

User Configuration

The user configuration page is available by clicking on the Users / Users submenu.

- [Creating a user](#)
- [Modifying users](#)
- [Invalidating users](#)
- [Deleting users](#)

Creating a user

You can create new Verba users by clicking on the **Add New User** link on the **Users \ Users** page. After selecting the link, the following page is opened.

User Configuration

[Find and List Groups](#)
[Back to Previous User List](#)

User Data

Group Assignment

⚠ Your email alert settings are missing or incomplete. [Learn how to configure.](#)

⚠ Synchronization is not enabled because there are no configured Active Directory Profiles.

?

User Data

Synchronized by Active Directory

Display Name*

Login ID*

E-mail Address

Location

Type*

Standard ▼

Authentication

Password*

Strength:

Confirm Password*

Password Expires

User Must Change Password at Next Logon

Step 1 - Provide the **Display Name**. This can be anything, but it should represent the ream name of the user.

Step 2 - Provide the **Login ID**. The user will use this ID when logging into the system.

Step 3 - Provide a password in the **Password** and the **Confirm Password** fields. The password field is used only when database credential-based authentication is configured for the user through the role configuration (default). For more information, see [Authentication](#).

Step 4 - Configure the user settings, see configuration reference below.

Step 5 - Click **Save**.

The following table describes the available fields:

Section	Field Name	Description	Requirements
---------	------------	-------------	--------------

User Data	ID	Unique user identifier in the database table. Automatically created, cannot be modified.	-
	Synchronized by Active Directory	Indicates if the user account was created by an Active Directory synchronization. When a user account is created by AD synchronization, fields that are synchronized from AD, cannot be changed.	-
	User's Environment	Defines the tenant for the user account. This field is only available in multi-tenant deployments.	Required field.
	Display Name	Full name of the user.	Required field. Minimum length: 3 Maximum length: 64
	Login ID	Login name of the user which is used during authentication. In the case of desktop screen capturing, the Login ID must match the user's Windows user ID (without the domain part). The desktop screen capture service lookups user information based on the Window user ID.	Required field. Minimum length: 3 Maximum length: 32 Only alphanumerical characters are allowed in this field. Must be unique in the tenant.
	Email address	Email address of the user	Minimum length: 6 Maximum length: 128 Only email addresses are allowed in this field.
	Location	Location of the user. This data is automatically populated to conversation records and can be used for filtering in search or data management policy configuration.	Maximum length: 255
	Type	Type of the user: <ul style="list-style-type: none"> Standard user - standard Verba system users with all the functionalities. Publishing Server user - Verba Publishing Server users only with very limited functionality. 	Required field.
Authentication	Password	Password for the previous Login Name field.	Required field. Minimum length: 5* Maximum length: 32 Password phrase must include at least one numeric character!** Password phrase must include at least one special character!** Password phrase must include at least one uppercase letter!** The field is case sensitive. *The minimum number of required password length can be configured. **These settings are optional and can be configured globally. For more information refer to Configuration settings for Verba Web Application .

Confirm Password	Confirmation of the Password field.	It has to match exactly the Password field.
Password Expires	<p>Indicates whether the password expires or not. If the password is expired, the user has to change it before accessing any features of the Verba system.</p> <p>The expiration duration can be configured as a global setting. For more information refer to Configuration settings for Verba Web Application.</p>	-
User must change password at next logon	Indicates whether the user has to change the password at next login or not. If this setting is enabled, the user has to change her/his password before accessing any features of the Verba system.	-
Valid From	Start date of the validation for the user. It can be configured for later or previous dates. This field is checked when a call record is inserted and the system tries to associate the call to a user through extension mapping. If a call with a phone number, which is mapped to a user, is recorded, but the Valid From date is later than the start date of the call, the call will not be associated to the user.	Required field.
Valid Until	<p>End date of the validation for the user. It can be configured for later or previous dates. This field is checked when a call record is inserted and the system tries to associate the call to a user through extension mapping. If a call with a phone number, which is mapped to a user, is recorded, but the Valid To date is earlier than the start date of the call, the call will not be associated to the user.</p> <p>Invalid or expired users are unable to login to the system.</p> <p>If the user never expires, the field is blank.</p> <p>Click on the Never expires link to invalidate the expiration of the user.</p>	Required field.
Recorder Line PIN	Press the Generate button to generate a new PIN code for the user in order to use PIN enabled Dial-in recorder ports/numbers. Simple press the Clear button to delete the PIN code.	-
Locked	<p>Indicates whether the user is locked or not. If a user is locked, she/he is unable to use the Verba Web Application.</p> <p>A user can be locked automatically if the user lockout feature is enabled in Verba Web Application. For more information refer to Configuration settings for Verba Web Application.</p>	-
API Access Only	When enabled, the user account can only be used to access the API, the user will not able to log in.	-

