cancel

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.

Protection	
the second s	protect your authenticators. Using a password is strongly recommended, otherwise your en by malware running on your computer.
	assword encrypted using your own password and you will need to enter your password to open rs will be inaccessible if you forget your password and you do not have a backup.
Password	
Verify	
you are going to reformat)	ter or user so they cannot be opened even if the files are copied. You MUST turn this off if our disk, re-install Windows or delete this user account.
you are going to reformat)	our disk, re-install Windows or delete this user account.
you are going to reformatly Encrypt to only be u And only by the Lock with a YubiKey Your YubiKey mathematic	our disk, re-install Windows or delete this user account. seable on this computer current user on this computer
you are going to reformatly Encrypt to only be u And only by the Lock with a YubiKey Your YubiKey mathematic	our disk, re-install Windows or delete this user account. seable on this computer current user on this computer
you are going to reformatly Encrypt to only be u And only by the CLock with a YubiKey Your YubiKey matt som personalization tool too	our disk, re-install Windows or delete this user account. seable on this computer current user on this computer or Challenge-Rencome using HMAC-SHAL in one of its accs. Use the YuckGey onfigure the slot or click the Configure Slot button.
you are going to reformatly Encrypt to only be u And only by the Lock with a YubiKey Your YubiKey must sup perioralization tool to Stor 1	our disk, re-install Windows or delete this user account. seable on this computer current user on this computer or Challenge-Rencome using HMAC-SHAL in one of its accs. Use the YuckGey onfigure the slot or click the Configure Slot button.

Figure 24: Protection config

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