	Observer User (four eyes login)	Defines the 2nd (observer) user account for 4-eyes login. When configured, the user is only able to log in to the system if the credentials of the observer user account are provided during the login.	-
	Observer Group (four eyes login)	Defines the group of the 2nd (observer) user account for 4-eyes login. When configured, the user is only able to log in to the system if the credentials of one of the group members of the observer group are provided during the login.	-
Data Retention	Retention Period (days)	Defines the retention period for the users which will be applied to recorded conversations through data management policies. For more information, see Data retention .	-
	Automatically Delete Conversations after the Retention Period is Over	Defines if conversations for the user should be automatically deleted when the retention period expires.	-
Direct Policies	Direct Upload Policies	The selected upload policies will be assigned to the user and the system will use the user-extension configuration (instead of the database) to determine which policy has to be applied for the conversation recorded on the server. For more information, see U pload policy .	-
	Direct Export Policies	The selected export policies will be assigned to the user and the system will use the user-extension configuration (instead of the database) to determine which policy has to be applied for the conversation recorded on the server. For more information, see E xport policy .	-
Customizations	User Interface Language	Language parameter for the user. All user interfaces will apply this language setting.	-
	Default Timezone	Timezone setting for the user. All types of date and time information will be displayed on the user interfaces of the system in this selected timezone.	-
	Authorization Workflow	Defines the authorization workflow for the user. It overrides the group-level setting. For more information, see Authorization Requests .	-
	Custom Date Format	Optional custom date format for the user. For information on the format, see https://docs.oracle.com/javase/10/docs/api/java/text/SimpleDateFormat.html	-
	Custom Time Format	Optional custom time format for the user. For information on the format, see https://docs.oracle.com/javase/10/docs/api/java/text/SimpleDateFormat.html	-

	Environment Admins cannot Update	When enabled, the user cannot be modified by users in the tenant. Only administrators from the reference tenant (environment) can update the user configuration.	Required field.
SfB/Lync Recording Announcement	Play Notification for PSTN /Federated Inbound Calls	Enables playing a prompt for the inbound PSTN/Federated calls. The audio file can be selected from the dropdown.*	-
	Play Notification for PSTN /Federated Outbound Calls	Enables playing a prompt for the outbound PSTN/Federated calls. The audio file can be selected from the dropdown.*	-
	Music On Hold File	The audio file played for the caller in case of outbound announcement.*	-
	Play Notification for Conference Calls	Enables playing a prompt to the conference participants. The audio file can be selected from the dropdown.*	-
	IM Notification for Conference Calls	Enables sending an IM notification to the conference participants. You can set the IM message in the text box.	-
Cisco Recording Announcement	Play Notification for Inbound Calls	Enables playing a prompt for the inbound calls. The audio file can be selected from the dropdown.**	-
	Play Notification for Outbound Calls	Enables playing a prompt for the outbound calls. The audio file can be selected from the dropdown.**	-
Microsoft Teams Recording Announcement	Play Notification for Internal Calls	Enables playing a prompt for the inbound calls.	-
	Play Notification for PSTN /Federated Inbound Calls	Enables playing a prompt for the inbound PSTN/Federated calls.	-
	Play Notification for PSTN /Federated Outbound Calls	Enables playing a prompt for the outbound PSTN/Federated calls.	-
	Play Notification for Conference Calls	Enables playing a prompt to the conference participants.	-
Assigned Roles	Shows the list of roles assigned to the user. A role can be removed by unchecking the checkbox. A new role can be added by checking the checkbox in the list of Available Roles. For more information, see User roles .	-	-

* To add custom notification prompts, refer to the [Installing and configuring the Verba SfB - Lync Announcement service](#) article and go to the **Configure custom prompt for users** section

** To add custom notification prompts, refer to the [Configuring Verba Cisco Recording Announcement for Inbound Calls](#) and [Configuring Verba Cisco Recording Announcement for Outbound PSTN Calls](#) articles and go to the **Configure custom prompt for users** section

After filling out the form, press the **Save** button to save user data in the database. After pressing the button the following settings are automatically applied to the user:

- The user is added to the **Default** group.
- The **Default Call List Layout** is added to the user.

Modifying users

To edit user data, you have to click on the desired row of the table showing registered Verba users.

For the changes to take effect, press the **Save** button. All conditions, which are described in the previous section, have to be met.

Invalidating users

You can invalidate a user by pressing the **Invalidate** button. The system does not delete the user record from the database it simply invalidates the user so functions/calls are not "lost", e.g. searching back for the user in the Users Call list is available, the name of the user is displayed in the call lists. Invalidating the user will disable the user login by setting the **Valid To** field to the current date and time. Invalidated users have * symbol next to their name.

Display Name	Login ID	Extensions	Groups	Roles	Authorization Workflow	Valid From	Type
Carrie Reid *	carrie	carrie@verba.com*	Default Customer Services Group US Legal - PipedRipper Team	Standard User Approval Workflow Managers		Jan 1, 1970	Standard

If you are unable to see your invalidated users then click on the **Show Expired Users** on the top right corner in the **Users List** view. You can hide your invalidated users by clicking on the **Hide Expired Users** on the top right corner in the **Users List** view.

Deleting users

To delete a user, click the **Delete** button.

When deleting a user, the system permanently deletes all associated data (except conversation records). Use this function with special care only. The system automatically deletes the following associated data:

Audit Log

Extension Delete or Remove User Association

Group Memberships

Search Criteria

Conversation Share

Calls User Association Will be Cleared

4-eyes Login Will be Cleared

Dashboard Snapshots

Compliance Policy Participant References